

Draft Agenda Regional Standards Group Monthly Meeting

May 14, 2012 | 1:00–3:00 p.m. ET

Dial-In: 866-740-1260 | Access Code: 4391390 | Security Code: 05142012

Agenda

1. Welcome—**Herb Schrayshuen**
2. Review NERC Antitrust and Open Meeting Reminder—**Herb Schrayshuen**
3. Establish Attendance of Regional Standards Group (RSG)—**Herb Schrayshuen**
4. Review Current Agenda—**Herb Schrayshuen**
5. Approval of April 12, 2012 Notes—**Herb Schrayshuen**
6. Review of Action Items*—**Herb Schrayshuen**
7. Elimination of Unnecessary Requirements—**Herb Schrayshuen**
 - What is the role of the Regions in identifying requirements for retirement per FERC's invitation? Compliance and standards personnel in the Regions may be an excellent source for identifying the existing standards and requirements that do not provide significant reliability benefits.
8. Composition of Standard Drafting Teams—**Herb Schrayshuen**
 - Should drafting teams include ERO/Region experts, in addition to industry personnel? It sometimes seems that no one is considering whether the standard is reasonably definite and measurable, and our comments often fall on deaf ears.
9. Winter-weather Event (Feb. 2011)—**Herb Schrayshuen**
 - Want to ensure that everyone is up to speed on efforts to consider how best to institutionalize lessons learned.
10. Future Meetings:
 - 06/11/2012 — Teleconference
 - 07/13/2012 — Face-to-Face (Denver, CO)
 - 08/13/2012 — Teleconference
11. Roundtable

*Background materials included.

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Public Announcements

REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

For face-to-face meeting, with dial-in capability:

Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

August 10, 2010

Draft Notes Regional Standards Group Monthly Meeting

April 12, 2012 | 3:00-6:00 p.m. ET

FRCC-10th Floor-Small Conference Room
The Towers at Westshore
1408 N. Westshore Blvd., Suite 1002
Tampa, FL 33607-4512
Phone Number: 813-289-5644

Dial-In: 866-740-1260 | Access Code: 4413162 | Security Code: 04122012

1. Welcome—**Herb Schrayshuen**

- Herb Schrayshuen welcomed the members of the Regional Standards Group (RSG) and participants.

2. Review NERC Antitrust and Open Meeting Reminder—**Herb Schrayshuen**

- Herb Schrayshuen delivered the Antitrust Guidelines and Open Meeting Reminder to all members and participants. There were no questions raised.

3. Establish Attendance of RSG—**Herb Schrayshuen**

- Meeting attendees:
 - Pete Heidrich, FRCC
 - Nick Henery, FERC
 - Pat Huntley, SERC
 - Don Jones, TRE
 - Steve Myers, ERCOT
 - Lee Pedowitz, NPCC
 - Emily Pennel, SPP RE
 - Steve Rueckert, WECC
 - Guy Zito, NPCC
 - Juan Villar, FERC
 - Howard Gugel, NERC

- Mallory Huggins, NERC
- Barb Nutter, NERC
- Herb Schrayshuen, NERC

4. Review Current Agenda—**Herb Schrayshuen**

- A number of changes were made to the agenda and some agenda items were handled out of order due to travel plans of certain participants. All modifications were agreed to by the group.

5. Approval of March 12, 2012 Notes—**Herb Schrayshuen**

- Meeting notes from March 12, 2012 were reviewed and approved with no changes.

6. Compliance Application Notices (CANs)-RSG Involvement—**Guy Zito**

- Guy discussed his concerns with CANs development and the need for the RSG to engage. No conclusion from the discussion.

7. Regional Standards Once Adopted by the Board of Trustees (BOT) and Approved by FERC-Roles of the Regions and NERC and Division of Responsibilities—**Guy Zito**

- The group discussed the issues related to “ownership” of regional standards once they become FERC approved. The discussion relates also to agenda items 12 and 13 on the next page. Conclusion: Standards, once approved, are “NERC” standards but the regions must be consulted in regard to retirement, or changes, because that is where the technical knowledge that originated the regional standard resides.

8. RSG Charter-Status Report—**Herb Schrayshuen**

- The email sent on April 13, 2012, containing the draft charter based on the Executive Management Group (EMG) instructions did not reach the group. The group will review the issued draft and provide comments by April 24, 2012. The meeting where the issues will be discussed with the EMG is on April 27, 2012.
- The RSG objectives remain unchanged in the initial draft.
- The governance changes called for by the EMG are largely acceptable (pending specific comments), except for the call for closed meetings. Those RSG members in attendance agree that meetings should be open and that recommendation will be made to the EMG.

9. Informal Feedback on Standards Under Development by Regional Standards Reviewers—**Mallory Huggins**

- Mallory solicited input from the group regarding the needs for regional input to standards under development by the regional technical committees. A plan was developed whereby

Mallory would reach out to each regional standards manager to initiate reviews when needed.

10. RSG Report to ERO EMG—**Howard Gugel**

- Howard solicited comments on the report to the EMG. None were offered and the report will go forward to the next EMG meeting to be included in the Standards Report to the Standards Oversight and Technology Committee (SOTC) in May, 2012.

11. Whitepaper (Regional Variances and Regional Standards) Comments from Regional Executives—**Howard Gugel**

- The Whitepaper with modifications from the EMG was accepted by the RSG.

12. Retirement of Regional Standards Requirements in light of North American Standards Approvals—**Herb Schrayshuen**

- The group discussed the need to develop processes for retiring regional standards and rapidly making changes in a lock-step manner with North American standard implementation plans, where regional standards requirements need to be changed or retired, so as to not conflict. It was discussed that the regional boards should have a role in the process. It was agreed to develop a common template/statement for addition to regional standards processes to accommodate this need. Those that have their processes open for review and redevelopment (FRCC, NPCC and others, if any) will take on the initial effort in that regard and share their proposal with the group.

13. Regional Standards—Where and How They Are Displayed on the NERC Website(s)—**Guy Zito & Kristin Iwanechko**

- It was agreed that the regions should be pointing to the NERC website as the source for regional standards which have been approved.

14. Additional Item from Allen Mosher—**Herb Schrayshuen**

- Allen Mosher requested that the RSG members solicit input from the regional compliance managers regarding the Standards Committee (SC) action on Violation Risk Factors (VRFs) and Violation Severity Levels Pro Forma (VSLs). They agreed to do so. Their initial reaction is that the regional compliance managers would oppose eliminating VRFs and VSLs until they see a better product proposal.

15. Future RSG Meetings:

- 5/14/2012-Teleconference
- 6/11/2012-Teleconference
- 7/13/2012-Face-to-Face

Regional Standards Group 2011-2012 Action Items

Action Item #	Meeting Date	Description	Owner	Next Step	Due Date	Comments	Status
08.15.2011.30	08/15/2011	Create a Whitepaper Explaining Regional Variances	Howard	Waiting for comments from Regional executives. Comment period closes 3/15. Comments compiled and sent to RSG on 4/12, comments due back by 4/20	04/20/2012		Open
01.12.2012.34	01/12/2012	Regional Definitions	Howard	Regions to review list Howard sent out on 3/12/2012; classify definitions as follows: BOT Approved, Used by Region, In-Development. Revised list sent on 4/12. RSG members to review and provide updates by 4/20.	04/20/2012		Open
02.21.2012.39	02/21/2012	Philosophy of Each Region on Regional Standards	Tony	Still compiling replies, one (1) region outstanding	04/12/2012		Completed
02.21.2012.40	02/21/2012	Prepare UFLS report	Herb	A draft of the report will be issued for review by the RSG	3/19/2012		Completed
03.12.2012.41	03/12/2012	Regions to Comment on Fill-in-the Blank Status Report	Herb	Herb will send out report to the RSG_plus list; Comments due back by 3/19	03/19/2012		Completed
04.12.2012.42	04/12/2012	Add Mallory Huggins to RSG list	Herb	Ensure Mallory appears on list	04/20/2012		Open
04.12.2012.43	04/12/2012	Continue Charter Drafting		Regions Respond by April 24	4/24/2012		Open

Draft Notes

Regional Standards Group Monthly Meeting

May 14, 2012 | 1:00-3:00 p.m. ET

Dial-In: 866-740-1260 | Access Code: 4391390 | Security Code: 05142012

1. Welcome—**Herb Schrayshuen**

- Herb Schrayshuen welcomed the members of the Regional Standards Group (RSG) and participants.

2. Review NERC Antitrust and Open Meeting Reminder—**Herb Schrayshuen**

- Herb Schrayshuen delivered the Antitrust Guidelines and Open Meeting Reminder to all members and participants. No questions were raised.

3. Establish Attendance of RSG—**Herb Schrayshuen**

- Meeting attendees:
 - Pete Heidrich, FRCC
 - Pat Huntley, SERC
 - Anthony Jablonski,
 - Don Jones, TRE
 - Lee Pedowicz, NPCC
 - Emily Pennel, SPP RE
 - Guy Zito, NPCC
 - Val Agnew, NERC
 - Howard Gugel, NERC
 - Barb Nutter, NERC
 - Herb Schrayshuen, NERC

4. Review Current Agenda—**Herb Schrayshuen**

- Herb Schrayshuen reviewed current agenda and requested the addition of two agenda items: Item 11 - RSG Charter Update from Herb and Item 12 – VSLs/VRFs Project Update from Pete Heidrich; due to scheduling restraints, original item #7 will be addressed first. There were no objections.

5. Elimination of Unnecessary Requirements—**Val Agnew**

- What is the role of the Regions in identifying requirements for retirement per FERC's invitation? Compliance and standards personnel in the Regions may be an excellent source for identifying the existing standards and requirements that do not provide significant reliability benefits.
 - i. Two meetings set up; Regions engaged and trades included; in initial stage on approach to project; will set up timeline and develop list of recommended requirements to consider for elimination.

6. Approval of April 12, 2012 Notes—**Herb Schrayshuen**

- Meeting notes from April 12, 2012 were reviewed and unanimously approved with no changes.

7. Review of Action Items*—**Herb Schrayshuen**

- Reviewed and updated.

8. Composition of Standard Drafting Teams—**Herb Schrayshuen**

- Should drafting teams include ERO/Region experts, in addition to industry personnel? It sometimes seems that no one is considering whether the standard is reasonably definite and measurable, and our comments often fall on deaf ears.
 - i. Regional Executives initially advised there will be no new regional standards; RFC removed theirs; FRCC has some on hold; TRE has one, WECC has three; per Tim Gallagher, regions may propose variances only but reserve the right to create standards, if necessary. Regional drafting teams – can participate with drafting NERC standards; assist with technical writing to facilitate better project management. Compliance will participate as well. Some Regions may have problems with locating correct staff/personnel for drafting teams and may need some assistance with development of team members and leadership.

9. Winter-weather Event (Feb. 2011)—**Herb Schrayshuen**

- i. Purpose of the project is to ensure that lessons learned are institutionalized. There is a need for a permanent fix and hopefully consensus on solutions will be the outcome. At a minimum, generators must disclose output shortfalls.

10. RSG Charter – Will send updated charter, as it stands, to Tim Gallagher; regional execs will have to discuss and propose their changes.
11. VSLs/VRFs Project – Pete Heidrich updated status on project; there is room for improvement. Some regions use them; need more consistency. With more technical personnel, crafting should become easier for drafting teams.
12. Future RSG Meetings:
 - 6/11/2012 — Teleconference
 - 7/13/2012 — Face-to-Face (Denver, CO) changed to afternoon of July 12-details to follow
 - 8/13/2012 — Teleconference
13. Roundtable – Emily Pennel from SPP advised that the SPP Board of Trustees has not, yet, approved the SPP UFLS standard, but expects to address it in a meeting in the near future. Howard Gugel from NERC will send out a memo re: definitions.

Meeting adjourned at 2:33 p.m.

Regional Standards Group 2011-2012 Action Items

Action Item #	Meeting Date	Description	Owner	Next Step	Due Date	Comments	Status
05.14.2012.44	05/14/2012	Legal and Compliance Status on Regional Criteria Embedded in Standards	Herb	Will report at next meeting.			Open
05.14.2012.45	05/14/2012	Share Regional Criteria Assessment with RSG	Pete	Will complete and share by next meeting			Open

Draft Agenda Regional Standards Group Monthly Meeting

July 12, 2012 | 3:00–6:00 p.m. MT

Xcel Energy Offices

1800 Larimer St., 2nd Floor, Boardroom

Denver, CO 80202

Dial-In: 866-740-1260 | Access Code: 4413162 | Security Code: 201207

Agenda

1. **Welcome — Herb Schrayshuen**
2. **Review NERC Antitrust and Open Meeting Reminder — Herb Schrayshuen**
3. **Establish Attendance of Regional Standards Group (RSG) — Herb Schrayshuen**
4. **Review Current Agenda — Herb Schrayshuen**
5. **Approval of May 14, 2012 Notes — Herb Schrayshuen**
6. **Review of Action Items* — Herb Schrayshuen**
7. **Regional Collaboration on Standards Development — Guy Zito**
8. **Regional Standards Removed From the NERC RSDP — Guy Zito**
9. **Review FERC Order 763 and its Relation to Regional UFLS Standards — Howard Gugel**
10. **Update on Standards Outreach — Mallory Huggins**
11. **RSG Charter – Herb Schrayshuen**
12. **Discussion on Latest Version of COM-003-1 - Draft form — Howard Gugel**
13. **Future Meetings:**
 - 08/13/2012 — Teleconference
 - 09/10/2012 — Teleconference
 - 10/12/2012 — Face-to-Face (Miami, FL)
14. **Roundtable**

*Background materials included.

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Public Announcements

REMINDER FOR USE AT BEGINNING OF MEETINGS AND CONFERENCE CALLS THAT HAVE BEEN PUBLICLY NOTICED AND ARE OPEN TO THE PUBLIC

For face-to-face meeting, with dial-in capability:

Participants are reminded that this meeting is public. Notice of the meeting was posted on the NERC website and widely distributed. The notice included the number for dial-in participation. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders.

August 10, 2010

Draft Notes

Regional Standards Group Monthly Meeting

May 14, 2012 | 1:00-3:00 p.m. ET

Dial-In: 866-740-1260 | Access Code: 4391390 | Security Code: 05142012

1. Welcome—**Herb Schrayshuen**

- Herb Schrayshuen welcomed the members of the Regional Standards Group (RSG) and participants.

2. Review NERC Antitrust and Open Meeting Reminder—**Herb Schrayshuen**

- Herb Schrayshuen delivered the Antitrust Guidelines and Open Meeting Reminder to all members and participants. No questions were raised.

3. Establish Attendance of RSG—**Herb Schrayshuen**

- Meeting attendees:
 - Pete Heidrich, FRCC
 - Pat Huntley, SERC
 - Anthony Jablonski,
 - Don Jones, TRE
 - Lee Pedowicz, NPCC
 - Emily Pennel, SPP RE
 - Guy Zito, NPCC
 - Val Agnew, NERC
 - Howard Gugel, NERC
 - Barb Nutter, NERC
 - Herb Schrayshuen, NERC

4. Review Current Agenda—**Herb Schrayshuen**

- Herb Schrayshuen reviewed current agenda and requested the addition of two agenda items: Item 11 - RSG Charter Update from Herb and Item 12 – VSLs/VRFs Project Update from Pete Heidrich; due to scheduling restraints, original item #7 will be addressed first. There were no objections.

5. Elimination of Unnecessary Requirements—**Val Agnew**

- What is the role of the Regions in identifying requirements for retirement per FERC's invitation? Compliance and standards personnel in the Regions may be an excellent source for identifying the existing standards and requirements that do not provide significant reliability benefits.
 - i. Two meetings set up; Regions engaged and trades included; in initial stage on approach to project; will set up timeline and develop list of recommended requirements to consider for elimination.

6. Approval of April 12, 2012 Notes—**Herb Schrayshuen**

- Meeting notes from April 12, 2012 were reviewed and unanimously approved with no changes.

7. Review of Action Items*—**Herb Schrayshuen**

- Reviewed and updated.

8. Composition of Standard Drafting Teams—**Herb Schrayshuen**

- Should drafting teams include ERO/Region experts, in addition to industry personnel? It sometimes seems that no one is considering whether the standard is reasonably definite and measurable, and our comments often fall on deaf ears.
 - i. Regional Executives initially advised there will be no new regional standards; RFC removed theirs; FRCC has some on hold; TRE has one, WECC has three; per Tim Gallagher, regions may propose variances only but reserve the right to create standards, if necessary. Regional drafting teams – can participate with drafting NERC standards; assist with technical writing to facilitate better project management. Compliance will participate as well. Some Regions may have problems with locating correct staff/personnel for drafting teams and may need some assistance with development of team members and leadership.

9. Winter-weather Event (Feb. 2011)—**Herb Schrayshuen**

- i. Purpose of the project is to ensure that lessons learned are institutionalized. There is a need for a permanent fix and hopefully consensus on solutions will be the outcome. At a minimum, generators must disclose output shortfalls.

10. RSG Charter – Will send updated charter, as it stands, to Tim Gallagher; regional execs will have to discuss and propose their changes.
11. VSLs/VRFs Project – Pete Heidrich updated status on project; there is room for improvement. Some regions use them; need more consistency. With more technical personnel, crafting should become easier for drafting teams.
12. Future RSG Meetings:
 - 6/11/2012 — Teleconference
 - 7/13/2012 — Face-to-Face (Denver, CO) changed to afternoon of July 12-details to follow
 - 8/13/2012 — Teleconference
13. Roundtable – Emily Pennel from SPP advised that the SPP Board of Trustees has not, yet, approved the SPP UFLS standard, but expects to address it in a meeting in the near future. Howard Gugel from NERC will send out a memo re: definitions.

Meeting adjourned at 2:33 p.m.

Regional Standards Group 2011-2012 Action Items

Action Item #	Meeting Date	Description	Owner	Next Step	Due Date	Comments	Status
05.14.2012.44	05/14/2012	Legal and Compliance Status on Regional Criteria Embedded in Standards	Herb	Will report at next meeting.			Open
05.14.2012.45	05/14/2012	Share Regional Criteria Assessment with RSG	Pete	Will complete and share by next meeting			Open

Regional Standards Group (RSG) Report to the ERO EMG

August 2012

Overview

This report highlights the key activities of NERC and the Regions in support of the RSG charter obligations in the year 2012.

The RSG meets on a monthly basis and has held six meetings this year, either in-person or by phone. The Regions have worked with NERC staff to perform quality reviews, post Regional Standards to the NERC website, and file Regional Standards and variances with FERC. In addition, the RSG has developed a whitepaper that helps define the differences between Regional Standards and Regional Variances. The RSG also contributed input to the standards section of the Business Plan and Budget Common Assumptions for 2013. As a result of these efforts we report the following:

Regional Standards:

- Regional Standards and Variances adopted by the BOT and filed by NERC with FERC:
 - o IRO-006-TRE-01
 - o PRC-006-SERC-01
 - o PRC-006-NPCC-01
- Regional Standard adopted by the NERC BOT with filings under development for FERC and the applicable Governmental Authorities in Canada
 - o VAR-001-3 – Voltage and Reactive Control (WECC Variance)
- Regional Standards and Variances approved by Regional Entity Board (not included above):
 - o MOD-25-RFC-01 (ReliabilityFirst has requested NERC staff to delay filing this standard with FERC)

Regional Standards Development Activities and Accomplishments:

- NERC Regional Standards staff working in conjunction with the RSG members have:
 - o prepared a unified schedule for all Regional projects in development (See attached)
 - o processed three Regional postings for comment on behalf of the Regions
 - o performed four Quality Reviews on Regional Standards and Variances

Other Activities

- RFC proposed a revised Standard Development Procedure which was approved for filing with the FERC by the NERC Board of Trustees (BOT) in 2011. Subsequent to BOT approval, RFC requested the filing with the FERC be held pending additional changes requested by RFC stakeholders. Those changes have been approved by RFC stakeholders [and Board](#) and were presented ~~to~~[and approved by](#) the [NERC BOT](#) ~~in~~[on](#) May [24, 2012](#). Work on the filing is underway [\(to be updated after word by legal\)](#).
- SERC proposed a revised Standard Development Procedure which was approved for filing with the FERC by the NERC BOT at their February 9, 2012 meeting. The revised procedure was filed with FERC on March 15, 2012. [FERC approved the revised SERC Regional Standard Development Procedure effective June 12, 2012.](#)

Formatted: Font color: Red

Status of Regional UFLS standards

On November 4, 2010, the NERC BOT adopted PRC-006-1 Automatic Underfrequency Load Shedding and directed NERC staff to file the standard with FERC. Included in PRC-006-1 are Interconnection-wide variances for Quebec and WECC. Concurrent with the development of PRC-006-1, several Regions were developing Regional underfrequency load shedding standards based on historical documents and practices. Two of those Regions, SERC and NPCC, subsequently submitted those Regional Standards for adoption by the NERC BOT and they were approved with their associated filings either completed or under development. SPP RE has developed its Regional Standard with stakeholder consensus and is expecting to present the standard at an upcoming Regional Entity Trustees meeting for action. MRO and TRE have evaluated the continent-wide standard and have determined that it provides sufficient reliability coverage in their respective Regions. FRCC is currently performing a comparison between the NERC BOT approved continent-wide standard and the FRCC Underfrequency Program to determine if there are any reliability gaps that would require further action in the form of a Regional Standard or a Regional Variance to the continent-wide standard. Finally, RFC has suspended the current RFC UFLS standard drafting efforts indefinitely until such time the associated NERC standard (PRC-006-1) is enforced and effective. [At such time, RFC will re-evaluate if any reliability gaps exist which would facilitate further action.](#)

Status of Efforts to Address Version 0 (Fill-In-The-Blank) Standards

The Regional Reliability Standards Working Group (RRSWG) issued a report in October of 2006 establishing a systematic methodology for resolving the potential issues surrounding the existing NERC Reliability Standards that contain "fill-in-the-blank" characteristics. The Report identified 31 continent-wide standards that needed to be addressed and established a workplan to meet the needs identified. Of the 31 fill-in-the-blank standards identified in that 2006 report, revisions to ten standards have been completed; seven are scheduled to be completed in 2012, two in 2014, one in 2015, nine in 2016, and the last two in 2017.

ID		Task Name	Duration	Start	Finish	2012												2013					
						e	Jan	e	Mar	Apr	a	Jun	Jul	Aug	e	Oct	o	De	Jan	e	Mar	Apr	a
1		PRC-012-NPCC-1 (on hold)	0 days	Mon 1/2/12	Mon 1/2/12																		
2		BAL-002-NPCC-1 (on hold)	0 days	Mon 1/2/12	Mon 1/2/12																		
3		PRC-006-SPP-01	1307 days	Thu 11/1/07	Fri 11/2/12																		
4		Regional standard development	1217 days	Thu 11/1/07	Fri 6/29/12																		
5		Posting of Documents for process evaluation at NERC	45 days	Mon 9/3/12	Fri 11/2/12																		
6		Prepare BOT Material	25 days	Mon 10/1/12	Fri 11/2/12																		
7		Develop Initial Draft of Regulatory Filings	20 days	Mon 10/1/12	Fri 10/26/12																		
8		BAL-001-TRE-1	666 days	Fri 9/10/10	Fri 3/29/13																		
9		Regional standard development	58.38 edays	Fri 9/10/10	Mon 7/9/12																		
10		Posting of Documents for process evaluation at NERC	45 edays	Mon 9/10/12	Thu 10/25/12																		
11		Prepare BOT Material	35 days	Mon 12/17/12	Fri 2/1/13																		
12		Develop Initial Draft of Regulatory Filings	40 days	Mon 2/4/13	Fri 3/29/13																		
13		BAL-002-WECC-1	472 days	Fri 12/10/10	Mon 10/1/12																		
14		Regional standard development	298 days	Fri 12/10/10	Tue 1/31/12																		
15		Posting of Documents for process evaluation at NERC	45 edays	Fri 1/6/12	Mon 2/20/12																		
16		Prepare BOT Material	25 days	Mon 7/2/12	Fri 8/3/12																		
17		Develop Initial Draft of Regulatory Filings	20 days	Tue 9/4/12	Mon 10/1/12																		
18		BAL-004-WECC-1	477 days	Fri 12/10/10	Mon 10/8/12																		
19		Regional standard development	298 days	Fri 12/10/10	Tue 1/31/12																		
20		Posting of Documents for process evaluation at NERC	45 edays	Fri 1/27/12	Mon 3/12/12																		
21		Prepare BOT Material	25 days	Mon 7/2/12	Fri 8/3/12																		
22		Develop Initial Draft of Regulatory Filings	20 days	Tue 9/11/12	Mon 10/8/12																		
23		VAR-001-WECC-1	442 days	Thu 10/14/10	Fri 6/22/12																		
24		Regional standard development	180 days	Thu 10/14/10	Wed 6/22/11																		
25		Posting of Documents for process evaluation at NERC	45 edays	Tue 11/1/11	Fri 12/16/11																		
26		Prepare BOT Material	25 days	Mon 3/12/12	Fri 4/13/12																		
27		Develop Initial Draft of Regulatory Filings	25 days	Mon 5/21/12	Fri 6/22/12																		

Project: Unified Regional Project Sche
Date: Tue 7/10/12

Task

Split

Progress

Milestone

Summary

Project Summary

External Tasks

External Milestone

Deadline

Agenda

Standards Committee

May 10, 2012 | 1-5 p.m. Eastern
Phone Number: 1-866-740-1260
Meeting Code: 4685998
Security Code: 1234321

Introductions and Chair's Remarks
NERC Antitrust Compliance Guidelines *
Public Announcement *
SC Expectations *
Agenda

1. Review of Agenda (Approve)

Quorum obtained.

SAR on footnote b added.

Request to defer discussion on item 5f as Herb is not available.

Add to 4a discussion on operating personnel communications protocol SDT.

Agenda approved as modified.

2. Waiver of 5-day Rule (Approve)

3. Consent Agenda (Approve)

a. April 11-12, 2012 Standards Committee Meeting Minutes * **(Approve)**

b. April 30, 2012 Standards Committee's Executive Committee Meeting Minutes* **(Ratify)**

The SCEC approved the Analysis of NERC Standards Process Results First Quarter 2102 Report for inclusion in NERC's quarterly filing to the Federal Energy Regulatory Commission.

Discussion:

3a pulled out of consent agenda.

Item 5dvii on Default Language in the Evidence Retention Section of Standards.

Question on whether staff or SC should make this determination as stated in the SC meeting minutes.

Language in minutes will be modified as per advice on NERC legal dept.

Minutes approved.

4. Projects under Active Development (Review)

a. Status of Projects Under Active Development* (A. Rodriguez)

Two Projects Pending Reforecast

- *Project 2007-12 Frequency Response. This project is currently showing as 1.5 months late, but is pending reforecast following the second of two proposed technical*

conferences. It is also reliant on FERC's approval of the proposed conferences and schedule development proposal.

- *Project 2010-13.2 Phase 2 of Relay Loadability: Generation. This project is moving from informal development to formal development, and its schedule is being revised.*

One Project with a New Schedule

- *2007-17 Protection System Maintenance and Testing (see below)*

Two Projects Ahead of Schedule

- *2007-03 Real-Time Operations*
- *2010-07 Generator Requirements at the Transmission interface*

Six Projects on Schedule (+/- One Month)

- *2006-06 Reliability Coordination*
- *2007-02 Operating Personnel Communication Protocols*
- *2008-06 Cyber Security order 706*
- *2010-05.1 Phase 1 of Protection Systems: Misoperations*
- *2009-01 Disturbance and Sabotage Reporting*
- *2010-17 Definition of BES Phase 2*

Three Projects behind Schedule

- *2007-09 Generator Verification: This project is approximately 3.5 months behind schedule (no change since last report)*
- *2007-06 System Protection Coordination: This project received greater attention while in QR to consider Results-based feedback. The project is approximately 6 months behind schedule largely due to taking additional time to improve the Results-based aspects of the documents, as previously discussed and reviewed with the SC at its March 2012 meeting.*
- *2010-14.1 Balancing Authority Reliability-based Controls: Reserves: This project is currently showing as 4.5 months late; however, the posting for this project was delayed 40 days to reduce overall posting load (per decision of the SCEC, based on staff analysis and recommendation). Dependences related to 2007-12 Frequency Response may result in changes to this schedule; additionally, this project may be expanded to incorporate additional work related to BAL-002 and/or BAL-004 (further discussion later in this agenda).*

One Rapid Revision Awaiting Filing

- *Project 2011-INT-01 Interpretation of MOD-028 for Florida Power & Light Company Two Rapid Revisions Awaiting Posting*
- *Project 2010-INT-01 Interpretation of TOP-006 for FMPP*
- *Project 2011-INT-02 Interpretation of VAR-002 for Constellation Power Gen*

b. Status of Outstanding Interpretations* (A. Rodriquez)

Two Interpretations Awaiting Filing

- Project 2008-10 Interpretation of CIP-006-1 for Progress Energy
- Project 2009-22 Interpretation of COM-002-2 for the IRC

Two Interpretations Awaiting Board Approval

- Project 2009-26 Interpretation of CIP-004-1 for WECC
- Project 2010-INT-05 CIP-002-1 for Duke Energy

Three Interpretations in Current Development

- Project 2012-INT-02 TPL-003-0a and TPL-004 for SPCS (In drafting)
- Project 2012-INT-03 CIP-007 for TECO (In drafting)
- Project 2012-INT-05 CIP-002-3 for OGE (In drafting)

Five Interpretations in Planning Queue

Discussion on COM-003: Concern that it potentially modifies definition of reliability directive.

Response: text box is just a reference; no intent to modify the definition.

Reliability directive is a subset of operating communications.

Comment could be to delay this standard until the Reliability Coordination team working on the definition has completed its project.

Also, the announced whitepaper is not available yet.

To be taken off-line to see if there are ways to clarify.

c. Posting Projections Through August 2012* (A. Rodriquez)

Interim Project Master Scheduler

Project	Task	Priority	Start	Finish	Lead/Lag	10/30/01	11/30/01	12/30/01	1/30/02	2/28/02	3/30/02	4/30/02	5/30/02	6/30/02	7/30/02	8/30/02	9/30/02	10/30/02	11/30/02	12/30/02	1/30/03	2/28/03	3/30/03	4/30/03	5/30/03	6/30/03	7/30/03	8/30/03	9/30/03	10/30/03	11/30/03	12/30/03	1/30/04	2/28/04	3/30/04	4/30/04	5/30/04	6/30/04	7/30/04	8/30/04	9/30/04	10/30/04	11/30/04	12/30/04	1/30/05	2/28/05	3/30/05	4/30/05	5/30/05	6/30/05	7/30/05	8/30/05	9/30/05	10/30/05	11/30/05	12/30/05	1/30/06	2/28/06	3/30/06	4/30/06	5/30/06	6/30/06	7/30/06	8/30/06	9/30/06	10/30/06	11/30/06	12/30/06	1/30/07	2/28/07	3/30/07	4/30/07	5/30/07	6/30/07	7/30/07	8/30/07	9/30/07	10/30/07	11/30/07	12/30/07	1/30/08	2/28/08	3/30/08	4/30/08	5/30/08	6/30/08	7/30/08	8/30/08	9/30/08	10/30/08	11/30/08	12/30/08	1/30/09	2/28/09	3/30/09	4/30/09	5/30/09	6/30/09	7/30/09	8/30/09	9/30/09	10/30/09	11/30/09	12/30/09	1/30/10	2/28/10	3/30/10	4/30/10	5/30/10	6/30/10	7/30/10	8/30/10	9/30/10	10/30/10	11/30/10	12/30/10	1/30/11	2/28/11	3/30/11	4/30/11	5/30/11	6/30/11	7/30/11	8/30/11	9/30/11	10/30/11	11/30/11	12/30/11	1/30/12	2/28/12	3/30/12	4/30/12	5/30/12	6/30/12	7/30/12	8/30/12	9/30/12	10/30/12	11/30/12	12/30/12	1/30/13	2/28/13	3/30/13	4/30/13	5/30/13	6/30/13	7/30/13	8/30/13	9/30/13	10/30/13	11/30/13	12/30/13	1/30/14	2/28/14	3/30/14	4/30/14	5/30/14	6/30/14	7/30/14	8/30/14	9/30/14	10/30/14	11/30/14	12/30/14	1/30/15	2/28/15	3/30/15	4/30/15	5/30/15	6/30/15	7/30/15	8/30/15	9/30/15	10/30/15	11/30/15	12/30/15	1/30/16	2/28/16	3/30/16	4/30/16	5/30/16	6/30/16	7/30/16	8/30/16	9/30/16	10/30/16	11/30/16	12/30/16	1/30/17	2/28/17	3/30/17	4/30/17	5/30/17	6/30/17	7/30/17	8/30/17	9/30/17	10/30/17	11/30/17	12/30/17	1/30/18	2/28/18	3/30/18	4/30/18	5/30/18	6/30/18	7/30/18	8/30/18	9/30/18	10/30/18	11/30/18	12/30/18	1/30/19	2/28/19	3/30/19	4/30/19	5/30/19	6/30/19	7/30/19	8/30/19	9/30/19	10/30/19	11/30/19	12/30/19	1/30/20	2/28/20	3/30/20	4/30/20	5/30/20	6/30/20	7/30/20	8/30/20	9/30/20	10/30/20	11/30/20	12/30/20	1/30/21	2/28/21	3/30/21	4/30/21	5/30/21	6/30/21	7/30/21	8/30/21	9/30/21	10/30/21	11/30/21	12/30/21	1/30/22	2/28/22	3/30/22	4/30/22	5/30/22	6/30/22	7/30/22	8/30/22	9/30/22	10/30/22	11/30/22	12/30/22	1/30/23	2/28/23	3/30/23	4/30/23	5/30/23	6/30/23	7/30/23	8/30/23	9/30/23	10/30/23	11/30/23	12/30/23	1/30/24	2/28/24	3/30/24	4/30/24	5/30/24	6/30/24	7/30/24	8/30/24	9/30/24	10/30/24	11/30/24	12/30/24	1/30/25	2/28/25	3/30/25	4/30/25	5/30/25	6/30/25	7/30/25	8/30/25	9/30/25	10/30/25	11/30/25	12/30/25	1/30/26	2/28/26	3/30/26	4/30/26	5/30/26	6/30/26	7/30/26	8/30/26	9/30/26	10/30/26	11/30/26	12/30/26	1/30/27	2/28/27	3/30/27	4/30/27	5/30/27	6/30/27	7/30/27	8/30/27	9/30/27	10/30/27	11/30/27	12/30/27	1/30/28	2/28/28	3/30/28	4/30/28	5/30/28	6/30/28	7/30/28	8/30/28	9/30/28	10/30/28	11/30/28	12/30/28	1/30/29	2/28/29	3/30/29	4/30/29	5/30/29	6/30/29	7/30/29	8/30/29	9/30/29	10/30/29	11/30/29	12/30/29	1/30/30	2/28/30	3/30/30	4/30/30	5/30/30	6/30/30	7/30/30	8/30/30	9/30/30	10/30/30	11/30/30	12/30/30	1/30/31	2/28/31	3/30/31	4/30/31	5/30/31	6/30/31	7/30/31	8/30/31	9/30/31	10/30/31	11/30/31	12/30/31	1/30/32	2/28/32	3/30/32	4/30/32	5/30/32	6/30/32	7/30/32	8/30/32	9/30/32	10/30/32	11/30/32	12/30/32	1/30/33	2/28/33	3/30/33	4/30/33	5/30/33	6/30/33	7/30/33	8/30/33	9/30/33	10/30/33	11/30/33	12/30/33	1/30/34	2/28/34	3/30/34	4/30/34	5/30/34	6/30/34	7/30/34	8/30/34	9/30/34	10/30/34	11/30/34	12/30/34	1/30/35	2/28/35	3/30/35	4/30/35	5/30/35	6/30/35	7/30/35	8/30/35	9/30/35	10/30/35	11/30/35	12/30/35	1/30/36	2/28/36	3/30/36	4/30/36	5/30/36	6/30/36	7/30/36	8/30/36	9/30/36	10/30/36	11/30/36	12/30/36	1/30/37	2/28/37	3/30/37	4/30/37	5/30/37	6/30/37	7/30/37	8/30/37	9/30/37	10/30/37	11/30/37	12/30/37	1/30/38	2/28/38	3/30/38	4/30/38	5/30/38	6/30/38	7/30/38	8/30/38	9/30/38	10/30/38	11/30/38	12/30/38	1/30/39	2/28/39	3/30/39	4/30/39	5/30/39	6/30/39	7/30/39	8/30/39	9/30/39	10/30/39	11/30/39	12/30/39	1/30/40	2/28/40	3/30/40	4/30/40	5/30/40	6/30/40	7/30/40	8/30/40	9/30/40	10/30/40	11/30/40	12/30/40	1/30/41	2/28/41	3/30/41	4/30/41	5/30/41	6/30/41	7/30/41	8/30/41	9/30/41	10/30/41	11/30/41	12/30/41	1/30/42	2/28/42	3/30/42	4/30/42	5/30/42	6/30/42	7/30/42	8/30/42	9/30/42	10/30/42	11/30/42	12/30/42	1/30/43	2/28/43	3/30/43	4/30/43	5/30/43	6/30/43	7/30/43	8/30/43	9/30/43	10/30/43	11/30/43	12/30/43	1/30/44	2/28/44	3/30/44	4/30/44	5/30/44	6/30/44	7/30/44	8/30/44	9/30/44	10/30/44	11/30/44	12/30/44	1/30/45	2/28/45	3/30/45	4/30/45	5/30/45	6/30/45	7/30/45	8/30/45	9/30/45	10/30/45	11/30/45	12/30/45	1/30/46	2/28/46	3/30/46	4/30/46	5/30/46	6/30/46	7/30/46	8/30/46	9/30/46	10/30/46	11/30/46	12/30/46	1/30/47	2/28/47	3/30/47	4/30/47	5/30/47	6/30/47	7/30/47	8/30/47	9/30/47	10/30/47	11/30/47	12/30/47	1/30/48	2/28/48	3/30/48	4/30/48	5/30/48	6/30/48	7/30/48	8/30/48	9/30/48	10/30/48	11/30/48	12/30/48	1/30/49	2/28/49	3/30/49	4/30/49	5/30/49	6/30/49	7/30/49	8/30/49	9/30/49	10/30/49	11/30/49	12/30/49	1/30/50	2/28/50	3/30/50	4/30/50	5/30/50	6/30/50	7/30/50	8/30/50	9/30/50	10/30/50	11/30/50	12/30/50	1/30/51	2/28/51	3/30/51	4/30/51	5/30/51	6/30/51	7/30/51	8/30/51	9/30/51	10/30/51	11/30/51	12/30/51	1/30/52	2/28/52	3/30/52	4/30/52	5/30/52	6/30/52	7/30/52	8/30/52	9/30/52	10/30/52	11/30/52	12/30/52	1/30/53	2/28/53	3/30/53	4/30/53	5/30/53	6/30/53	7/30/53	8/30/53	9/30/53	10/30/53	11/30/53	12/30/53	1/30/54	2/28/54	3/30/54	4/30/54	5/30/54	6/30/54	7/30/54	8/30/54	9/30/54	10/30/54	11/30/54	12/30/54	1/30/55	2/28/55	3/30/55	4/30/55	5/30/55	6/30/55	7/30/55	8/30/55	9/30/55	10/30/55	11/30/55	12/30/55	1/30/56	2/28/56	3/30/56	4/30/56	5/30/56	6/30/56	7/30/56	8/30/56	9/30/56	10/30/56	11/30/56	12/30/56	1/30/57	2/28/57	3/30/57	4/30/57	5/30/57	6/30/57	7/30/57	8/30/57	9/30/57	10/30/57	11/30/57	12/30/57	1/30/58	2/28/58	3/30/58	4/30/58	5/30/58	6/30/58	7/30/58	8/30/58	9/30/58	10/30/58	11/30/58	12/30/58	1/30/59	2/28/59	3/30/59	4/30/59	5/30/59	6/30/59	7/30/59	8/30/59	9/30/59	10/30/59	11/30/59	12/30/59	1/30/60	2/28/60	3/30/60	4/30/60	5/30/60	6/30/60	7/30/60	8/30/60	9/30/60	10/30/60	11/30/60	12/30/60	1/30/61	2/28/61	3/30/61	4/30/61	5/30/61	6/30/61	7/30/61	8/30/61	9/30/61	10/30/61	11/30/61	12/30/61	1/30/62	2/28/62	3/30/62	4/30/62	5/30/62	6/30/62	7/30/62	8/30/62	9/30/62	10/30/62	11/30/62	12/30/62	1/30/63	2/28/63	3/30/63	4/30/63	5/30/63	6/30/63	7/30/63	8/30/63	9/30/63	10/30/63	11/30/63	12/30/63	1/30/64	2/28/64	3/30/64	4/30/64	5/30/64	6/30/64	7/30/64	8/30/64	9/30/64	10/30/64	11/30/64	12/30/64	1/30/65	2/28/65	3/30/65	4/30/65	5/30/65	6/30/65	7/30/65	8/30/65	9/30/65	10/30/65	11/30/65	12/30/65	1/30/66	2/28/66	3/30/66	4/30/66	5/30/66	6/30/66	7/30/66	8/30/66	9/30/66	10/30/66	11/30/66	12/30/66	1/30/67	2/28/67	3/30/67	4/30/67	5/30/67	6/30/67	7/30/67	8/30/67	9/30/67	10/30/67	11/30/67	12/30/67	1/30/68	2/28/68	3/30/68	4/30/68	5/30/68	6/30/68	7/30/68	8/30/68	9/30/68	10/30/68	11/30/68	12/30/68	1/30/69	2/28/69	3/30/69	4/30/69	5/30/69	6/30/69	7/30/69	8/30/69	9/30/69	10/30/69	11/30/69	12/30/69	1/30/70	2/28/70	3/30/70	4/30/70	5/30/70	6/30/70	7/30/70	8/30/70	9/30/70	10/30/70	11/30/70	12/30/70	1/30/71	2/28/71	3/30/71	4/30/71	5/30/71	6/30/71	7/30/71	8/30/71	9/30/71	10/30/71	11/30/71	12/30/71	1/30/72	2/28/72	3/30/72	4/30/72	5/30/72	6/30/72	7/30/72	8/30/72	9/30/72	10/30/72	11/30/72	12/30/72	1/30/73	2/28/73	3/30/73	4/30/73	5/30/73	6/30/73	7/30/73	8/30/73	9/30/73	10/30/73	11/30/73	12/30/73	1/30/74	2/28/74	3/30/74	4/30/74	5/30/74	6/30/74	7/30/74	8/30/74	9/30/74	10/30/74	11/30/74	12/30/74	1/30/75	2/28/75	3/30/75	4/30/75	5/30/75	6/30/75	7/30/75	8/30/75	9/30/75	10/30/75	11/30/75	12/30/75	1/30/76	2/28/76	3/30/76	4/30/76	5/30/76	6/30/76	7/30/76	8/30/76	9/30/76	10/30/76	11/30/76	12/30/76	1/30/77	2/28/77	3/30/77	4/30/77	5/30/77	6/30/77	7/30/77	8/30/77	9/30/77	10/30/77	11/30/77	12/30/77	1/30/78	2/28/78	3/30/78	4/30/78	5/30/78	6/30/78	7/30/78	8/30/78	9/30/78	10/30/78	11/30/78	12/30/78	1/30/79	2/28/79	3/30/79	4/30/79	5/30/79	6/30/79	7/30/79	8/30/79	9/30/79	10/30/79	11/30/79	12/30/79	1/30/80	2/28/80	3/30/80	4/30/80	5/30/80	6/30/80	7/30/80	8/30/80	9/30/80	10/30/80	11/30/80	12/30/80	1/30/81	2/28/81	3/30/81	4/30/81	5/30/81	6/30/81	7/30/81	8/30/81	9/30/81	10/30/81	11/30/81	12/30/81	1/30/82	2/28/82	3/30/82	4/30/82	5/30/82	6/30/82	7/30/82	8/30/82	9/30/82	10/30/82	11/30/82	12/30/82	1/30/83	2/28/83	3/30/83	4/30/83	5/30/83	6/30/83	7/30/83	8/30/83	9/30/83	10/30/83	11/30/83	12/30/83	1/30/84	2/28/84	3/30/84	4/30/84	5/

5. Actions

a. New Requests for Interpretation* (L. Hussey)

i) Request for Interpretation of CIP-002-4 through CIP-009-4 for Lincoln Electric* **(Endorse)**

*Request for Interpretation of CIP-002-4 through CIP-009-4 for Lincoln Electric
The request for interpretation asks for clarity on the following issues:*

- 1. Does a registered entity have 8 calendar quarters to become fully compliant with CIP-002-4, i.e. adopt and apply the Attachment 1 Critical Asset Criteria?*
- 2. Does a "Milestone Category 1" entity per the "Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities" document have 24 months after the identification of new Critical Cyber Asset to implement the protections and documentation as required by CIP-003-4 to CIP-009-4?*

*Recommendation: The standards process staff recommends **rejecting** this request as it is not asking for clarity on a requirement, it is asking for clarity on the details of the implementation schedule.*

Discussion: This RFI is asking about the implementation plan. This is new. Possibility of providing clarification to the requestor by some other means.

Proposal to accept recommendation to reject with the understanding that Herb gets an answer to the question and discusses with the requestor and if necessary modify the RSAW so that industry is also aware.

Herb will report at the next meeting.

Motion approved.

ii) Request for Interpretation of EOP-005-2 for Lincoln Electric* **(Endorse)**

The request for interpretation asks for clarity on the following issues relative to Requirement R6:

- 1. When must a TOP perform its first analysis per R6?*
- 2. Must the TOP have its analysis done prior to the enforcement date and then every 5 years thereafter OR must the TOP complete its first analysis within 5 years after the enforcement date?*

*R6. Each Transmission Operator shall verify through analysis of actual events, steady state and dynamic simulations, or testing that its restoration plan accomplishes its intended function. This shall be completed every five years at a minimum. Such analysis, simulations or testing shall verify:
[Violation Risk Factor = Medium] [Time Horizon = Long-term Planning]*

R6.1. The capability of Blackstart Resources to meet the Real and Reactive Power requirements of the Cranking Paths and the dynamic capability to supply initial Loads.

- R6.2. The location and magnitude of Loads required to control voltages and frequency within acceptable operating limits.*
- R6.3. The capability of generating resources required to control voltages and frequency within acceptable operating limits.*

The compliance operations staff has advised that the Compliance Application Notice addressing this issue (CAN021) is under revision to remove language stating that the first instance of performing some periodic action must occur on or before the compliant date.

*Recommendation: The standards process staff recommends **rejecting** this request as it is not asking for clarity on a requirement, it is asking for clarity on an enforcement issue.*

Discussion: Proposal to accept recommendation to reject with the understanding that Herb gets an answer to the question and discusses with the requestor and if necessary modify the RSAW so that industry is also aware.

Herb will report at the next meeting.

Motion approved.

b. SAR for Revisions to PER-005 – System Personnel Training* (Reject)

The standards process staff received a request to revise PER-005-1 – System Personnel Training from Portland General Electric.

The purpose identified for revising the standard includes the following:

The purpose of the Standard Authorization Request (SAR) is to amend the wording in Requirement R3 of PER-005-1 to conform with the System Personnel Training Standard Drafting Team's (SPT SDT) original intent, which was to allow entities to define the 12-month period to meet their training program requirements. As presently written, the standard has been interpreted by some Compliance Enforcement Authorities (CEA) as requiring a "rolling" twelve-month compliance test.

Requirement R3 states:

R3. At least every 12 months each Reliability Coordinator, Balancing Authority and Transmission Operator shall provide each of its System Operators with at least 32 hours of emergency operations training applicable to its organization that reflects emergency operations topics, which includes system restoration using drills, exercises or other training required to maintain qualified personnel.

*Recommendation: The standards process staff recommends **rejecting** this SAR as the clarity requested already exists in the language contained within CAN010.*

Discussion:

Alice: The CAN cannot be used because the requirement does not use the word "annual"

Motion to defer action until the RSAW is prepared and ask the requestor whether it answers the concern.

Motion approved with one opposed (alice) and one abstention (David K.).

d. SAR for Revisions to PRC-005 – Protection System Maintenance* (Accept)

The standards process staff received a request to revise PRC-005-2 – Protection System Maintenance from the Project 2007-17 Protection System Maintenance and Testing drafting team.

Order 758 that included approval of an interpretation of PRC-005-1- Transmission and Generation Protection System Maintenance and Testing included a directive to revise PRC-005 to include "...maintenance and testing of reclosing relays that can affect the reliable operation of the Bulk-Power System, as discussed above, within these reinitiated efforts to revise Reliability Standard PRC-005."

The drafting team working on PRC-005-2 does not want to stop its work to address the addition of reclosing relays as the team already has consensus on most aspects of PRC-005-2 (the last ballot achieved a 74% approval). The drafting team wants to bring closure to the version of PRC-005 currently under development and immediately thereafter work on the necessary revisions to add reclosing relays.

The work involved in addressing the directive from Order 758 includes the following:

- 1. Modify the definition of Protection System to add reclosing relays.*
- 2. Modify the Facilities portion of the Applicability of PRC-005-2 to describe explicitly those reclosing relays that entities are to maintain in accordance with the revised standard.*
- 3. Modify the Tables within PRC-005-2 to include intervals and activities appropriate for reclosing relays, with consideration for the technology of the reclosing relays and for any condition monitoring that may be in place on the relays.*
- 4. Modify Table 1-5 of PRC-005-2 to include the control circuitry associated with reclosing relays being addressed.*
- 5. Modify the Measures and Violation Severity Levels as necessary to address the modified requirements.*

The team also intends to modify the Supplementary Reference Document (provided as a technical reference for PRC-005-2) to provide the rationale for the maintenance activities and intervals within the modified standard, as well as to provide application guidance to industry.

Recommendation: The standards process staff recommends accepting this SAR and posting it for information but recommends deferring activity in modifying PRC-005-2 and the definition of Protection System until PRC-005-2 has completed its recirculation ballot.

Motion to accept the SAR as phase 2 of the project 2007-17.

Would follow on the high priority due to FERCs directive.

Motion approved.

e. SAR for Statutory Definitions – Bulk Power System, Reliability Standard, Reliable Operation* (Accept)

In paragraph 1894 of Order 693 the Commission directed the Electric Reliability Organization to include the statutory definitions of Bulk Power System, Reliability Standard, and Reliable Operation in the NERC Glossary of Terms Used in Reliability Standards:

“1894. The Commission directs the ERO to modify the glossary through the Reliability Standards development process to include the statutory definitions of the terms Bulk-Power System, Reliable Operation and Reliability Standard. However, this determination does not negate our discussion in the Applicability section of the Final Rule. While the glossary should be revised to include the statutory definition of Bulk-Power System, the Reliability Standards refer to the bulk electric system, which is also defined in the glossary.”

The proposed definitions are:

- “Bulk Power System” means, depending on the context: (i) Facilities and control systems necessary for operating an interconnected electric energy supply and transmission network (or any portion thereof), and electric energy from generating facilities needed to maintain transmission system reliability. The term does not include facilities used in the local distribution of electric energy.*
- “Reliability Standard” means a requirement to provide for Reliable Operation of the Bulk Power System, including without limiting the foregoing, requirements for the operation of existing Bulk Power System Facilities, including cyber security protection, and including the design of planned additions or modifications to such Facilities to the extent necessary for Reliable Operation of the Bulk Power System, but the term does not include any requirement to enlarge Bulk Power System Facilities or to construct new transmission capacity or generation capacity. A Reliability Standard shall not be effective in the United States until approved by the Federal Energy Regulatory Commission and shall not be effective in other jurisdictions until made or allowed to become effective by the Applicable Governmental Authority.*
- “Reliable Operation” means operating the Elements of the Bulk Power System within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or Cascading failures of such system will not occur as a result of a sudden disturbance, including a Cyber Security Incident, or unanticipated failure of system Elements.*

Request:

NERC’s legal staff advises posting the SAR and definitions without a formal comment period and then balloting and submitting the definitions for Board of Trustee adoption.

Discussion:

Technically this would be a waiver of the process.

Changing a definition changes all the standards where it’s used.

Approved with one abstention (David K.)

Statement in the SAR that it applies only to USA.

f. SAR for Project 2010-15 – Flow Limited Paths* (Accept)

Last year, a problem was identified in MOD-029 – Rated System Path Methodology. Compliance issued a temporary waiver to address this concern, with acknowledgement that a modification to the standard to address the

concern would follow. A group of technical industry experts from several western utilities formed to address this issue and draft a solution. The group reached out to many transmission providers and stakeholders in the Columbia Grid, Northern Tier Transmission Group, WestConnect organizations and the California ISO. This issue and solution have been presented to the WECC Operations Committee, Planning Committee and Market Interface Committee and the steering committees of WestConnect, Columbia Grid and Northern Tier Transmission Group. The attached SAR and whitepaper were submitted to NERC staff relative to this issue and include draft modifications to MOD-029.

Request:

Accept the MOD-029 SAR for Rapid Revision, and direct staff to process using the Rapid Revision process, waiving the 30-day posting and proceeding directly to the 45-day initial ballot posting (subject to scheduling and coordination with existing workload).

Discussion:

Andy: Good candidate for rapid revision process.

Motion to accept the SAR and defer action on initiation of the project depending on prioritization process and staff availability.

Question on whether it should go to SCPS for prioritization?

Motion approved.

g. BAL-002 – Disturbance Control Performance*

The NWPP submitted a request for an interpretation of BAL-002 and that interpretation was not completed. A clear interpretation is necessary to protect system operators from taking extreme measures to move ACE, such as shedding load when it is not operationally necessary to do so, to prevent a finding of noncompliance.

The interpretation drafting team concluded that the language clarifying the requirement is embedded in the compliance section of the standard and cannot be used to develop the interpretation based on the team's interpretation of the Board of Trustees's 2009 guidance relative to interpretations. There is a lack of clarity on the scope of what the board meant when it advised drafting teams to remain within the 'strict construction' of a standard.

This issue was discussed during the April 11-12, 2012 meeting of the Standards Committee and that discussion led to the conclusion that the confusion surrounding BAL-002 is a high priority issue from a reliability perspective and that the best course of action is to seek relief, in this one instance, from the "strict construction policy" for addressing interpretations. Consequently the following request was submitted to the Board of Trustees' Standards Oversight and

Technology Committee (BOT SOTC) for review during its May 2012 BOT SOTC meeting:

If by “strict construction” drafting teams are only allowed to use the language in the requirements of the standard to develop an interpretation, then the drafting team cannot develop an interpretation. However, if the team were allowed to apply “strict construction” to the four corners of the standard, rather than just the language in the requirements, then the drafting team can develop a clear interpretation.

Granting this relief would permit the use of the language in the compliance section of the standard and would make it clear to operators what the limits of their obligations are with respect to responses to rebalance the system after system disturbances.

Alternatives:

If the BOT SOTC determines that the drafting team may, in this instance, use the information contained in the compliance section of the standard to develop its interpretation, then the standards staff recommends that the Standards Committee direct staff to reconvene the interpretation drafting team and develop the interpretation.

If the BOT SOTC does not determine that the drafting team may use the information contained in the compliance section of the standard to develop its interpretation, then the standards staff recommends that the Standards Committee accept the SAR from the NWPP for processing.

Three Options:

Option 1 – Expedited Standard Development Process: Because the lack of clarity in BAL-002 has, in at least one instance, already caused a Balancing Authority to shed load unnecessarily, the revisions to the standard qualify for processing under the “Expedited” Process. The following language from the Standard Processes Manual describes the conditions for use of the

Expedited Process:

NERC may need to develop a new or modified standard, VRFs, VSLs, definition, variance, or implementation plan

- *Shorten the 45-day formal comment period under specific time constraints (such as to meet a time constrained regulatory directive) or to meet an urgent reliability issue such that there isn’t sufficient time to follow all the steps in the normal standards development process.*

Under those conditions, the Standards Committee shall have the authority to approve any of the following actions to expedite development:

- *Shorten the 30-day period for forming the ballot pool*

- *Allow significant modifications following the initial ballot without the need for another formal comment period provided the modifications are highlighted before conducting any successive ballot*

- *Shorten any of the 10-day ballot windows*

If a new or modified standard is developed, approved by its ballot pool, and subsequently adopted by the NERC Board of Trustees through this expedited process, one of the following three actions shall occur²

- *If the standard is to be made permanent without additional substantive changes, then a SAR and a proposed standard shall be submitted to the standards staff immediately after the ballot. The project shall be added to the list of approved projects and shall proceed through the regular standard development process, including balloting by stakeholders, without any intentional delay.*

- *If the standard is to be substantively revised or replaced by a new standard, then a project for the new or revised standard shall be added to the list of projects to be added to the Reliability Standard Development Plan. The project shall be initiated as soon as practical after the ballot and the project shall proceed through the regular standard development process, including balloting by stakeholders, as soon as practical but within two years of the date the standard was approved by stakeholders using the expedited process.*

- *The standard shall be withdrawn through a ballot of the stakeholders within two years of the date the standard was approved by stakeholders using the expedited process.*

Option 2 – Rapid Revision Process: The Standards Committee could use the “Rapid Revision” process and authorize posting the SAR and standard at the same time for a 45-day comment period with an initial ballot during the final 10 days of that comment period.

Option 3 – Normal Process treated as High Priority: Project 2010-14.1 Balancing Authority Reliability Based Controls: Reserves is already in the process of modifying BAL-002 and is seeking to post a new draft of BAL-002 that appears to address the concerns expressed in the NWPP BAL-002 SAR before the end of May 2012. The Standards Committee could direct the Project 2010-14.1 Balancing Authority Reliability Based Controls: Reserves team to move this standard forward in parallel with the other standards in its project with a goal of submitting the revised BAL-002 to the Board of Trustees as soon as possible (separately from the other BARC standards, if necessary).

Issues:

The Project 2010-14.1 team plans has its set of standards ready to post but has delayed posting due to limit the number of standards posted at the same time as the CIP Version 5 standards. If the Standards Committee moves revisions to BAL forward in parallel with the work of Project 2010-14.1, there will be two different versions of BAL-002 posted for comment at the same time. The Project 2010-14.1 team is trying to move its standards forward in support of BAL-003 - Frequency Response.

Discussion:

Allen: BoT-SOTC said we are acting excessively restricted on this and SC has some latitude on how to proceed. SOTC gave authorization to depart from strict construction in this case.

Laura: The most expeditious option is to treat it as an interpretation. Means starting it in 5-6 weeks.

Motion approved.

h. Revised Project Schedule for Project 2007-17 Protection System Maintenance and Testing* (Endorse)

Project 2007-17 Protection System Maintenance and Testing

Based on stakeholder feedback, the team believes it needs to make additional substantive changes to the standard, necessitating another successive ballot period. This increase the estimated delivery date to November of 2012.

Request:

Endorse the revised project schedule for Project 2007-17 Protection System Maintenance and Testing.

i. Disposition of BAL-004-1 – Time Error Correction* (Endorse)

Stakeholders approved a revision to the BAL-004 standard (version 1), which was subsequently adopted by the Board of Trustees and filed with FERC. These revisions were undertaken to eliminate potential “perverse incentives,” in that the standard created a compliance risk for entities providing a voluntary service (acting as Interconnection Time Monitor). That compliance risk served as a disincentive to volunteer to be the Interconnection Time Monitor; hence, the removal of requirements that applied to the volunteer.

FERC issued a NOPR proposing to remand this standard, expressing concern that the elimination of these provisions would result in a lowering

of reliability, and proposed several additional areas for improvement to the standard that would put protections in place to minimize the potential for harm that could be caused by an improper Time Error Correction being initiated.

NERC responded that the performance of Time Error Corrections was not critical to reliability, and that the industry was considering eliminating the obligation to perform Time Error Corrections altogether. NERC recommended that FERC defer action until such time as NERC had been able to perform a field test to determine the feasibility of eliminating Time Error Corrections. Recently, the Operating Committee determined that while there was no reliability risk associated with eliminating Time Error Corrections, the risk of societal harm from such action was not worth the perceived economic and reliability benefits of elimination.

Accordingly, the OC determined that the field test was not appropriate at this time.

However, we still have an outstanding NOPR, proposing remand and several directives. It should be noted that Phase 2 of the BARC project (2010-14) includes BAL-004 within its scope.

Recommendation:

- Direct staff to ask the Board of Trustees for permission to withdraw our petition for the approval of BAL-004-1.*
- Expand the scope of the Project 2010-14.1 team to include modifications to BAL-004 that will (a) eliminate compliance risk for the Interconnection Time Monitor, and (b) ensure adequate protections are in place to minimize the potential for harm that could be caused by an improper Time Error Correction being initiated.*

j. Prioritization of CANS* (To be sent separately)

The Standards Committee received a request to prioritize four new compliance application notices (CANS). The CANS involve four standards:

- COM-002 R1.1*
- EOP-008 R1*
- EOP-005*
- PRC-017 R1.1*

Staff completed the template using compliance information and information from the approved standards.

Recommendations

The standards staff researched the compliance information needed to complete the CAN prioritization template and used that data to populate the CAN prioritization template. The score from the template along with other information available to the standards process staff was used to develop the following recommendations:

- COM-002 R1.1 – Low Priority – The tool produced a score of 425, however this requirement is proposed for retirement one calendar quarter after approval of the revised standard.*
- EOP-008 R1 – Low Priority – The tool produced a score of 400, however this requirement is approved for retirement in 2013.*
- EOP-005 – Medium Priority – The tool produced a score of 355. The information provided does not identify the version of the standard or the associated requirement, however the request for clarity appears to be associated with EOP-005-2 Requirement R17 and some other requirement. The requester should be asked for more details on the specific requirement(s) associated with the need for clarity.*
- PRC-017 R1.1 – Low Priority – The tool produced a score of 355, however for the following reasons, the need for clarity is questionable:*
 - ☐ The standard has been in effect since 2007*
 - ☐ Maintenance programs for SPS systems should have been audited at least once*
 - ☐ Both the old and new definitions of Protection System include all of the devices identified in the request for clarity*

k. Footnote b in TPL standards SAR

On April 19, 2012, FERC issued a Final Rule remanding TPL-002-0b and a Notice of Proposed Rulemaking (NOPR) proposing to remand TPL-001-2. The primary reason cited for both the actual and proposed remand is a lack of clarity regarding a footnote related to allowing a transmission planner to plan for “non-consequential load loss,” i.e., load shedding, following a single contingency. In the Final Rule, the Commission stated that the footnote was “vague, unenforceable and not responsive to the previous Commission directives.” FERC provides a number of suggestions for the industry’s consideration regarding how it might modify the footnote such that it is just, reasonable, not unduly discriminatory or preferential, and in the public interest.

In its NOPR, FERC made the following statement:

“A rapid resolution of this one matter will allow the industry, NERC and the Commission to go forward with the consideration of other improvements contained in proposed Reliability Standard TPL-001-2.”

Accordingly, NERC is proposing to move forward with an effort to resolve this matter expeditiously. NERC staff has reached out to the members of the Project 2006-02 Assess Transmission Future Needs standard drafting team, and begun dialogue to determine an appropriate path forward. In order to expedite the handling of this effort, NERC staff has prepared a SAR to cover this scope of work.

Request:

- *Authorize posting the SAR to revise this TPL Footnote b/Footnote 12 for informal comment with no obligation to respond to the comments*
- *Assign the work to the already formed ATFN SDT*
- *Waive the initial 30-day comment period*
- *Post the following for a 45-day comment period with the formation of a new ballot pool during the initial 30 days of the comment period and an initial ballot during the last 10 days of the comment period:*
 - o TPL-001, TPL-002, TPL-003, TPL-004 from Project 2006-02 with the new Footnote b*
 - o TPL-001 from Project 2011-02 with the new Footnote 12*
- *Direct the drafting team to vet the proposed revision informally before posting formally to gain assurance that the posted version of Footnote b/Footnote 12 will have stakeholder support.*

Order directed to use the expedited review process, thus must be addressed quickly to approve at the Feb BoT meeting.

Approved.

6. Discussion Items

a. Review of MRC/BOT/BOT SOTC Meetings (A. Mosher and H. Schrayshuen)

b. Update on Standards Process Input Group* (A. Mosher)

The Standards Process Input Group (SPIG) organized by the NERC Member Representatives Committee (MRC) is proposing in this report a number of changes to the way NERC develops Reliability Standards and other solutions intended to improve the priority, product and process of standards development. Inherent in these proposed changes is an effort to better understand, articulate and incorporate, into the standards development process, the appropriate accountabilities for standards development.

For example, Section 215 of the Federal Power Act creates accountability for the Federal Energy Regulatory Commission (FERC), first to certify an Electric Reliability Organization (ERO) for the purpose of establishing and enforcing

reliability standards for the bulk power system, and then to approve the standards developed by the ERO. As such, FERC is accountable to the U.S. Congress, which passed the law that created Section 215.

Section 215 also creates accountability for NERC by requiring that the ERO, certified by FERC, have a demonstrated ability to develop and enforce reliability standards that provide for an adequate level of reliability of the bulk power system. This accountability extends to the NERC management to see that high quality standards are developed in an efficient and effective way and to the NERC Board of Trustees (Board) that must approve those standards before they are filed with governmental regulatory authorities in the U.S. and Canada.

Finally, the stakeholders, whose technical expertise is essential to the development of the standards, have a shared accountability with NERC and with each other to see that the right standards are developed in a fair, open, balanced and inclusive way.

One of the principal recommendations of the SPIG, is the creation of a Reliability Issues Steering Committee (RISC) that is intended to address these issues of accountability by ensuring that NERC develops the right standards, in the right way, and in a timely and efficient manner. To accomplish this, the RISC will conduct front-end, high level review of nominated reliability issues and direct the initiation of standards projects or other solutions that will address the reliability issues.

In addition to recommending the creation of the RISC, the SPIG also recommends that Reliability Standards Audit Worksheets (RSAWs) be developed concurrent with their associated standards and posted along with those standards for comment. The purpose here is to make sure that the RSAWs are aligned with the intent and wording of the standards to reduce the need for Interpretations and Compliance Application Notices.

Lastly, the SPIG is recommending a redesign of the composition and process used by Standards Drafting Teams to make more efficient and effective use of the subject matter expertise resident in the industry, and to provide those experts with additional support resources in terms of project management and facilitation, legal expertise, and technical writing support.

The recommendations also aim to strengthen consensus building, first on the need for a standard and then on the requirements themselves.

Collectively, these recommendations suggest a major revision of how decisions to develop standards are determined in the first place and, once the decision is made that a new or revised standard is needed, to see that it is developed in the most efficient, effective, and timely way, taking into account throughout the process the costs, benefits and justification for all standards.

The SPIG provides five recommendations designed for action and for discussion. The analysis of feedback received throughout this project indicates that more discussion should occur around the variety of the changes, improvements, and

implementation being proposed in these recommendations, as listed below and described in more detail in this report.

Recommendation 1: American National Standards Institute — NERC should continue to meet the minimum requirements of the American National Standards Institute (ANSI) process to preserve ANSI accreditation.

Recommendation 2: Reliability Issues Steering Committee — The NERC Board is encouraged to form a Reliability Issues Steering Committee (RSIC) to conduct front-end, high level review of nominated reliability issues and direct the initiation of standards projects or other solutions that will address the reliability issues.

Recommendation 3: Interface with Regulatory and Governmental Authorities — The NERC Board is encouraged to task NERC management, working with a broad array of ERO resources (e.g., MRC, technical committees, Regional Entities, trade associations, etc.) to develop a strategy for improving the communication and awareness of effective reliability risk controls which increases input and alignment with state, federal, and provincial authorities.

Recommendation 4: Standards Product Issues — The NERC board is encouraged to require that the standards development process address:

- *The use of results-based standards (RBS);*
- *Cost effectiveness of standards and standards development;*
- *Alignment of standards requirements/measures with Reliability Standards Audit Worksheets (RSAWs); and*
- *The retirement of standards no longer needed to meet an adequate level of reliability.*

Recommendation 5: Standards Development Process and Resource Issues — The NERC Board is encouraged to require the standards development process to be revised to improve timely, stakeholder consensus in support of new or revised reliability standards. The Board is also encouraged to require standard development resources to achieve and address:

- *Formal and consistent project management; and*
- *Efficient formation and composition of Standard Drafting Teams (SDTs).*

Allen: MRC's view: continue to adhere to ANSI principles but it seems NERC has "over-engineered" process and should take advantage of opportunities to make it more efficient.

Software changes will be needed for the negative votes.

c. Update on Adequate Level of Reliability Task Force* (A. Mosher)

The ALRTF's work re-examines the current NERC definition of ALR, which was adopted by the NERC BOT in February 2008 and filed for informational purposes with the Federal Energy Regulatory Commission in May 2008. The ALRTF has developed seven reliability objectives and associated performance outcomes that collectively describe the performance state that the design, planning, and operation of the BES will achieve when the reliability objectives are met. The ALRTF's work has been reviewed by the standing committees (primarily the Operating Committee, Planning Committee, Standards Committee, and Critical Infrastructure Protection Committee) and approved for industry posting by the Standing Committees Coordination Group. The ALRTF looks forward to reviewing additional input from industry stakeholders.

d. Update on ERO Response to Cold Weather Event* (H. Schrayshuen)

The Reliability Standard Development Plan 2012-2014 included the following in a joint letter from Allen and Herb:

This Plan is intended to be a forecast of the standards work expected to be developed in the coming years. However, a wide variety of electric system events and emerging risks to bulk power system reliability may necessitate deviations from this plan. In order to respond to such threats and initiate development of new or revised standards, the actual deployment of resources to staff this plan may shift. Additionally, the estimated times listed for project completion may change as more is learned about a given project.

NERC currently is investigating the following "emerging issues," each of which may result in the identification of additional standards development work:

- Cold weather preparedness and winterization*
- Geomagnetic disturbances*
- Right-of-way clearances and maintenance*
- System design and planning*
- High Impact/Low Frequency events and disaster preparedness*

Not every issue is addressable or best addressed through development of a new industry standard; the issues outlined above illustrate that truism. But where a standards related response is indicated, we will be ready to reprioritize and adjust.

Herbert is currently working with a group of stakeholder volunteers to review each of the 26 recommendations for the electric utility industry included in the subject report with a goal of determining whether the recommendation should be addressed in a new or revised reliability standard. As envisioned, the work of this ad hoc team will result in a SAR.

There will be a meeting in the first week of June (Atlanta).

e. Status of Process Subcommittee Task Groups (B. Li and L. Campbell)

During the April 2012 Standards Committee Process Subcommittee meeting, the subcommittee formed the following teams to work on developing suggestions for improvements to various aspects of the standard development process:

- **Team 1:** *Analyze areas of the current process that exceed or partially exceed ANSI*

Essential Requirements, and develop recommendations on which of those are necessary to keep and where we could streamline the process without negative consequences (Lead: Cathy Wesley)

- **Team 2:** *Review essential elements of a standard and develop recommendations concerning which elements could be eliminated (Lead: Linda Campbell)*

- **Team 3:** *Make recommendations for simplifying the balloting/commenting process (Lead: Steve Myers)*

- **Team 4:** *Develop draft criteria for evaluating whether a 'No' vote in a ballot should be counted in calculating the ballot approval (Lead: Joe Tarantino)*

The Process Subcommittee has a meeting scheduled in Atlanta on June 7, 2012, but teams have already been working on their assigned tasks.

In view of the later developments, a smaller group (Linda, Ben, Allen and staff) will discuss next week to plan, set priorities and map the recommendations to the 4 teams. Leads of the teams will be included.

Goal is to have BoT approval in November.

7. Coordination (Review)

- a. Coordination with Regulatory and Governmental Authorities (H. Hawkins and A. Dressel)
- b. Coordination with Regional Managers (H. Schrayshuen)

Accepted Regions' view is there will be no new regional standards initiated.

This means that at present there are none scheduled to be developed but if the need arises in the future there might be new regional standards.

Question on whether existing standards would be retired (not discussed).

8. Informational Items (Review)

- a. Drafting Team Vacancies*

Project	Vacancy Description
Project 2010-13.2 Relay Loadability: Generator	Seeking an individual with experience in generator protection systems from the FRCC or MRO region and either the cooperative or merchant electricity generator sector.
Project 2007-12 Frequency Response	Seeking individual representing Transmission Dependent Utilities (TDU) with experience in analyzing or modeling frequency response.
Project 2007-06 System Protection Coordination	Seeking an individual from a Canadian entity with experience in coordination of Protection Systems (new installations and revisions).

- b. Standards Committee Roster*
- c. Highlights of Parliamentary Procedure*
- d. Status of Standards Committee Election (M. Long)

9. Executive Committee Actions (Pre-authorize)

- a. Add Members to CIP IDT
- b. *Other agenda items not discussed today.*

Approved.

10. Adjourn

From: david.kiguel@HydroOne.com
To: [Brian Hogue](#)
Cc: [Guy V. Zito](#); [Lee R. Pedowicz](#)
Subject: RE: My SC Meeting notes
Date: Friday, May 11, 2012 11:55:40 AM

Thank you Brian,

You are correct with the dates.

The discussion at the SC did not get into this as it addressed only the procedural aspect of the request for interpretation and whether questions like the one asked meets the criteria for interpretation or was rather a compliance question.

The decision was to reject the RFI and directed NERC staff to consult and get an answer from Mike Moon and his shop.

David

From: Brian Hogue [mailto:bhogue@npcc.org]
Sent: Friday, May 11, 2012 11:46 AM
To: KIGUEL David
Cc: Guy V. Zito; Lee R. Pedowicz
Subject: RE: My SC Meeting notes

David –

FYI

CIP version 4 Implementation Plan is 7 full calendar quarters. I made the same mistake – concluding it is 8 quarters. The NERC staff that everyone will go corrected me. I would not be surprised if that is part of the reason that FERC's "approval" date is June 25 – only a few days before the next quarter begins. All this means that US enforcement starts April 1, 2014.

-brian

From: david.kiguel@HydroOne.com [mailto:david.kiguel@HydroOne.com]
Sent: Friday, May 11, 2012 8:13 AM
To: Lee R. Pedowicz; rscmembers; joelC@aesi-inc.com; donald.e.nelson@state.ma.us; rjfalsetti@cogeco.ca; guyzito@yahoo.com
Subject: My SC Meeting notes

Hello all,

Please find attached my May 10 SC Teleconference notes.

David

This email and any of its attachments may contain information that is privileged,

confidential, classified as CEII, or subject to copyright belonging to NPCC. This email is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this email, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this email is strictly prohibited and may be unlawful. If you receive this email in error, please notify the sender immediately and permanently delete the original and any copy of this email and any printout.

From: david.kiguel@HydroOne.com
To: kgoodman@iso-ne.com; [Lee R. Pedowicz](#); [rscmembers](#); joelC@aes-inc.com; donald.e.nelson@state.ma.us; rjfalsetti@cogeco.ca; guyzito@yahoo.com
Subject: RE: My SC Meeting notes
Date: Friday, May 11, 2012 3:59:35 PM

Thank you Kathleen,

Let me clarify. What was recommended by staff and approved by the SC is to skip the formal comment period and proceed directly to ballot the definitions.

Skipping the formal comment period constitutes a violation of the process in the manual and must be reported to the CCC. The SC actually has the authority to do this:

Conduct Formal Comment Periods

Most proposed new or modified standards will require a minimum of two formal comment periods where the new or modified standard, its associated VRFs and VSLs, and implementation plan or the proposal to retire a standard and its associated VRFs, VSLs and implementation plan are posted. **The Standards Committee has the authority to waive the initial 30-day formal comment period if the proposed revision to a standard is minor and not substantive.**

In any case, to me, the whole idea of inserting these definitions in the glossary is absurd, thus my abstention in the vote.

David

From: Goodman, Kathleen [mailto:kgoodman@iso-ne.com]
Sent: Friday, May 11, 2012 3:46 PM
To: KIGUEL David; lpedowicz@npcc.org; rscmembers@npcc.org; joelC@aes-inc.com; donald.e.nelson@state.ma.us; rjfalsetti@cogeco.ca; guyzito@yahoo.com
Subject: RE: My SC Meeting notes

David, thanks. I would point out that the below is not a WAIVER of the process, there are no such authority given to the SC to WAIVE anything in the process, though they seem to not follow more than follow.

Thanks for not supporting.

I wonder if there is any recourse for these continued VIOLATIONS of process??? Do you know of any?

- a. SAR for Statutory Definitions – Bulk Power System, Reliability Standard, Reliable Operation* **(Accept)**
- b. *Discussion:*
- c. *Technically this would be a waiver of the process.*
- d. *Changing a definition changes all the standards where it's used.*

From: david.kiguel@HydroOne.com [mailto:david.kiguel@HydroOne.com]
Sent: Friday, May 11, 2012 8:13 AM
To: lpedowicz@npcc.org; rscmembers@npcc.org; joelC@aes-inc.com; donald.e.nelson@state.ma.us;

rjfalsetti@cogeco.ca; guyzito@yahoo.com

Subject: My SC Meeting notes

Hello all,

Please find attached my May 10 SC Teleconference notes.

David

This email and any of its attachments may contain information that is privileged, confidential, classified as CEII, or subject to copyright belonging to NPCC. This email is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this email, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this email is strictly prohibited and may be unlawful. If you receive this email in error, please notify the sender immediately and permanently delete the original and any copy of this email and any printout.

Agenda Standards Committee

June 14, 2012 | 1-5 p.m. Eastern

Phone Number: 1-866-740-1260

Meeting Code: 9834121

Security Code: 1234321

Introductions and Chair's Remarks

NERC Antitrust Compliance Guidelines *

Public Announcement *

SC Expectations *

Agenda

1. Review of Agenda (Approve)

Quorum obtained.

2. Waiver of 5-day Rule (Approve)

Item added on the SCEC authorization item.

3. Consent Agenda (Approve)

a. May 10, 2012 Standards Committee Meeting Minutes * **(Approve)**

b. May 24, 2012 Standards Committee's Executive Committee Meeting Minutes* **(Ratify)**

Minor typographical error to be corrected.

Approved.

4. Projects under Active Development (Review)

a. Status of Projects Under Active Development* (A. Rodriguez)

Project 2006-06 Reliability Coordination

Second set of standards: Successive ballots ended on February 9, 2012.

The balloted standard, COM-001 receive 54.64% approval; however, COM-002, and IRO-001 received considerable approval at 80.62% and 80.21%, respectively.

The three standards were submitted for quality review on May 10. The COM-001-2 QR feedback was received on May 16. The team met on May 18 to respond to QR. The Advisor returned the QR feedback and revised standard to QR. The standards COM-002-3 and IRO-001-3 are proceeding to recirculation ballot.

Project 2007-03: Real-time Operations r0

NERC Legal is now working on the draft filing document but the filing can't be made until coordination issues with other projects are resolved.

Project 2007-09 Generator Verification

MOD-025, MOD-07 and PRC-019: The standards were posted for a 45-day formal comment period and concurrent initial ballot period from February 29 through April 16. The team met May 15-17 and developed responses to comments and revisions to the standards. The team is finalizing the responses to comments and preparing documents for Quality Review.

MOD-026 and PRC-024: The standards were posted for a 30 day formal comment period and successive ballot between February 29th and March 29th. The successive ballot began on March 19 and ended on March 29th. The team is responding to comments and making conforming revisions to the standards. The team met May 15-17 and developed responses to comments and revisions to the standards. The team is finalizing the responses to comments and preparing documents for Quality Review. The team plans to post both standards for a successive ballot.

A coordination issue with RFC standards MOD-024 and MOD-025 is being addressed. RFC is withholding filing of their MOD-024 and MOD-025 standards until the continent-wide standard MOD-025 is approved. They will then evaluate whether the continent-wide standard meets their needs.

Project 2010-07: Generator Requirements at the Transmission Interface

FAC-001-1 and PRC-004-2.1a were adopted by the BOT on February 9, 2012. PRC-005-1.1b and FAC-003-3 were adopted by the BOT on May 9, 2012. All standards will be prepared for filing with FERC.

Note that the schedule has been adjusted to account for the latest modifications to PRC-005 and both versions of FAC-003. Because the project was several months ahead of schedule before these modifications, the overall completion date has not changed since the original projections.

Project 2010-13.2 Generator Relay Loadability

The GENRLOSDT met the week of May 21 at Georgia Power Company, Atlanta. The first draft of standard PRC-025-1 is complete and will be delivered for quality review the week of the Memorial Day holiday. The schedule is still in the process of being developed and finetuned.

Project 2010-17 Definition of BES Phase 2

Phase 2 is well underway. The Planning Committee is taking the lead on investigating threshold limits while the SDT works on a guidance document based on the Phase 1 filing as well as clarification items. The PC has been given a deadline of December 20, 2012 for the completion of its work.

Project 2010-INT-01 Interpretation of TOP-006-2 for FMPP

This project is awaiting 45-day posting and Initial Ballot.

Project 2011-INT-01 Interpretation of MOD-028 for Florida Power & Light Company

Rapid Revision Pilot. Approved at the February Board of Trustees meeting. Awaiting filing. Legal is finalizing the draft petition.

Project 2011-INT-02 Interpretation of VAR-002 for Constellation Power Gen

This Interpretation Request was approved by the SC for Rapid Revision on Jan 12, 2012. The team held two conference calls the week of April 9-13 to discuss comments received and determine the next step for the standard. The team has completed developing responses to comments and made conforming revisions to the standard for QR on April 26th. The documents were submitted to QR on April 30. The team received feedback from QR and made appropriate revisions to the documents and resubmitted them for posting on May 15. The draft standard was posted for a 30 day successive ballot / comment period on May 22.

Project 2007-02 Operating Personnel Communication Protocols

The second draft of COM-003 was posted on May 10, 2012 for a 45-day comment period and the initial ballot (which commences on June 11, 2012). Additionally, the COM 003-01 white paper was posted on May 17.

A Webinar, that will feature how COM-002-3 Draft 6 (RCSDT, Project 2006-6) and COM-003-1 will interact, is scheduled and announced for June 7, 2012.

Project 2007-06 System Protection Coordination

A 45-day formal comment period with a 10-day concurrent initial ballot for draft standard, PRC-027-1 began on Monday, May 21 and end on Thursday, July 5. A new ballot pool will be formed during the first 30 days of the comment period.

NOTE: The SC agreed the delay associated with the QR and results based feedback is acceptable, but did not want to reforecast completion.

The project will continue to be reported as behind schedule, with the understanding that this is an acceptable delay.

Project 2007-12 Frequency Response

NERC filed for an extension of time to complete the proposed standard. FERC responded granting an extension of one year (May 31, 2013) to file a revised standard. NERC held two technical conferences on Frequency Response. The conferences provided additional ideas for the SDT to consider. The SDT is preparing a draft schedule for completing the revised standard. The SDT will be meeting in late June 2012 to address comments from the technical conferences.

Project 2007-17 Protection System Maintenance and Testing

The team continues to discuss several proposed changes to the communication and relay tables. The standard and associated documents will be posted for a 30-day formal comment period with successive ballot. All documents will be submitted for QR when final decisions have been made regarding the tables.

Project 2008-06 Cyber Security Order 706

The SDT continues its work on developing Version 5 of CIP-002 through CIP-011 in response to FERC Order 706. Formal comment and parallel successive ballot ended May 21, 2012.

On April 19, 2012, FERC approved CIP Version 4, which directs a filing deadline of March 31, 2012, to file Version 5.

Project 2009-01 Disturbance and Sabotage Reporting

The standard was posted for a 30-day comment period and successive ballot which ended on May 24, 2012. The team will address comments and prepare for the next meeting which is scheduled for June 6-8, 2012.

Project 2010-05.1 Phase 1 of Protection Systems: Misoperations

The SDT drafted a new version of the standard (requirements and measures only) and sent it to Standards Process for review and feedback before any further work is done. Standards Process returned the feedback from a Quality Reviewer on Friday, May 18 and that was forwarded to the SDT. A Ready Talk meeting is scheduled for Wednesday, May 23 to discuss the comments and recommendations.

Team member assignments will be made for updates and another conference call will be scheduled to review and finalize all documents.

The standard and associated documents are targeted to be posted for a 45-day formal comment period with initial ballot beginning in June.

Project 2010-14.1 Balancing Authority Reliability-based Controls – Reserves

The Standards have been received from Quality Review. The SDT has developed their responses to the Quality Review.

The posting of the draft standards have been delayed due to the posting of other higher priority projects. The draft standards are expected to be posted the week of May 27, 2012.

The SDT will be scheduling meetings to address comments received from the first posting once the proposed standards are posted.

b. Status of Outstanding Interpretations* (A. Rodriquez)

Project 2008-10 Interpretation of CIP-006-1 for Progress Energy

Approved by Board of Trustees on 2/9/2012 (Recirculation ballot: Quorum: 88.02%, Approval: 96.04%). Awaiting filing.

Project 2010-INT-05 CIP-002-1 for Duke Energy

Approved by stakeholders (Recirculation ballot: 94.61% approval). Adopted by BOT at May 2012 meeting. Awaiting filing.

Project 2012-INT-05 CIP-002-3 for OGE

Assigned to CIP IDT. A project team has been formed, and the team is developing the interpretation to be posted for formal comment. Anticipated posting for formal comment in June 2012.

The Request for Interpretation requests clarity on whether a company's SmartGrid Advanced Meter Infrastructure ("AMI") functionality, which may be able to disconnect more than 300 MW of load, is considered a system or facility critical to automatic load shedding under a common control system capable of shedding 300 MW or more under CIP-002-3, Requirement 1.2.5.

Project 2009-26 Interpretation of CIP-004-1 for WECC

Approved by stakeholders (Recirculation ballot: 80.08% approval). Adopted by BOT on May 24, 2012. Awaiting filing.

Project 2012-INT-03 CIP-007 for TECO

Interpretation requests clarification on CIP-007-3, Requirement R5. Specifically, the questions relate to the use of “technical and procedural controls” in Requirement R5, and whether each sub-requirement requires both technical and procedural controls. A project team from the Interpretation Drafting Team has begun to review the request for interpretation to prepare an initial draft for formal comment.

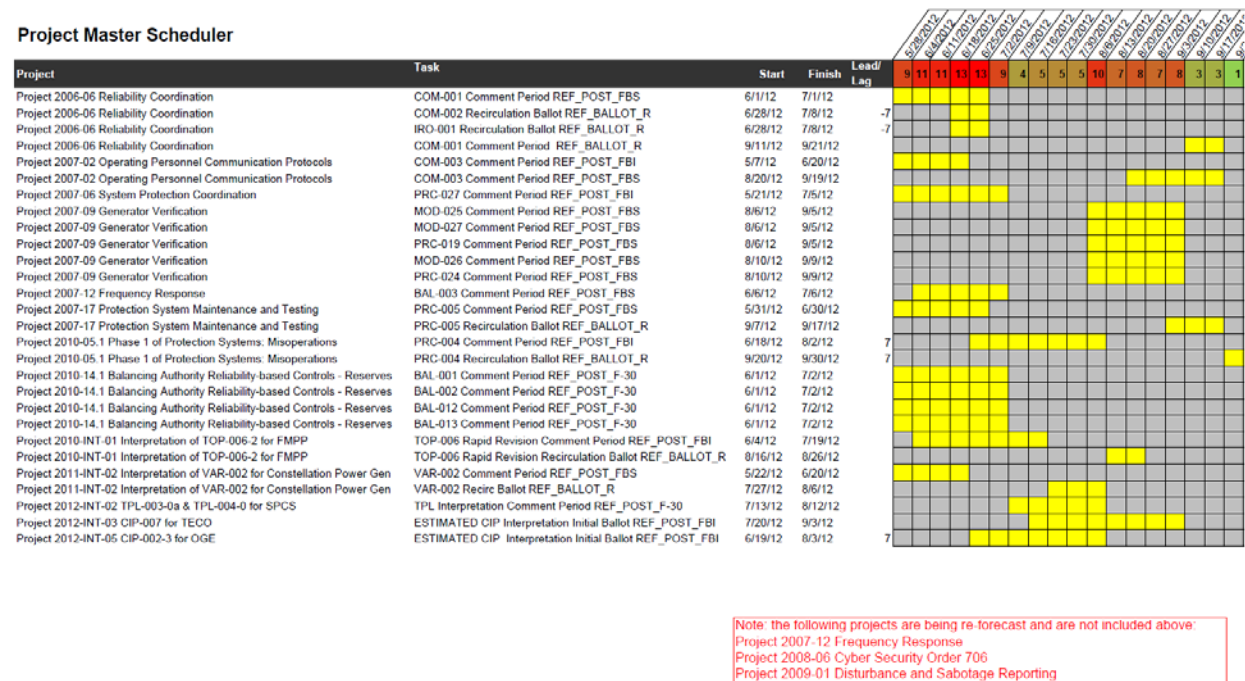
Project 2009-22 Interpretation of COM-002-2 for the IRC

Filing discussed with legal on 4-27-2012. Attorney reviewing filing. Targeting May/June 2012.

Project 2012-INT-02 TPL-003-0a & TPL-004-0 for SPCS

The team met on May 9, 2012 and finalized the responses to the two questions posed by the System Protection and Control Subcommittee. The informal feedback from the regions affirmed the team has provided responses that are consistent with the request. The Advisor is preparing documents for Standards Process quality review to be delivered the week of May 21.

c. Posting Projections Through August 2012* (A. Rodriquez)



5. Actions

a. New Requests for Interpretation* (L. Hussey)

i) Request for Interpretation of TPL-003 and TPL-004 for SPCS (Endorse)

This interpretation request has been developed to address Commission concerns related to the term “Single Point of Failure” and how it relates to system performance and contingency planning clarification regarding the following questions about the listed standards,

requirements and terms. More specifically, clarification is needed about the comprehensive study of system performance relating to Table 1's, Category C and D contingency of a "protection system failure" and specifically the impact of failed components (i.e., "Single Point of Failure"). It is not entirely clear whether a valid assessment of a protection system failure includes evaluation of shared or non-redundant protection system components. Protection systems that have a shared protection system component are not two independent protection systems, because both protection systems will be mutually impacted for a failure of a single shared component. A protection system component evaluation would include the evaluation of the consequences on system performance for the failure of any protection system component that is integral to the operation of the protection system being evaluated and to the operation of another protection system.

On March 30, 2009, NERC issued an Industry Advisory — Protection System Single Point of Failure (i.e., NERC Alert) for three significant events. One of which, the Westwing outage (June 14, 2004) was caused by failure of a single auxiliary relay that initiated both breaker tripping and the breaker failure protection. Since breaker tripping and breaker failure protection both shared the same auxiliary relay, there was no independence between breaker tripping and breaker failure protection systems, therefore causing both protection systems to not operate for the single component failure of the auxiliary relay. The failure of this auxiliary relay is known as a "single point of failure." It is not clear whether this situation is comprehensively addressed by the applicable entities when making a valid assessment of system performance for both Category C and D contingencies.

Discussion:

There have been some changes introduced after submitting the RFI.

Motion to endorse this RFI with its revisions.

Related to the footnote "b" project.

Approved with no opposed or abstentions.

b. Revisions to Standard Processes Manual* ~~(to be sent later)~~ **(Authorize)**

Discussion on treatment of negative votes.

Adjustments to the manual language should be done before posting.

Measures replaced by RSAWs but no reference to RSAWs in the SPM.

VRFs and VSLs eliminated as part of a standard. Replaced by Sanctions Guidelines. SDT will identify type of requirement as per table in the guideline.

Discussion on who may submit a SAR and where it goes (SC or RISC)?

Good communication plan needed.

Staff will introduce revisions to manual and supporting documents by COB June 15 and distribute to the SC.

SC will do an e-mail ballot closing at 1 PM June 18.

c. Revisions to TPL Footnote b/Footnote 12* **(Authorize)**

Revision to the SAR introduced taken from FERC Order. Proposal to use the expedited process.

On April 19, 2012, FERC issued a Final Rule remanding TPL-002-0b and a Notice of Proposed Rulemaking (NOPR) proposing to remand TPL-001-2. The primary reason cited for both the actual and proposed remand is a lack of clarity regarding a footnote related to allowing a transmission planner to plan for “non-consequential load loss,” i.e., load shedding, following a single contingency. In the Final Rule, the Commission stated that the footnote was “vague, unenforceable and not responsive to the previous Commission directives.” FERC provides a number of suggestions for the industry’s consideration regarding how it might modify the footnote such that it is just, reasonable, not unduly discriminatory or preferential, and in the public interest.

In its NOPR, FERC made the following statement:

“A rapid resolution of this one matter will allow the industry, NERC and the Commission to go forward with the consideration of other improvements contained in proposed Reliability Standard TPL-001-2.”

Accordingly, NERC is proposing to move forward with an effort to resolve this matter expeditiously. NERC staff has reached out to the members of the Project 2006-02 Assess Transmission Future Needs standard drafting team, and begun dialogue to determine an appropriate path forward. In order to expedite the handling of this effort, NERC staff has prepared a SAR to cover this scope of work.

At its May 10, 2012 meeting, the Standards Committee approved posting a draft SAR (attached as item 5ci) in the following motion, which was approved without objection or abstention:

- Authorize posting the SAR to revise this TPL Footnote b/Footnote 12 for informal comment with no obligation to respond to the comments*
- Assign the work to the already formed ATFN SDT*
- Waive the initial 30-day comment period*
- Post the following for a 45-day comment period with the formation of a new ballot pool during the initial 30 days of the comment period and an initial ballot during the last 10 days of the comment period:*

☐ TPL-001 from Project 2006-02 with the new Footnote b

☐ ~~TPL~~001, TPL-002, TPL-003, TPL-004 from Project 2011-02 with the new Footnote 12

- Direct the drafting team to vet the proposed revision informally before posting formally to gain assurance that the posted version of Footnote b/Footnote 12 will have stakeholder support*

Following the May SC meeting, the ATFN SDT began working and is scheduled to deliver its documents for quality review at the end of next week. In reviewing the order to make sure we had captured accurately what FERC directed, NERC staff identified possible clarifications to the SAR to align the SAR to align more closely with what is required in

the order. A redlined SAR showing the proposed revisions is included in the agenda materials as item 5cii.

Request: Authorize replacing the SAR included in the May 10, 2012 SC agenda with the revised SAR provided, and otherwise proceeding as previously authorized by the SC.

Approved

6. Discussion Items

a. Update on Standards Process Input Group RISC Mandate* (A. Mosher)

b. Status of Process Subcommittee Task Groups **(to be sent later)** (L. Campbell)

SCPS discussed removal of measures, VRFs and VSLs from the standards replaced by the sanctions table reference. SCPS decided to move forward and let the industry comment.

Whitepapers will be consolidated into one single document.

c. Communications and Planning Subcommittee Report (A. Brown and M. Huggins)

d. SC Role in Prioritization of CANS* (A. Mosher)

The SCPS developed a tool for the prioritization of CANS, which has been applied to an existing group of CANS to rank them as high, medium and low priority for development. However, the SC membership and leadership does not believe it is an appropriate role for the SC as a committee to make the technical judgments that are required to rank CANS for development. Many SC members have individual, company or segment views on the relative importance or need for potential CANS. (For example, APPA has weighed in on the content and priority of a number of different CANS.) However, the SC's committee charter makes it clear that the SC exists to manage the standards process, rather than to act as a technical committee, like the OC, PC and CIPC. In particular, to manage the standards process, the SC:

e. Develops and maintains a work plan (annual) for standards development that prioritizes the existing and future work of the committee and its subgroups, consistent with the strategic and business plans of NERC

f. Develops and maintains a long-term (multi-year) strategic vision that describes the goals and direction for development of standards

Thus in the Three Year Reliability Standards Development Plan, we try to prioritize development based on factors such as potential reliability benefits of the project, regulatory directives/deadlines, cost of compliance and benefits from eliminating ambiguities in the standards, etc. However, the technical assessment of potential reliability improvements or gaps does not come from the SC itself – it comes from our analysis of documents such as NERC's Top Reliability Issues, the technical assessments of the other standing committees, and the subject-matter expertise of stakeholders/segments that the SC's members represent. The SC also relies on the SMEs that make up our standard drafting teams as well as the Standards Departments' project coordinators to advise us on the technical issues associated with standard development.

Suggested course of action:

1. *The Compliance Department with the assistance of other on NERC staff should use the CAN prioritization tool to pre-sort proposed CANS for development. Should you need assistance in updating the tool, the SC can help in that effort.*
2. *The Compliance Department may cc the SC on any request to the other standing committees to prioritize CAN development, but the SC will treat this request as an informational item.*
3. *The SC will also facilitate any technical input on specific CANS that you need – but that input will come from the appropriate Standard Drafting Teams and Interpretation Drafting Teams for the applicable standard or from the members of such SDTs or IDTs. Such inputs will likely be limited to assessing whether or not the proposed CAN expands on the standard/requirement in question, but not on the substance on examples of evidence and compliance interpretation or obligation.*

Also, The SC Process Subcommittee is working on a proposal for a “Single Portal” procedure through which all stakeholders, registered entities, regional entities, and NERC staff can submit requests for formal or informal interpretation and/or guidance on any aspect of a NERC Reliability Standard, including the compliance-related elements of a standard. The idea underlying this proposal is that registered entities often need guidance on both the meaning of a standard and what they need to do to ensure compliance – but their questions often don’t fit neatly into the scope of either a CAN or a formal interpretation. Since the registered entity often just wants to know what it has to do, but wants it in writing from NERC or its region to make sure the entity doesn’t have continuing compliance risk of unmitigated violations, our thinking is that NERC should develop a single portal for “guidance requests” and use a cross-departmental team approach to triage the requests, under which the staff will have a number of options to recommend on how to process the request (which could include informal guidance, formal interpretation, CAN, revised RSAW, a new compliance bulletin, etc.). Once the request is triaged (for the proposed response category and priority) and NERC receives the stakeholder’s concurrence, we will assign responsibility to respond to a cross departmental team (standards, compliance and industry SMEs). Oversight of the response has yet to be determined. (The teams could report to the SC, to the CCC, to NERC or to a hybrid joint committee).

- e. Update on ERO Response to Cold Weather Event (H. Schrayshuen)

Herb asked for volunteers. Good response: 14 industry reps met.

7. Coordination (Review)

- a. Coordination with Regulatory and Governmental Authorities (H. Hawkins)
A number of filings being prepared.
Data request coming on the TPL Order.
- b. Coordination with Regional Managers (H. Schrayshuen)

8. Informational Items (Review)

a. Drafting Team Vacancies*

Four vacancies open. Looking for System Protections SDT Canadian member.

b. Standards Committee Roster*

c. Highlights of Parliamentary Procedure*

9. Executive Committee Actions (Pre-authorize)

a. SAR for Revisions to PER-005 – System Personnel Training*

The standards process staff received a request to revise PER-005-1 – System Personnel Training from Portland General Electric.

The purpose identified for revising the standard includes the following:

The purpose of the Standard Authorization Request (SAR) is to amend the wording in Requirement R3 of PER-005-1 to conform with the System Personnel Training Standard Drafting Team's (SPT SDT) original intent, which was to allow entities to define the 12-month period to meet their training program requirements. As presently written, the standard has been interpreted by some Compliance Enforcement Authorities (CEA) as requiring a "rolling" twelve-month compliance test.

Requirement R3 states:

R3. At least every 12 months each Reliability Coordinator, Balancing Authority and Transmission Operator shall provide each of its System Operators with at least 32 hours of emergency operations training applicable to its organization that reflects emergency operations topics, which includes system restoration using drills, exercises or other training required to maintain qualified personnel.

The Compliance Operations staff issued a Compliance Application Notice (CAN) on this issue which includes the following:

In all standards where the term "annual" is not defined, CEAs are to determine if the registered entity established its own implementation of annual requirements within the parameters provided below. CEAs are instructed to look for a registered entity's documented implementation of annual requirements as the basis for determining compliance. CEAs are to verify whether a registered entity documented either one implementation of annual across all standards that do not specify how an annual requirement is implemented, or an implementation for each individual standard.

CEAs are to verify that a registered entity implemented annual requirements pursuant to the guidelines below:

a) Within a Calendar Year, beginning on January 1 and ending on December 31

(Calendar Year):

In this option, CEAs are to verify that the activity or event is conducted at least once every Calendar Year. A best practice is that the activities or events should not be too far apart. For example, a registered entity's documentation may state that there should be no more than 15 months between the events required by the standard.

Or:

b) Rolling 12 months: The activity or event is conducted at least once within the last 12-month period. Or:

c) CEAs are to verify whether registered entities have documented another implementation of annual requirements along with procedures that define that implementation. However, CEAs are to verify that any alternative documented method demonstrates that the required activity was conducted at least once every Calendar Year.

Regardless of the registered entity's documented implementation of annual, that implementation will not supersede any requirement stated in the standard.

On May 12, 2012, the SC decided to defer action on the SAR until the RSAW for PER-005-2 has been prepared and the requester has had an opportunity to review the RSAW and see if the SAR is still necessary.

Approved

10. Adjourn

*Background materials included.

From: [Goodman, Kathleen](#)
To: david.kiguel@HydroOne.com; [Lee R. Pedowicz](#); [rscmembers](#); joelC@aesi-inc.com; donald.e.nelson@state.ma.us; rjfalsetti@cogeco.ca; guyzito@yahoo.com
Cc: ben@benli.ca
Subject: RE: My SC Meeting notes
Date: Friday, July 13, 2012 2:02:26 PM

David, thanks again. WRT the Interpretation and BOT action, I am continually concerned. NERC and the SC *had taken the position* that the BOT action had limited Interpretations to the Requirements. However, upon further inquiry regarding the Level 1 appeal for the NWPP FRI on BAL-002, the BOT instructed that their *action had been too strictly interpreted and that there action did not limit things contained within the “four corners” of the Standard.*

However, even after this clarification, as I look through the SPM changes, there continues to be this egregious attempt to limit the Industry’s ability to request an appropriate Interpretation and, therefore, stay off inappropriate enforcement.

If need be, I can dig up the BOT action on this.

From: david.kiguel@HydroOne.com [mailto:david.kiguel@HydroOne.com]
Sent: Thursday, July 12, 2012 5:48 PM
To: Goodman, Kathleen; lpedowicz@npcc.org; rscmembers@npcc.org; joelC@aesi-inc.com; donald.e.nelson@state.ma.us; rjfalsetti@cogeco.ca; guyzito@yahoo.com
Cc: ben@benli.ca
Subject: RE: My SC Meeting notes

Thank you Kathleen,

Answers below.

David

From: Goodman, Kathleen [mailto:kgoodman@iso-ne.com]
Sent: Thursday, July 12, 2012 5:17 PM
To: KIGUEL David; lpedowicz@npcc.org; rscmembers@npcc.org; joelC@aesi-inc.com; donald.e.nelson@state.ma.us; rjfalsetti@cogeco.ca; guyzito@yahoo.com
Cc: Ben Li
Subject: RE: My SC Meeting notes

David:

Thanks. Upon review, I have a couple of questions:

Do we know what role Andy is moving into?

Andy's new role is Director of Reliability Risk Analysis and Control. There are more changes in the NERC organization but Herb reported only on those that are related to standards.

I think on the CIP v5, you meant by March 31, 2013, right? Yes, it was a typo, 2013 is correct

Has there been any discussion around disbanding the disturbance and sabotage reporting team now that we have an EA and there does not seem to be an abundance of support from the industry? As a matter of fact, these standards were discussed for inclusion in Phase II of the P81 initiative.

Not that I am aware of.

Has there been any discussion around eliminating the OPSCOM standards initiative? I believe I requested an IRC rep to raise this as a point of discussion at this meeting. Again, there does not seem to be an abundance of support from the industry to pursue these...also, it looks as though there is a proposal to use COM-003 as a trial – for what? I think it's doubtful that this standard will pass

No discussion around eliminating the OPSCOM initiative that I know of.

The trial idea is for having the SDT drafting the RSAWs.

On the RFI for BAL-002 from NWPP: what, exactly, is the hold-up? The SC already approved moving forward with this and yet it does not appear to be getting any “traction”?

There wasn't much discussion other than what was reported by staff and that is in the notes. As you remember from discussions earlier this year, there was a BoT policy that interpretations should only use the language in the requirements and ignore material that could be in other documents. This was waived and now work can proceed. Al DiCaprio can give you more information.

Any input is welcome, thanks.

From: david.kiguel@HydroOne.com [<mailto:david.kiguel@HydroOne.com>]

Sent: Thursday, July 12, 2012 1:01 PM

To: lpedowicz@npcc.org; rscmembers@npcc.org; joelC@aesi-inc.com; donald.e.nelson@state.ma.us; rjfalsetti@cogeco.ca; guyzito@yahoo.com

Subject: My SC Meeting notes

Hello all,

Please find attached my July 11-12 SC meeting notes.

David

This email and any of its attachments may contain information that is privileged, confidential, classified as CEII, or subject to copyright belonging to NPCC. This email is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this email, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this email is strictly prohibited and may be unlawful. If you receive this email in error, please notify the sender immediately and permanently delete the original and any copy of this email and any printout.

Agenda (Revised) Standards Committee

July 11, 2012 | 8-5 p.m. MT
July 12, 2012 | 8-3 p.m. MT

Meeting Location:
Xcel Energy
1800 Larimer St.
2nd Floor Conference Center
Denver, CO 80202

Phone Number: 1-866-740-1260
Meeting Code: 9834121
Security Code: 1234321

Introductions and Chair's Remarks

NERC Antitrust Compliance Guidelines *

Public Announcement *

SC Expectations *

Herb: Changes in NERC staff: Andy Rodriquez moving to other role. Valerie Agnew to replace Andy in Standards.

Agenda

1. Review of Agenda (Approve)

Agenda approved.

2. Waiver of 5-day Rule (Approve)

Approved.

3. Consent Agenda (Approve)

- a. June 14, 2012 Standards Committee Meeting Minutes * **(Approve)**

Approved.

4. Projects under Active Development (Review)

- a. Status of Projects Under Active Development* (A. Rodriguez and V. Agnew)

Two Projects Pending Reforecast

- **2008-06 Cyber Security Order 706.** Several standards in this project failed their most recent ballot, and a new schedule needs to be developed to incorporate an additional ballot period.

The SDT continues its work on developing Version 5 of CIP-002 through CIP-011 in response to FERC Order 706. Formal comment and parallel successive ballot ended May 21, 2012, with several ballots receiving significant improvement.

The team is reviewing comments and will plan to conduct another successive ballot.

On April 19, 2012, FERC approved CIP Version 4, which directs a filing deadline of March 31, 2012, to file Version 5.

The SDT met in Atlanta from June 5-7, 2012, and made significant progress on identifying key industry concerns from the last comment period. They will meet again in Minneapolis in July to continue to refine the standards.

- **2009-01 Disturbance and Sabotage Reporting.** This project failed its most recent ballot, and a new schedule needs to be developed to incorporate an additional ballot period.

The standard was posted for a 30-day comment period and successive ballot which ended on May 24, 2012. The team met June 6-8 and began to respond to comments and revise the standard. The team is preparing for a successive ballot and will be conducting stakeholder outreach over the next month to ensure that the next revision of the standard is ready for a successful ballot. The team plans to hold an industry webinar July 30, 2012 and then hold a team meeting to finalize all documents for posting and successive ballot.

Two Projects Awaiting Schedule Approval

- **Project 2007-12 Frequency Response.**

NERC filed for an extension of time to complete the proposed standard.

FERC responded granting an extension of one year (May 31, 2013) to file a revised standard. NERC held two technical conferences on Frequency Response.

The conferences provided additional ideas for the SDT to consider. The SDT is preparing a draft schedule for completing the revised standard. The SDT met on June 21 & 22 to review comments from the Technical Conference comment period.

- **Project 2010-13.2 Phase 2 of Relay Loadability: Generation.**

The Advisor and Director of Standards Development met via conference call with the team leadership to discuss restructuring the standard into Results-Based Standard (RBS) format. The leadership and advisor planned to introduce the concepts to the team on June 21; however, many did not join the call. The advisor issued the document to the team with a June 29 request for a conference call to reach consensus and move to the first formal 30-day comment period.

The advisor has reached out to the Mark Bennett, Generator Forum to solicit informal feedback before going to the first comment period. Additionally, the team is considering soliciting informal feedback from Jack Cashin from the Electric Power Supply Association (EPSA).

Two Projects Awaiting Filing

- **2007-03: Real-time Operations**

NERC Legal is now working on the draft filing document but the filing can't be made until coordination issues with other projects are resolved.

A pre-filing meeting has been scheduled with FERC staff for July 3, 2012.

- **2010-07: Generator Requirements at the Transmission Interface**

FAC-001-1 and PRC-004-2.1a were adopted by the BOT on February 9, 2012. PRC-005-1.1b and FAC-003-3 were adopted by the BOT on May 9, 2012.

All standards will be prepared for filing with FERC.

Note that the schedule has been adjusted to account for the latest modifications to PRC-005 and both versions of FAC-003. Because the project was several months ahead of schedule before these modifications, the overall completion date has not changed since the original projections.

One Project Ahead of Schedule

- **2007-17 Protection System Maintenance and Testing**

A 30-day formal comment period with a 10-day concurrent successive ballot for draft standard, PRC-005-2 began on Monday, May 29 and ended on Wednesday, June 27. The weighted segment vote was 79% in favor of the standard. The team is reviewing comments and considering next steps.

Three Projects on Schedule (+/- One Month)

- **2006-06 Reliability Coordination**

First set of standards: The industry approved IRO-002, IRO-005, and IRO-014 on July 25, 2011. The BOT approved the standards at their August 4, 2011 meeting.

The current and previous coordinator met with NERC Legal and other staff on January 31, 2012 regarding the filing for these BOT approved standards in this project. Discussion is on-going regarding the timing of the filing due to coordination with the RTOSDT and OPCPSDT. Filing may be delayed until the RTOSDT set of standards is approved by the BOT and is ready to file.

Next steps are to determine when to file.

Second set of standards: The standard COM-001-2 was posted for a Successive Comment period on June 7 through July 6. The recirculation ballot of standards COM-002-3 and IRO-001-3 are being re-evaluated in conjunction with COM-003.

Ideally, the COM standards should go to the board as a package.

- **2010-17 Definition of BES Phase 2**

Phase 2 is well underway. The Planning Committee is taking the lead on investigating threshold limits while the SDT works on a guidance document based on the Phase 1 filing as

well as clarification items. The PC has been given a deadline of December 20, 2012 for the completion of its work.

FERC issued a NOPR on Phase 1 on June 21, 2012. The intent is to approve Phase 1 when the final ruling is made but a number of questions have been asked.

- **2007-02 Operating Personnel Communication Protocols**

The SDT conducted a Webinar on June 7, 2012. The Webinar featured how COM-002-3, Draft 6 (RCSDT, Project 2006-6) and COM-003-1, Draft 2 will interact. 283 stakeholders attended. The audience expressed a strong interest in the potential impacts they anticipate from COM-003-1. The SDT believes it provided a solid rationale on how these two standards will function and why they will contribute to greater reliability. The SDT's goal is to gain approval from industry in the initial ballot.

The second draft of COM-003 was posted on May 10, 2012 for a 45-day comment period and the initial ballot (which commenced on June 11, 2012). Additionally, the COM 003-01 white paper was posted on May 17.

Four Projects Behind Schedule

- **2007-09 Generator Verification:** *This project is approximately 4 months behind schedule (no significant change since last report).*

MOD-025, MOD-07 and PRC-019: The standards were posted for a 45-day formal comment period and concurrent initial ballot period from February 29 through April 16. The team met May 15-17 and developed responses to comments and revisions to the standards. The team has submitted MOD-027 for QR on June 27.

MOD-026 and PRC-024: The standards were posted for a 30 day formal comment period and successive ballot between February 29th and March 29th. The successive ballot began on March 19 and ended on March 29th. The team is responding to comments and making conforming revisions to the standards. The team met May 15-17 and developed responses to comments and revisions to the standards. The team has submitted MOD-026 for QR on June 28.

A coordination issue with RFC standards MOD-024 and MOD-025 is being addressed. RFC is withholding filing of their MOD-024 and MOD-025 standards until the continent-wide standard MOD-025 is approved. They will then evaluate whether the continent-wide standard meets their needs.

- **2007-06 System Protection Coordination:** *The project is currently two months behind schedule (no significant change since last report).*

A 45-day formal comment period with a 10-day concurrent initial ballot for draft standard, PRC-027-1 began on Monday, May 21 and ends on Thursday, July 5. A new ballot pool will be formed during the first 30 days of the comment period.

NOTE: The SC agreed the delay associated with the QR and results-based feedback is acceptable, but did not want to reforecast completion. The project will continue to be reported as behind schedule, with the understanding that this is an acceptable delay.

- **2010-05.1 Phase 1 of Protection Systems: Misoperations:** This project is currently three months late (it was erroneously reported on-schedule at the last meeting). This delay is due to extensive quality review suggestions to improve the standard being considered and implemented.

The NERC Standards Advisor is preparing the standard and all associated documents for another Quality Review submittal. The targeted timeframe for the 45-day formal comment posting with initial ballot is mid July.

- **2010-14.1 Balancing Authority Reliability-based Controls: Reserves:** This project is currently showing as 5 months late (no significant change since last report).

The four draft Standards were posted on June 4, 2012 for a 30 day formal comment period. The SDT is meeting on July 17 through July 20 to address comments received from the first posting.

One Rapid Revision Project Awaiting Filing

- **Project 2011-INT-01 Interpretation of MOD-028 for Florida Power & Light Company**

Rapid Revision Pilot

Approved at the February BoT meeting. Awaiting filing. Legal is finalizing the draft petition.

One Rapid Revision Posted for Ballot

- **Project 2010-INT-01 Interpretation of TOP-006 for FMPP**

This project was posted for a 45-day posting and Initial Ballot ending on July 30, 2012.

One Rapid Revision reviewing comments

- **Project 2011-INT-02 Interpretation of VAR-002 for Constellation Power Gen**

This Interpretation Request was approved by the SC for Rapid Revision on Jan 12, 2012. The team held two conference calls the week of April 9-13 to discuss comments received and determine the next step for the standard. The team has completed developing responses to comments and made conforming revisions to the standard for QR on April 26th. The documents were submitted to QR on April 30. The team received feedback from QR and made appropriate revisions to the documents and resubmitted them for posting on May 15. The draft standard was posted for a 30 day successive ballot / comment period on May 22. Due to a technical issue with NERC e-mail, the posting notice did not get distributed correctly. A new announcement was sent out and resulted in the posting being extended until June 27. The standard achieved a quorum and passed the successive ballot. The team has a conference call scheduled for July 2 to discuss the comments received on the ballot and prepare for the recirculation ballot.

b. Status of Outstanding Interpretations* (A. Rodriguez and V. Agnew)

Three Interpretations Awaiting Filing

- **Project 2009-22 Interpretation of COM-002-2 for the IRC**

Targeting July/August 2012 for filing.

- **Project 2009-26 Interpretation of CIP-004-1 for WECC**

Approved by stakeholders (Recirculation ballot: 80.08% approval). Adopted by BOT on May 24, 2012. Awaiting filing.

- **Project 2010-INT-05 CIP-002-1 for Duke Energy**

Approved by stakeholders (Recirculation ballot: 94.61% approval). Adopted by BOT at May 2012 meeting. Awaiting filing.

Four Interpretations in Current Development

- **Project 2012-INT-02 TPL-003-0a and TPL-004 for SPCS (In drafting)**

The interpretation response was posted on June 20 for a 30-day formal comment period ending on July 20. Next steps, the team will consider comments submitted by stakeholders and post for a 45-day comment period and initial ballot.

- **Project 2012-INT-03 CIP-007 for TECO (In drafting)**

Interpretation requests clarification on CIP-007-3, Requirement R5. Specifically, the questions relate to the use of “technical and procedural controls” in Requirement R5, and whether each sub-requirement requires both technical and procedural controls. A project team from the Interpretation Drafting Team has begun to review the request for interpretation to prepare an initial draft for formal comment.

- **Project 2012-INT-05 CIP-002-3 for OGE (awaiting formal posting)**

Assigned to CIP IDT. A project team has been formed, and the team is has prepared and submitted the interpretation for its first formal comment period. Anticipated posting for formal comment in June 2012.

The Request for Interpretation requests clarity on whether a company’s SmartGrid Advanced Meter Infrastructure (“AMI”) functionality, which may be able to disconnect more than 300 MW of load, is considered a system or facility critical to automatic load shedding under a common control system capable of shedding 300 MW or more under CIP-002-3, Requirement 1.2.5.

- **Project 2009-19 Interpretation of BAL-002-0 R4 and R5 by NWPP**

Project restarted based on BOT Action re: the scope of this interpretation and the team’s ability to rely on language other than solely the requirements. New chair Al DiCaprio assigned.

Five Interpretations in Planning Queue

- **Project 2010-INT-03 TOP-002-2a for FMPP**

Possible candidate for Rapid Revision.

- **Project 2012-INT-04 CIP-007 for ITC**

Assigned to CIP IDT, to be processed when earlier requests have been moved through the process.

- **Project 2012-INT-06 CIP-003 for Consumers Energy**

Assigned to CIP IDT, to be processed when earlier requests have been moved through the process.

- **Project 2012-INT-07 CIP-005 for AEP**

Assigned to CIP IDT, to be processed when earlier requests have been moved through the process.

- **TBD RFI received on 7/22/11 from EEI and NRECA on CIP-001-1**

In August the SC voted to move forward with this interpretation. Drafting team appointment on hold pending finalization of CAN-0016 to see if the revision of the CAN provides clarification. In September, the SC reaffirmed this decision. In October, EEI indicated their intent (in policy input to the Board of Trustees) to pursue an appeal of CAN-0016.

One other RFI received from NWPP.

c. Posting Projections Through November 2012* (A. Rodriguez and V. Agnew)



Several projects waiting prioritization are not in this posting schedule. Will be updated after decisions at this meeting.

5. Actions

a. Revised Project Schedules (A. Rodriguez and V. Agnew) **(Endorse)**

i) Project 2007-12 – Frequency Response

ii) Project 2010-13.2 Phase 2 of Relay Loadability: Generation

New schedule approved for both projects.

b. New Requests for Interpretation* (L. Hussey)

i) Request for Interpretation of PRC-006 for Consumers* **(Endorse)**

Overall this standard is predominately a system modeling standard, not a protection standard and should be separated into at least two standards.

Clarification needed: Requirement 3 provides three generic generator performance characteristics that the Planning Coordinator is required to use in their event simulations to plan a UFLS program. It does not require knowledge of the non-protection characteristics of each generator, nor does it take into consideration the actual set points of protection or control devices, which may affect the outcome in determining the UFLS plan. R3 assumes that all generators will operate within the described parameters.

The requirements of R4 (4.1-4.6) do not become effective until one year after the data required by PRC-024-1 (currently not approved) is provided. PRC-024-1 is currently written to require notification to the Planning Coordinator once it is determined that a protective device will operate in the no trip zone, however the time frame allows the initial determination to occur at up to three years after the regulatory approval of PRC-024-1. The elapsed time frame could be 4 years for the notification and if it arrives just after the five year review, the total time frame could be 9 years from the initial plan. R4 requires a dynamic simulation design assessment, using the under and over frequency trip settings (not specified as actual set points), but does not require (by name) the use of the volts per hertz trip settings. Although it may be inferred, there is no place in the standard which requires the process of incorporating the actual trip settings into creating the UFLS plan.

The PRC-006 Standard does not require the Planning Coordinator to request the actual characteristics of each generator. In PRC-006, there is no requirement to communicate any changes to the generator protective system settings, which may occur due to changes in equipment or due to a conditional assessment of the generator which requires a more conservative setting. The requirement to communicate these settings is left to the as yet unapproved PRC-024-1 standard. There is no guidance provided as far as the coordination of the settings of the generation protection versus the settings of the UFLS tripping devices nor does it specify margins or rate of change parameters. Since these functions may well be executed by different companies and by equipment with varying performance tolerances, some guidance as to the required margins (sensitivity and time) is needed to assure the proper overall functioning of the UFLS system.

Is it sufficient for the studies to model all generators within the parameters described in Attachment 1? Does this only concern modeling or is it expected that the generators actually meet the performance characteristics? It seems like a lot of the UFLS planning is done in a vacuum and with the assumption that by decreeing the expected generation performance, it will be so. A reduction in the probability of a UFLS event could be realized by the communication and incorporation of the actual protection and control set points and performance parameters, as well as the real generator limitations into the system studies.

The noted lack-of-clarity will result in the simulations, upon which the Planning Coordinator's UFLS program are based, not reflecting the actual system behavior to be expected should an underfrequency event occur. Alternatively, this lack-of-clarity could cause

the Planning Coordinator to direct that protective relaying on generators be set in a manner that may not facilitate protection of those generators.

Discussion:

Staff recommends rejecting as it is a compliance question.

Question on how to address the question.

Proposal to have staff will look at what can be done in other projects and report back to the SC at the next meeting.

Staff will assess and draft a letter.

Approved.

ii) Request for Interpretation of PER-005 for NIPSCO* **(Endorse)**

Requirement Number and Text of Requirement: Purpose, and R1 (via the NERC definition of System Operator)

To ensure that System Operators performing real-time, reliability-related tasks on the North American Bulk Electric System (BES) are competent to perform those reliability-related tasks.

Clarification needed: NIPSCO is seeking clarification for the phrase “real-time”. The NERC definition simply states “Present time as opposed to future time.” Individual entities may consider real-time as within the next 60 minutes. Others may decide that real-time is the current shift. What is the acceptable time frame for “real-time”?

An incorrect interpretation of the intent of this phrase could lead to an entity developing an incomplete task list resulting in a training program that might be found insufficient during a compliance audit.

Discussion:

Staff recommends rejecting as it is a compliance question.

Recommends putting some language in the RSAW. RSAW is not the appropriate place to respond to this question.

Looking for a definition that cannot be changed by the DT.

Real time is only in the purpose but not in the requirements.

Motion to accept the recommendation to reject based on not being a valid interpretation.

Staff will inform the requestor on available options (SAR, compliance, etc.).

Approved.

c. Project 2008-06 – Request to Defer CIP Non-binding Polls* **(Endorse)**

PROPOSAL:

To facilitate completion of the CIP Version 5 standards drafting before the FERC-directed deadline for filing, direct the Project 2008-06 SDT to postpone further development of VSLs

in the CIP Version 5 standards until after the standards have been completed and filed with FERC.

BACKGROUND:

In preparing and completing the ten different standards that are part of Project 2008-06's development of CIP Version 5, the drafting team has expended significant effort and time in preparing VSLs in parallel with development of the requirements.

On April 19, 2012, FERC issued Order No. 761, which imposes a deadline for filing the next version of the CIP Reliability Standards by March 31, 2013. The drafting team expects that it must finish its work before the end of 2012 to support meeting this deadline. As the drafting team works to complete the standards within this short timeline, postponing development of the VSLs until after completing the standards best supports the drafting team and NERC in meeting the deadline.

There are several outstanding topics related to the CIP Version 5 work that the team is focusing on to gather industry consensus, and the limited time available to the drafting team can be better spent on focusing on the requirement language of the standards. Focusing on the VSLs while also trying to meet the tight timeline to complete the CIP Version 5 requirements may threaten completion by the deadline imposed by FERC Order No. 761.

Discussion:

There is precedent; it has been done in other standards.

Doing otherwise will affect the schedule. Some may prefer seeing VSLs before approving the requirements.

Motion to authorize the SDT to defer work on VSLs but post for non-binding poll concurrent with the recirculation ballot.

Approved without abstention or opposed.

d. VRF/VSL Changes* (M. Huggins) (Endorse)

Request: Endorse proposed process and approve associated schedule for revisions to outstanding Violation Risk Factors (VRFs) and Violation Severity Levels (VSLs).

Background

NERC standards, legal, and enforcement staffs have been working in coordination with FERC staff to review a set of VRFs and VSLs assignments for possible revision or further justification. The VRFs and VSLs in need of review could have one of two origins:

- Deferred VRFs and VSLs: A couple of years ago, sub-requirement VRFs and VSLs were rolled up with main requirement VSLs, and new guidelines.*
- VSLs from "Filing 2": During the VRF and VSL roll-up process, NERC staff identified already existing VSLs that needed modification to make them conform to the roll-up or to other aspects of the FERC and NERC guidelines. NERC staff filed those corrections in two big batches were issued by FERC and NERC with respect to how VRFs and VSLs are assigned. A few orders approving standards were issued in the midst of this roll-up process, and FERC deferred approval of the VRFs and VSLs associated with those standards until the new VRF/VSL assignment process was formally approved and implemented.*

FERC has now reviewed those VRFs and VSLs, and in cases where staff caught issues that may be correctable (typos and obvious guideline violations) or that require further justification, they have identified those VRFs and VSLs to give NERC staff a chance to review them and modify them before the Commission issues a final order.

Filing 1 and Filing 2. As with Filing 1, FERC staff has reviewed Filing 2 and identified VSLs that could require additional work before an order is issued. They are giving NERC staff a chance to address those issues now.

NERC staff has proposed preliminary changes to some of the VSLs – the low-hanging fruit, or the VSLs with typos or obvious guideline violations – and have reviewed those proposed fixes with FERC staff.

The staff coordinating this project will next work with technical experts and drafting team coordinators on staff to either make changes to the VRFs and VSLs that are more technical in nature or provide further justification for those VRFs and VSLs as written.

Both VRFs and VSLs are typically posted with standards and subject to review periods and non-binding polls. Because these VRF and VSL changes are not associated with active standards projects, there is no built-in mechanism for ensuring their review by stakeholders.

According to the Standard Processes Manual, in the typical drafting of a standard,

The drafting team shall work with NERC staff in developing a set of VRFs and VSLs that meet the latest criteria established by NERC and governmental authorities. The drafting team shall document its justification for selecting each VRF and for setting each set of proposed VSLs by explaining how its proposed VRFs and VSLs meet these criteria. NERC staff is responsible for ensuring that the VRFs and VSLs proposed for stakeholder review meet these criteria.

Before the drafting team has finalized its standard, implementation plan, VRFs and VSLs, the team should seek stakeholder feedback on its preliminary draft documents.

Because there is no drafting team associated with this VRF and VSL work, but the Standard Processes Manual calls for some sort of industry review of the proposed changes or justifications before they are submitted to the Board of Trustees for approval, NERC staff proposes that the VRF and VSL changes and associated justifications are posted for a 45-day review and comment period, with a 10-day nonbinding poll. A ballot pool would be formed in the first 30 days of the posting period. Unless major modifications are required after the comment period and non-binding poll, the VRFs and VSLs would then be presented to the NERC Board of Trustees for approval and filed with FERC.

While revisions to the Standard Processes Manual propose eliminating VRFs and VSLs in favor of a Sanctions Table, we still want to take advantage of this offer from FERC to address concerns it has with filed VRFs and VSLs before an order is issued.

Proposed Schedule:

- July and August 2012: Further NERC staff review of VRFs and VSLs that are more technical in nature; finalization of proposed changes and justifications; meeting with FERC staff to review proposed changes*
- September 3-October 17, 2012: Posting for a 45-day comment period and 10-day non-binding poll*

- *October 17-November 16, 2012*: Make conforming changes to VRFs and VSLs, if necessary; prepare comment responses and post*
- *November 16-December 21, 2012: Preparation and finalization of materials for February Board of Trustees meeting*
- *February 7, 2013: Presentation to NERC Board of Trustees for approval*
- *February 15, 2013: Goal for filing with FERC*

**If significant changes to the VRFs and VSLs are required to be responsive to comments, NERC staff will arrange for a second (30-day) comment period with a 10-day non-binding poll; however, based on the changes staff is proposing so far, we do not expect that the second comment period will be necessary.*

Discussion:

Aim to have all this work done for the February BoT meeting.

Scope of changes varies from typos to inconsistency with FERC orders.

Around 60 requirements are involved and work will be done by staff (some SDTs no longer exist).

If work is not done, FERC may take action and issue an Order.

Evaluation of priorities is needed before approving.

Intent is to post a draft SAR requesting comments and posting the proposed VSLs at the same time.

Together with the P81 these are relatively large postings.

Motion to approve the approach proposed by staff and ask them to develop a schedule, consistent with other priorities, to move the project to posting as expeditiously as possible.

Approved.

- e. Proposal to Retire Standards in Response to Find Fix Track Order Paragraph 81 * (J. Tarantino)

- i) Standards Authorization Request* **(Accept)**

On March 15, 2012, the Federal Energy Regulatory Commission (FERC) issued an order on NERC's Find, Fix and Track process that stated:

"The Commission notes that NERC's FFT initiative is predicated on the view that many violations of requirements currently included in Reliability Standards pose lesser risk to the Bulk-Power System. If so, some current requirements likely provide little protection for Bulk-Power System reliability or may be redundant. The Commission is interested in obtaining views on whether such requirements could be removed from the Reliability Standards with little effect on reliability and an increase in efficiency of the ERO compliance program. If NERC believes that specific Reliability Standards or specific requirements within certain Standards should be revised or removed, we invite NERC to make specific proposals to the Commission identifying the Standards or requirements and setting forth in detail the technical basis for its belief. In addition, or in the alternative, we invite NERC, the Regional Entities and other interested entities to

propose appropriate mechanisms to identify and remove from the Commission-approved Reliability Standards unnecessary or redundant requirements. We will not impose a deadline on when these comments should be submitted, but ask that to the extent such comments are submitted NERC, the Regional Entities, and interested entities coordinate to submit their respective comments concurrently."

Consistent with P81, the problem this SAR is resolving is to identify Reliability Standards requirements that either: (a) provide little protection to the BPS; (b) are unnecessary or (c) are redundant; and, thereafter, to have NERC file the identified Reliability Standard requirements with FERC to have them removed from the FERC-approved list of Reliability Standards.

Discussion:

Collaborative work by trades, staff and regions with industry volunteers.

This is an initial phase, not the open stage will come later, including the "non-controversial standards."

Discussion on whether the SAR should contain the list of possible candidates or just define the scope.

Work has to compete with the prioritization wrt other projects in the plan.

Motion to post the draft SAR along with the list of requirements for a 30-days comment period.

Approved with no opposition or abstentions.

ii) Proposed Project Schedule* (Endorse)

Rough Proposed Process Timeline P81 SAR, Comment and Ballot, Etc.

June 27th -28th – Trades, NERC and Regions agree to proposed SAR with criteria (and partial or full list, if time.)

June 29th – Submit to NERC Staff: (1) proposed SAR (with or without partial/full list of requirements – which would include justifications) and (2) proposed names for appointed to SDT

July 10th – Trades, NERC and Regions finish work on list of requirements to be included in SAR; finalize insert

July 10th – List provided to NERC staff for insertion in draft SAR

July 11th or 12th – Brian Murphy and Joe Tarantino present P81 project to SC; SC approves SAR for posting for 30-day informal comment period; SC appoints core SDT members/sends out request for self-nomination for remainder of SDT members

July 13th – Announcement

July 16th – Core SDT begins work on the proposed list of requirements

Week July 16th – Core SDT members work with SC communication subcommittee to develop outreach plan for P81 project; creation of portal for stakeholders to make suggestions for phase two Reliability Standard requirements

Week of July 16th (2 times) – Webinar to industry

July 16th - August 15 – SAR is posted for 30-day informal comment period and request for nominations is posted

July 26th – State of Standards

August 15th – August 21st (SDT, as appropriate, support NERC staff's formatting and preparation of Reliability Standard requirements in SAR for 45-day posting)

Week of August 20th, SDT meets for two days to consider any comments from SAR posting

Week of August 20th, SDT works with NERC staff on posting of Phase One P81 requirements for formal comment and balloting; also SC has a call to authorize the posting of the paragraph 81 project for a 45-day formal comment and balloting period (last ten days), and waives the 30-day formal commenting period

August 24th – October 8th – NERC posts Phase One Paragraph 81 Reliability Standard requirements for 45-day formal comment and balloting

Week of September 24th (2 times) – Webinar to industry

October 8th – Comments and balloting are due, provided to SDT

Week of October 8th, SDT meets for two or three days to consider comments, works with NERC staff on any adjustments for next posting

October 12th – NERC posts for 10-day recirculation (assuming no Successive Comments and Balloting needed)

Week of October 22nd, SDT has conference call to consider any comments from the 10-day recirculation ballot and works with NERC staff to finalize project for BOT review

November 6th -7th presented to the BOT for approval

December – Phase One filed with FERC for approval

Discussion:

Schedule is ambitious.

Motion to defer action on schedule until SAR posted, comments received and consideration of prioritization in context of other active projects.

Approved.

- iii) Proposal for Formation of Drafting Team* **(Endorse)** (Confidential – to be sent separately)

Discussion:

Motion to endorse the appointment of the ad-hoc group as initial SDT, including the proposed chair and vice-chair, to respond to the SAR comments, with the final composition of the SDT to be modified as needed to address the technical breadth of the final SAR.

Approved without opposed or abstentions.

- f. Project 2010-13.2 Generator Relay Loadability – Request to Replace Drafting Team Member* **(Endorse)** (Confidential – to be sent separately)

Not available. Move to SCEC for resolution.

- g. Regional Standard Errata – IRO-006-WECC-1* **(Approve)**

Withdrawn

- h. Project 2007-17 Protection System Maintenance and Testing* **(Endorse)**

Request

The Protection System Maintenance and Testing SDT (PSMTSDT) plans to make one change to PRC-005-2 – Protection System Maintenance, Table-1-2, to revert one maintenance interval back to the value that was used in that table for every other posting of the standard. The PSMTSDT requests authorization to proceed to a Recirculation ballot on PRC-005-2 with this change.

Ordinarily, changes such as the one proposed by the PSMTSDT would be considered substantive and would necessitate posting of the standard for a 30-day formal comment period with a successive ballot. In this case, the team believes, and NERC staff supports, that the concept that is the subject of the change has been thoroughly vetted and no further industry review is needed.

Background

In the draft of PRC-005-2 that was posted for ballot through June 27, 2012, the second entry in Table 1-2 of PRC-005-2, addressing maintenance intervals for Communications Systems, was modified through an editing error.

In all previous postings of PRC-005-2, including the draft that originally achieved a successful ballot (April 2011), the draft that failed the Recirculation ballot (June 2011), the following draft that achieved 61% approval (August 2011), and the draft that next achieved industry approval (March 2012), this Table Entry consistently was drafted as follows:

Component Attributes: Any unmonitored communications system necessary for correct operation of protective functions, and not having all the monitoring attributes of a category below.

Maximum Maintenance Interval: 6 calendar years

Maintenance Activities: Verify that the channel meets performance criteria pertinent to the communications technology applied (e.g. signal level, reflected power, or data error rate). Verify operation of communications system inputs and outputs that are essential to proper functioning of the Protection System.

In the draft posted for ballot in May-June 2012, the maximum maintenance interval was changed for this group of activities was changed from 6 calendar years to 12 calendar years, with no change to the component attributes of maintenance activities themselves. There were no comments supporting the change to 12 years in any posting. This change was made in error. The SDT proposes to correct this maximum maintenance interval from 12 calendar years to 6 calendar years, which is consistent with similar activities for Protective Relays. As this change was made in error, and the correct text has twice before achieved industry approval (and has additionally twice BARELY failed to achieve industry approval), the drafting team believe that this is a CORRECTION, rather than a SUBSTANTIVE CHANGE, and requests approval to make the change and proceed to a Recirculation ballot.

Discussion:

Only one commenter noticed. Alternative is successive ballot instead of re-circulation.

This standard had no regulatory deadline to meet.

Motion to submit to successive ballot with the change to 6 years

Approved, with one nay.

i. Standards Authorization Request to address SW Cold Weather event* **(Accept)**

Standards EOP-001-0, TOP-002-3 and MOD-025-2, require an additional definition and clarification of reporting requirements to ensure that BAs and TOPs have a complete set of data concerning availability of generation facilities in order to effectively plan and manage the resources available to reliably meet load requirements under both normal and extreme weather conditions. In particular, further specificity is needed concerning reporting of weather-related constraints that affect the ability of a generating unit or plant in their footprint to operate safely and without damage to equipment.

Standards should also include requirements for GO/GOPs to create, maintain, implement and then monitor their plants winterization plan to ensure it can operate during cold weather events.

The goals of the SAR are:

- GO/GOPs are to define “Minimum Ambient Operating Temperature” for a generating unit including effects from wind speed.
- To require GO/GOPs to report their plant’s availability based on this Minimum Ambient Operating Temperature to the BA and TOP before the winter season and during the winter season if plant availability is impacted by expected cold weather conditions.
- GO/GOPs must ensure plant winterization plans are created, maintained, implemented and monitored to help ensure generating facilities can operate at their respective Minimum Ambient Operating Temperature.

Discussion:

- Herb reviewed efforts to address recommendations from the February 2011 report on the SW Cold Weather event and the desire to institutionalize some of those recommendations to prevent a repeat of the event.
- Question on why this initiative has to modify or create standards and not take place through alerts, guidance documents, pre-season reminders, etc.
- There might be jurisdictional issues (FERC has no purview over generation) and even confidentiality issues. The SAR and standards could be more of a performance based nature rather than as prescriptive as presented.
- There might be other ways of achieving the desired objectives.
- SC reminded that its role is not to question the SAR merits but rather whether it meets the SAR criteria. It’s up to the industry to comment on the need of the standard(s) or other technical questions.
- The SAR addresses a regional (actually 5 regions) issue but proposes a continent wide standard.

Motion to remand to the requester with the suggestion to revise the Goals section to allow to consider other alternatives to MOAT that may be identified by stakeholders and bring back the revised SAR to the SC at a future meeting.

Approved with 2 opposed.

Second day: As approved motion does not meet SPM. SARs are remanded to staff.

Reworded as:

Motion to remand to staff to work with the requester with suggestion to revise the SAR to be consistent with a results based approach and to broaden its scope with the option to bring the SAR to the SC for consideration at a future meeting.

Approved with 2 abstentions.

6. Discussion Items

a. Controls-Based Approach to Monitoring Compliance* (M. Moon)

Background

On January 7, 2011, NERC announced a preliminary set of high priority reliability issues intended to focus ERO program areas, including standards setting, compliance, and training and education.¹ Subsequent to this posting, NERC’s technical and standing committees have

reviewed the identified elements, provided suggestions and enhancements and have agreed to work with stakeholders in accepting accountability for implementing an action plan addressing these reliability issues. This document provides an action plan towards addressing these reliability issues, including priorities and milestones.

Top Priority Reliability Issues

The priority list is based partially on experience from reviewing actual system events (topics 1 to 4) and forward looking issues (topics 5 to 8). Though the reliability issues were offered as a starting point for discussion with industry experts, the standing committees believed them important enough to develop this action plan. In the next few years, it is expected that new reliability performance measures and root cause analysis methods being initiated by NERC will further reinforce the setting of reliability priorities. The goal is to develop a list of priorities to focus work in the one to three year horizon on those areas most likely to have a positive impact on bulk power system reliability. The following high level list addresses technical issues, and does not enumerate matters that should be dealt with in alternative governance and regulatory forums:

- Misoperations of relay protection and control systems*
- Human errors by field personnel*
- Ambiguous or incomplete voice communications*
- Right-of-way maintenance*
- Changing resource mix*
- Integration of new technologies*
- Preparedness for high impact, low frequency events*
- Non-traditional threats via cyber security vulnerabilities*

Internal Controls:

- Five interrelated components*
 - Control Environment*
 - Risk Assessment*
 - Control Activities*
 - Information and Communication*
 - Monitoring*
- Mechanisms*
 - Preventive*
 - Detective*
 - Corrective*

Standards:

- *Prescriptive*
 - *Discrete requirements*
 - *Zero tolerance Violations Severity Levels (VSL)*
- *Enforcement*
 - *Repeat violations*
 - *Credit for self reports*

End state:

- *Empower and encourage industry*
- *Reduce emphasis on individual instances*
- *Shift focus: continual self assessment and improvement*

Example with PRC-005:

R1. Have a program with internal controls to FFT and report and refine program

R2. Implement the program to FFT and refine the program

- *VSL:*
 - *Program is not follows*
 - *No program*
 - *Egregious or systemic problems*

Discussion:

Internal controls are a natural complement to results based standards.

Question on how this relates with the proposed elimination of VRFs and VSLs with replacement with the sanctions table.

A vision paper or whitepaper is needed to explain the concept and gameplan.

We have to get away from zero tolerance standards.

b. Reliability Standards Development Plan* (A. Mosher)

We are a bit behind schedule.

Andy R.: Assumptions were made in updating prioritization matrix particularly with the P81 and cold weather projects.

Draft Workplan 2013-2015 Rough	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Does not include Rapid Revisions and Interpretations	2012	2013	2014	2015	2016	2017											
RELIABILITY	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q4
Project 2006-06 Reliability Coordination (ACTIVE)																	
Project 2007-02 Operating Personnel Communications Protocols (ACTIVE)																	
Project 2009-01 Disturbance and Sabotage Reporting (ACTIVE)																	
Project 2007-09 Generator Verification (ACTIVE)																	
Project 2010-05.1 Phase 1 of Protection Systems: Misoperations (ACTIVE)																	
Project 2008-06 Cyber Security - Order 706 (ACTIVE)																	
Project 2007-17 Protection System Maintenance and Testing																	
Project 2007-06 System Protection Coordination (ACTIVE)																	
Project 2009-07 Reliability of Protection Systems																	
Project 2012-06 Generator Capabilities																	
Project 2012-04 Protection System Commissioning Testing																	
Project 2010-05.2 Phase 2 of Protection Systems: SPS and RAS																	
Project 2008-02 Undervoltage Load Shedding																	
Project 2010-01 Support Personnel Training																	
Project 2008-01 Voltage and Reactive Planning and Control (INFORMAL)																	
Project 2010-13.3 Phase 3 of Relay Loadability: Stable Power Swings																	
Project 2007-09 Generator Verification (ACTIVE)																	
Project 2012-01 Equipment Monitoring and Diagnostic Devices																	
Project 2010-03 Modeling Data																	
Project 2009-04 Phasor Measurements																	
Project 2009-05 Resource Adequacy Assessments																	
Project 2012-02 Physical Protection																	
Project 2010-04 Demand Data																	
Project 2006-06.2 Phase 2 of Reliability Coordination																	
Project 2010-16 Definition of System Operator																	
Project 2010-08 Functional Model Glossary Revisions																	
Project 2010-02 Connecting New Facilities to the Grid																	
Project 2012-14 Risk Analysis																	
Project 2012-07 Obsolescence Review																	
TIME SENSITIVE																	
Project 2007-12 Frequency Response (ACTIVE)																	
Project 2010-13.2 Phase 2 of Relay Loadability: Generation (ACTIVE)																	
Project 2010-14.1 Phase 1 of Balancing Authority Reliability-based Control: Reserves (ACTIVE)																	
Project 2013-1 Cold Weather Preparedness																	
PRACTICALITY																	
Project 2010-07 Generator Requirements at the Transmission Interface (COMPLETED)																	
Project 2007-03 Real-time Transmission Operations (COMPLETED)																	
Project 2012-08.1 Glossary Updates (ACTIVE)																	
Project 2010-17 Definition of BES - Phase 1 and Phase 2 (ACTIVE)																	
Project 2013-2 Paragraph 81 Revisions																	
Project 2009-02 Real-time Reliability Monitoring and Analysis Capabilities (INFORMAL)																	
Project 2009-03 Emergency Operations (INFORMAL)																	
Project 2012-15 Flow Limited Paths																	
Project 2008-12 Coordinate Interchange Standards (INFORMAL)																	
Project 2007-11 Disturbance Monitoring (INFORMAL)																	
Project 2010-14.1 Phase 2 of Balancing Authority Reliability-based Control: Time Error, AGC, and Inadvertent (INFORMAL)																	

Input on the prioritization process will be requested from the SPIG.

- c. Update on Adequate Level of Reliability Task Force (A. Mosher)

Allen reported that the ALRTF is proposing to revise the definition to focus on reliability outcomes. Tx and Gen adequacy were the most controversial items in the comments received.

There were also questions on how will the ALR be used.

- d. Update on Standards Process Input Group (A. Mosher)

SPIG will work on the RISC mandate.

- e. Subcommittee Reports

Planning and communications subcommittee SCCP

Working on plan responding to feedback received in the workshop.

Revising SCCP's scope

Starting work on developing a plan for communications associated with P81 work.

SCPS**o CEAP**

Comments just compiled, not yet reviewed.

CEAP will be initially used as a guideline. Later, after piloting, will determine whether it should go to the SPM.

Individual response to comments

After review based on comments will ask the SC to authorize another posting.

o SPM revisions

Teams set up to respond to comments

Individual response to comments

o RSAW drafting and approval

Use COM-003 as trial

Question: who approves RSAWS and should they be balloted?

To be answered by BOTCC

o Rapid Revision Procedure

Draft to be revised in 2 weeks. Target to finalize and present to SC August meeting

Flow chart of single portal process to be drafted with a limited scope to triaging requests for clarification only.

Unique request form to include RFI, RFC, compliance, Rapid revisions, etc.

o Treatment of "Orphan" Standards

SDT and QR Team to identify and bring issue to the SC for advice

o Changes to standards posted for recirc. ballot/after industry approval. (To be added to SPM changes)

Motion to allow SCPS to add language to the next SPM revision to provide authority to make errata changes to standards between the successive and recirculation ballot and standards approved by RBB before submission to BoT/filing.

Approved

o Teams set up to assess the need to revise SC's documents to reflect the SPM changes and implementation of SPIG recommendations.**7. Coordination (Review)**

- a. Coordination with Regulatory and Governmental Authorities (H. Hawkins and S. Tyrewala)

Multiple reports filed or on their way to filing.

Preparing comments on the BES NOPR. Will be circulated to the trades and regions.

- b. Coordination with Regional Managers (H. Schrayshuen)

Budget coordination progressing.

8. Informational Items (Review)

- a. Drafting Team Vacancies*
- b. Standards Committee Roster*
- c. Highlights of Parliamentary Procedure*
- d. NERC Listserv Policy*

NERC provides email lists, or "listservs," to NERC Committees, groups, and teams to facilitate sharing information about NERC activities; including balloting, committee, working group, and drafting team work, with interested parties. It is the policy of NERC that all emails sent to NERC listserv addresses be limited to topics that are directly relevant to the listserv group's assigned scope of work. NERC reserves the right to apply administrative restrictions to any listserv or its participants, without advance notice, to ensure that the resource is used in accordance with this and other NERC policies. Prohibited activities include using NERC-provided listservs for any price-fixing, division of markets, and/or other anti-competitive behavior.

Recipients and participants on NERC listservs may not utilize NERC listservs for their own private purposes. This may include lobbying for or against pending balloted standards, announcements of a personal nature, sharing of files or attachments not directly relevant to the listserv group's scope of responsibilities, and/or communication of personal views or opinions, unless those views are provided to advance the work of the listserv's group. Any offensive, abusive, or obscene language or material shall not be sent across the NERC listservs.

- Updated June 2012

Discussion:

Practice has been to allow communications only until ballot starts.

Laura H: balloting time windows are not for lobbying.

Comments received will be made available as soon as received. Software enhancements are required. Not known when will happen.

SCPS can help in a test run of the software.

9. Executive Committee Actions (Pre-authorize)

a. Project 2010-13.2 Generator Relay Loadability – Request to replace SDT member by addition of two people.

10. Adjourn

*Background materials included.

Agenda

State of Standards Webinar

July 26, 2012 | 1:00–5:00 p.m. ET

Click here for [Webinar Registration](#)

Dial-in: 1.800.408.6335 | Access Code: 4469735 | Broadcast Audio Code: 810461

Agenda

1:00–1:15 p.m.	Introductions, Opening Remarks, and Review of Antitrust Guidelines and Public Notice	Vice President of Standards and Training, Herb Schrayshuen and Standards Specialist, Mallory Huggins
1:15–2:00 p.m.	Review of Active Projects	Standards Development Advisors, Scott Barfield-McGinnis and Steve Noess
2:00–3:00 p.m.	Standard Process Input Group Recommendations and Revisions to the Standard Processes Manual	Standards Committee Chair, Allen Mosher
3:00–3:15 p.m.	Break	
3:15–3:45 p.m.	Risk Forecast for the ERO and Impact on Standards Development	Herb Schrayshuen
3:45–4:30 p.m.	Status of the Reliability Standards Development Plan	Director of Standards Development, Val Agnew
4:30–4:55 p.m.	Q&A	NERC Staff and Standards Committee Chair
4:55–5:00 p.m.	Closing Remarks	Herb Schrayshuen

From: [Lee R. Pedowicz](#)
To: [rscmembers](#); [joelc@aesl-inc.com](#); [carmen.agavriloi@ieso.ca](#); [donald.e.nelson@state.ma.us](#); [rjfalsetti@cogeco.ca](#)
Subject: FW: Reminder: NERC Industry Webinar | State of Standards | July 26, 2012
Date: Thursday, June 28, 2012 12:06:50 PM

Good afternoon.

For information.

Lee

From: NERC Standards Announcements (Do Not Reply) [mailto:NERC-StandardsAnnouncements-DoNotReply@nerc.net]
Sent: Thursday, June 28, 2012 11:10 AM
To: Wendy Kinnard
Subject: Reminder: NERC Industry Webinar | State of Standards | July 26, 2012

Industry Webinar **Reminder** State of Standards

July 26, 2012 | 1:00–5:00 p.m. ET

This State of Standards webinar will provide an overview of the recent work of NERC's Standards Department and the Standards Committee, along with information about ongoing and upcoming initiatives.

Click here for [Webinar Agenda](#)

Click here for [Webinar Registration](#)

Teleconference: 1.800.408.6335 | **Access Code:** 4469735 | **Broadcast Audio Code:** 810461

For more information or assistance, please contact [Mallory Huggins](#) (via email) or at (202) 644-8062 or [Wendy Kinnard](#) (via email) or at (404) 446-9735.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Wendy J. Kinnard
Standards Development Administrative Assistant
North American Electric Reliability Corporation
wendy.kinnard@nerc.net
(404) 446-9735 (O)
(404) 823-1366 (C)

NERC. Reliability. Accountability.

This email and any of its attachments may contain NERC proprietary information that is privileged, confidential, or subject to copyright belonging to NERC. This message and any attachments may contain confidential information protected by the attorney-client or other privilege. This email is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this email, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this email is strictly prohibited and may be unlawful. If you receive this email in error, please notify the sender immediately and permanently delete the original and any copy of this email and any printout

You have received this email because you are a registered representative in the
Registered Ballot Body.

From: [Monica Benson](#)
To: monica.benson@nerc.net
Subject: NERC Industry Webinar: State of Standards | July 26, 2012
Date: Friday, May 11, 2012 2:12:44 PM

Industry Webinar

State of Standards

July 26, 2012 | 1:00 to 5:00 p.m. ET

This State of Standards webinar will provide an overview of the recent work of NERC's Standards Department and the Standards Committee, along with information about ongoing and upcoming initiatives.

An agenda will be circulated by the end of May 2012.

Click here for: [Webinar Registration](#)

Teleconference: 800.408.6335 | **Access Code:** 4469735 | **Broadcast Audio Code:** 810461

For more information or assistance, please contact [Mallory Huggins](#) (via email) or at (202) 644-8062 or [Wendy Kinnard](#) (via email) or at (404) 446-9735.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

You are currently subscribed to nerc-info as: lpedowicz@npcc.org
To unsubscribe send a blank email to leave-1291714-325654.1ca6f85fb1574a8515cc07df72d3bfe0@listserv.nerc.com

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

2012 State of Reliability

May 2012

RELIABILITY | ACCOUNTABILITY



3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Preface

The North American Electric Reliability Corporation (NERC) has prepared the following assessment in accordance with the Energy Policy Act of 2005, in which the United States Congress directed NERC to conduct periodic assessments of the reliability and adequacy of the bulk power system of North America.^{1,2} NERC operates under similar obligations in many Canadian provinces as well as a portion of Baja California Norte, México.

NERC Mission

The North American Electric Reliability Corporation (NERC) is an international regulatory authority established to evaluate reliability of the bulk power system in North America. NERC develops and enforces Reliability Standards; assesses reliability annually via a 10-year assessment and winter and summer seasonal assessments; monitors the bulk power system; and educates, trains, and certifies industry personnel. NERC is the Electric Reliability Organization for North America, subject to oversight by the U.S. Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada.³

Figure A: NERC Regional Entities

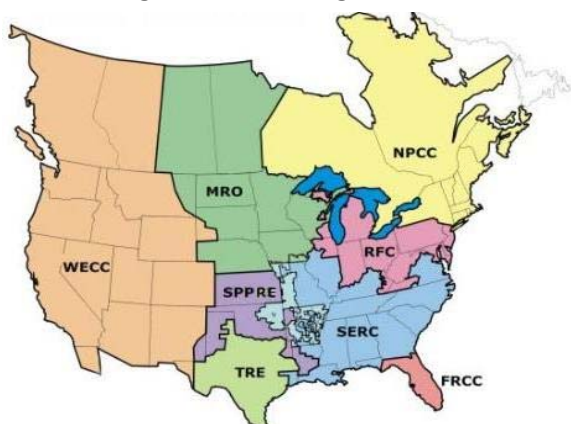


Table A: NERC Regional Entities

FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RFC	ReliabilityFirst Corporation
SERC	SERC Reliability Corporation
SPP	Southwest Power Pool Regional Entity
TRE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Note: The highlighted area between SPP and SERC denotes overlapping Regional area boundaries. For example, some load serving entities participate in one Region and their associated transmission owner/operators in another.

¹ H.R. 6 as approved by of the One Hundred Ninth Congress of the United States, the Energy Policy Act of 2005: <http://thomas.loc.gov/cgi-bin/bdquery/z?d109:HR00006:@@L&summ2=m&>.

² The NERC Rules of Procedure, Section 800, further detail the Objectives, Scope, Data and Information requirements, and Reliability Assessment Process requiring annual seasonal and long-term reliability assessments.

³ As of June 18, 2007, the U.S. Federal Energy Regulatory Commission (FERC) granted NERC the legal authority to enforce Reliability Standards with all U.S. users, owners, and operators of the bulk power system, and made compliance with those standards mandatory and enforceable. In Canada, NERC presently has memorandums of understanding in place with provincial authorities in Ontario, New Brunswick, Nova Scotia, Québec, and Saskatchewan, and with the Canadian National Energy Board. NERC standards are mandatory and enforceable in Ontario and New Brunswick as a matter of provincial law. NERC has an agreement with Manitoba Hydro making reliability standards mandatory for that entity, and Manitoba has recently adopted legislation setting out a framework for standards to become mandatory for users, owners, and operators in the province. In addition, NERC has been designated as the “electric reliability organization” under Alberta’s Transportation Regulation, and certain reliability standards have been approved in that jurisdiction; others are pending. NERC and NPCC have been recognized as standards-setting bodies by the Régie de l’énergie of Québec, and Québec has the framework in place for reliability standards to become mandatory. Nova Scotia and British Columbia also have frameworks in place for reliability standards to become mandatory and enforceable.

Table of Contents

Executive Summary.....	vi
Introduction	vi
2012 State of Reliability	vii
Future Advancements.....	ix
Report Organization.....	x
Key Findings and Conclusions	1
2011 Overall Reliability Performance	1
Key Finding 1: Bulk Power System Reliability Remains Adequate.....	1
Key Finding 2: Frequency Response is Stable with No Deterioration	5
Key Finding 3: Protection System Misoperations are a Significant Reliability Issue	6
Key Finding 4: Equipment Failure Warrants Further Analysis	10
Key Finding 5: Resource Mix Changes Necessitate New Metrics	11
Key Finding 6: More Data and Research is Needed.....	12
Daily Performance Severity Risk Assessment	13
NERC Assessment.....	13
Eastern Interconnection Assessment	18
Western Interconnection Assessment.....	20
ERCOT Interconnection Assessment.....	22
Québec Interconnection Assessment.....	24
Reliability Indicator Trends	25
Overview	25
ALR Characteristic: Boundary	28
ALR Characteristic: Contingencies	36
ALR Characteristic: Integrity	40
ALR Characteristic: Protection	42
ALR Characteristic: Adequacy	46
Disturbance Event Analysis.....	66
Introduction	66
Performance Trends	67
Conclusions	73
Transmission Availability Analysis	74

Introduction	74
Performance Analysis	74
Transmission Outage Events.....	81
Conclusions	84
Generating Availability Analysis.....	86
Introduction	86
Generation Key Performance Indicators	86
Suggestions for Improving the Quality of Data	96
Conclusion.....	97
Demand Response Availability Analysis.....	98
Introduction	98
Background	98
Summer 2011 Reporting Period Summary	100
Demand Response Enrollment	100
Demand Response Program Categories	104
Reliability Event Details	108
Ancillary Services	113
Conclusions	114
2011 Post Summer Assessment.....	115
Operational Highlights	115
Demand Response Contributed to Improved Reliability.....	118
Transmission Constraints.....	121
Protection and Control Misoperations.....	122
MISO.....	123
ISO-NE	123
NYISO	124
SASKPOWER	124
SERC	124
SPP	125
WECC.....	125
Abbreviations Used in This Report	126
Contributions	130

Acknowledgements	130
NERC Industry Groups.....	130
Regional Entity Staff.....	131
NERC Staff	132

Notice

Many datasets and analyses conducted in the *2012 State of Reliability* report are still in an early stage. The defined characteristics of an Adequate Level of Reliability are currently being reviewed and refined. This report presents metrics and trends derived from the data available at the time of publication and may be modified pending further review and analysis.

Executive Summary

Introduction

The North American Electric Reliability Corporation (NERC) *2012 State of Reliability* report represents NERC's independent view of ongoing bulk power system reliability trends to objectively analyze the state of reliability based on metric information and provide an integrated view of reliability performance. The key findings and recommendations serve as technical input to NERC's Reliability Standards and project prioritization, compliance process improvement, event analysis, reliability assessment, and critical infrastructure protection. This analysis of bulk power system performance not only provides an industry reference for historical bulk power system reliability, it also offers analytical insights towards industry action, and enables the discovery and prioritization of specific actionable risk control steps.

The 2012 report builds on the 2011 foundational report, *2011 Risk Assessment of Reliability Performance*.¹ It was prepared by the NERC staff and NERC Performance Analysis Subcommittee² (PAS) under the direction of the Operating and Planning Committees. Further, this year's report was developed in collaboration with many technical groups,³ including the:

- Operating Committee (OC):
 - Resources Subcommittee (RS)
 - Frequency Working Group (FWG)
 - Event Analysis Working Group (EAWG)/Event Analysis Subcommittee (EAS)
 - Operating Reliability Subcommittee (ORS)
- Planning Committee (PC)
 - Reliability Assessment Subcommittee (RAS)
 - System Protection and Control Subcommittee (SPCS)
 - Transmission Availability Data System Working Group (TADSWG)
 - Generating Availability Data System Working Group (GADSWG)
 - Demand Response Availability Data System Working Group (DADSWG)

Since its first 2009 annual reliability metrics report,⁴ the PAS (formerly the Reliability Metrics Working Group⁵) has advanced data collection and trend analysis for all 18 reliability indicators⁶ through NERC's voluntary or mandatory data requests. In this year's report, the metric assessment also includes frequency response, system voltage performance, and protection system misoperations.

¹ http://www.nerc.com/files/2011_RARPR_FINAL.pdf

² <http://www.nerc.com/filez/pas.html>

³ <http://www.nerc.com/page.php?cid=1|117>

⁴ http://www.nerc.com/files/RMWG_Metric_Report-09-08-09.pdf

⁵ <http://www.nerc.com/filez/rmwg.html>

⁶ http://www.nerc.com/filez/Approved_Metrics.html

2012 State of Reliability

Bulk power system reliability is stable since the metrics show no significant upward or downward trends for the period 2008 to 2011. The severity risk index and 18 metrics that measure characteristics of adequate level of reliability (ALR) indicate the bulk power system is within the defined acceptable ALR conditions. The system achieves an ALR when it possesses the following six characteristics:⁷

1. Controlled to stay within acceptable limits during normal conditions;
2. Perform acceptably after credible contingencies;
3. Limit the impact and scope of instability and cascading outages when they occur;
4. Facilities are protected from unacceptable damage by operating them within facility ratings;
5. Integrity can be restored promptly if it is lost; and
6. Have the ability to supply the aggregate electric power and energy requirements of the electricity consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components.

An improved ALR definition is being developed.⁸ Its trend analysis and risk control measures will continue to evolve as an understanding of what factors contribute to, or indicate the level of, reliability. Also the cause-effect model will be expanded with deeper analysis of initiating events and their impact.

Bulk Power System Reliability Remains Adequate

From 2008 to 2011, excluding the events caused by factors other than the performance of the transmission system (e.g., weather initiated events), the number of bulk power system transmission-related events resulting in loss of firm load has been relatively flat, with an average of between eight to 10 events per year. The 2011 daily severity risk index (SRI)⁹ value, measuring events resulting in the loss of transmission, generation, and load showed the majority of the year's performance was improved compared to 2008, 2009 and 2010. However, when weather initiated events are included, 2011 had more "high stress days" (eight days with an SRI greater than 5.0) than had been experienced in prior years (two to five days with an SRI higher than 5.0).

Transmission Availability Performance is High

As shown from the transmission performance data, availability of the bulk transmission system continues to remain high with no statistically significant change from 2008 to 2011. The AC circuit availability is above 98 percent, and the transformer availability is above 96 percent for both 2010 and 2011.

⁷ <http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf>

⁸ The draft of a revised ALR definition, including socio-economic impact consideration, can be viewed at: <http://www.nerc.com/filez/alrtf.html>.

⁹ http://www.nerc.com/docs/pc/rmwg/pas/index_team/SRI_Equation_Refinement_May6_2011.pdf

On average, roughly two percent of the events per year (92 events out of 4,185 total events) contain between three and 14 momentary and sustained automatic outages. Some of these events are beyond the NERC TPL (transmission planning) Reliability Standards,¹⁰ including the Category B events commonly used in planning and daily operations. Further, additional analysis is needed to improve the understanding of the assumptions used for contingency criteria which form the basis for system planning adequacy studies and daily operations. A recent survey of 133 of these events (from 2008 to 2011) shows that over 60 percent of the returned survey responses involve abnormal clearing of one or more of the element outages. Nearly half of them involved element outages initiated by protection system misoperations. Industry efforts¹¹ are underway to understand the risks from protection system misoperations and to develop effective risk controls needed to reduce future misoperation occurrences.¹²

Generating Unit Availability Supports Adequate Reserve Margin

Based on the 2011 generating unit availability data, generating units continue to be sufficiently reliable to support adequate electric capacity. Individual generating equipment outages did not have any significant impact on the reliability of the bulk power system. Transmission and weather events (tornadoes, lightning, and ice storms) resulted in more multiple unit forced outage trips, hours of down time, and power production lost during 2008 to 2011 than individual unit equipment specific outages.

New generating units are replacing older ones to maintain power production capability to meet load, increase the efficiency of the existing fleet and to address environmental rules. Most new generating units are gas-fired, though new coal-fired unit capacities are also being added to the system.

Resource Mix Changes Necessitate New Metrics

Wind generation has grown in many parts of the bulk power system, and this trend is expected to continue.¹³ The variable and uncertain nature of wind generation complicates the inclusion of wind resources in the calculation of reserve margins. Improvements in wind forecasting are necessary to assure that adequate resources are in place in operational horizon.

As recommended in NERC's *Accommodating High Levels of Variable Generation* report,¹⁴ and further developed in the follow-on study *Flexibility Requirements and Potential Metrics for Variable Generations: Implications for System Planning Studies*,¹⁵ reliability metrics are needed to measure system flexibility requirements to account for large-scale wind generation integration. Considerations should include ramping requirements, minimum generation levels, required shorter scheduling intervals, and transmission interconnections. Additional data is needed to support the system flexibility and resource adequacy assessment.

¹⁰ <http://www.nerc.com/files/TPL-002-0b.pdf>

¹¹ <http://www.nerc.com/filez/psmtf.html>

¹² <http://www.nerc.com/filez/psmtf.html>

¹³ http://www.nerc.com/files/2011%20LTRA_Final.pdf

¹⁴ [Special Report: Accommodating High Levels of Variable Generation](#)

¹⁵ http://www.nerc.com/files/IVGTF_Task_1_4_Final.pdf

As the role of demand response increases, both NERC and stakeholders need to analyze its performance to measure its benefits and impacts on reliability. In 2011, NERC collected reliability related demand response information across 133 entities within North America. This includes enrollment and actual performance data from April 1 to September 30, 2011. There were 664 deployments during this period with July (247 events, 16,283 MW, 70 percent realization rate¹⁶) and August (153 deployments, 10,896 MW, 77 percent realization rate) being the most active.

Future Advancements

The 2012 State of Reliability report marks a vital step towards an overall view of the risk to bulk power system reliability. The goal is to quantify performance, highlight areas for improvement as well as reinforce and measure success in controlling these risks. To address this objective, a number of activities are ongoing:

1. In 2011, the Sandia National Laboratories (SNL) and U.S. Energy Information Administration (EIA) both provided technical support to identify and monitor areas for improving the value of indices such as the SRI. Based on their recommendations,^{17,18} the PAS will consider applying risk cluster and other statistical analysis applications to link the reliability data used in the event-driven index (EDI),¹⁹ standards-driven index (SDI)²⁰ and condition-driven index (CDI) to identify significant initiating events and measure their reliability impact. The resulting model could be used to characterize and monitor the state of bulk power system reliability, and cause-effect relationships may emerge.
2. In March 2012, the EDI measure was endorsed by the Operating and Planning Committees. The SDI measure was endorsed by the Compliance and Certification Committee. The PAS's index team is finalizing the details of the CDI measure. The trend analysis of these three indices, measuring different reliability aspects, will be included in future reliability reports. Further, under the direction of the Critical Infrastructure Protection Committee (CIPC), the PAS is collaborating with the Bulk Electric System (BES) Security Metrics Working Group to develop bulk electric system security performance metrics.

The PAS recognizes the importance of detecting system reliability risks promptly to ensure risks to reliability are identified and actionable steps can be deliberated upon by industry to address these risks. However, many datasets and performance analyses conducted in this report are still in an early stage. The PAS expects that as it continues its performance analysis and measurement of reliability risks, limitations and enhancements of data and metrics will be identified, which will require review and modification of the reported data. These enhancements will be captured in future reports. At the present time, the defined

¹⁶ Realization Rate is defined as Actual MW achieved for the event divided by MW requested for the event.

¹⁷ http://www.nerc.com/docs/pc/rmwg/pas/Mar_2012_OCPC/Final_Memo_Sandia.pdf

¹⁸ http://www.nerc.com/docs/pc/tadswg/07_agenda%20item%20EIA%20Memo.pdf

¹⁹ http://www.nerc.com/docs/pc/rmwg/pas/Mar_2012_OCPC/EDI_Whitepaper.pdf

²⁰ http://www.nerc.com/docs/pc/rmwg/Integrated_Bulk_Power_System_Risk_Assessment_Concepts_Final.pdf

characteristics of ALR are being reviewed and refined. Once the enhanced definition becomes final, the PAS will evaluate the current ALR metrics and modify them accordingly.

Report Organization

Following the key findings and conclusions chapter, the second chapter details the severity risk index trend analysis. The third chapter presents assessments for eighteen reliability metrics. The fourth chapter provides a brief summary of reported disturbances based on event categories described in the enhanced event analysis field test process document.²¹ The fifth chapter outlines transmission system performance results that the TADSWG has endorsed using the four-year history of TADS data. Reviewed by the GADSWG, the sixth chapter provides an overview of generating availability trends for over 70 percent of generators in North America. The seventh chapter is an overview of 2011 reliability related demand response information summarized by the DADSWG. It includes enrollment and actual performance data from April 1, to September 30, 2011. The final chapter highlights 2011 summer operations.

²¹ http://www.nerc.com/files/ERO_Event_Analysis_Process_Document_Version_1_Feb_2012.pdf

Key Findings and Conclusions

2011 Overall Reliability Performance

Bulk power system reliability is stable since the metrics show no significant upward or downward trends for the period 2008 to 2011. The SRI and 18 metrics that measure characteristics of ALR indicate the bulk power system is within the defined acceptable ALR conditions. Based on the data and analysis in the later chapters of this report, the following six key findings were identified:

1. Bulk power system reliability remains adequate.
2. Frequency response is stable with no deterioration.
3. Protection system misoperations are a significant reliability issue.
4. Equipment failure warrants further analysis.
5. Resource mix changes necessitate new metrics.
6. More data and research is needed.

Key Finding 1: Bulk Power System Reliability Remains Adequate

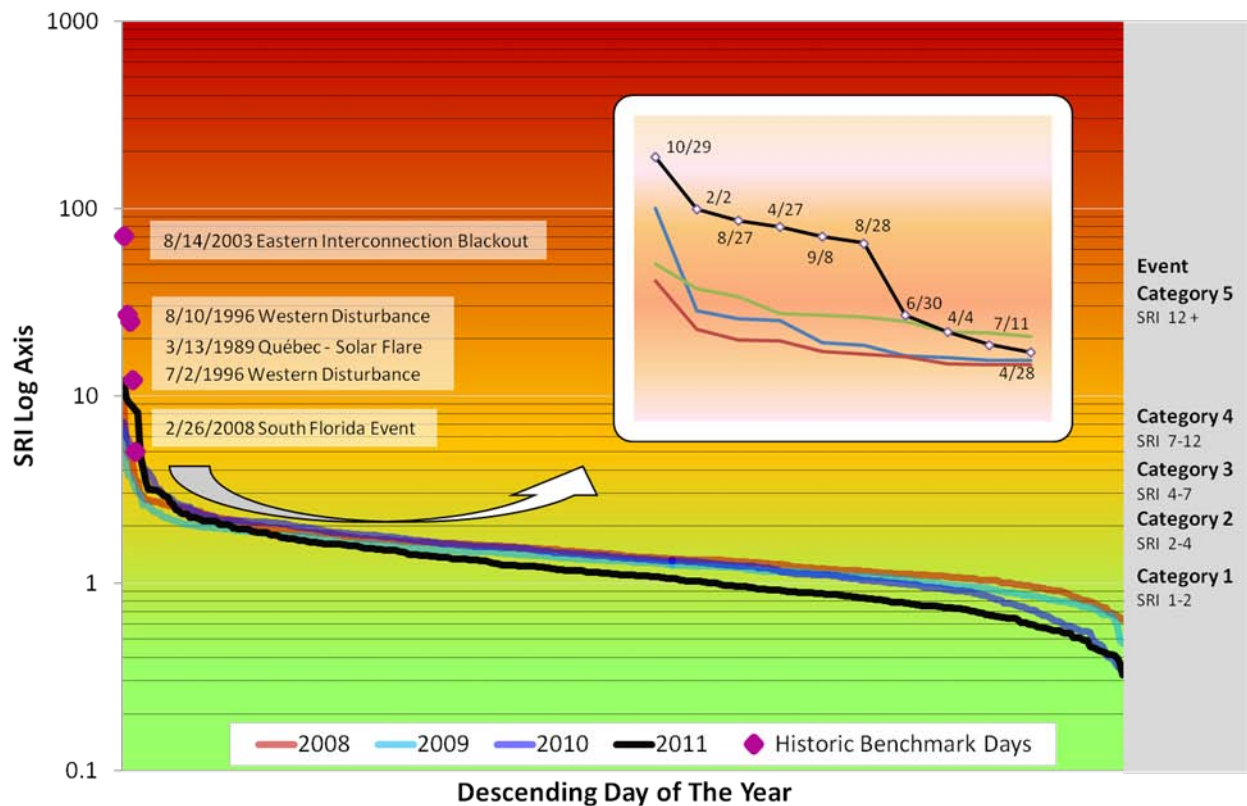
Daily Performance Severity Risk Assessment

Bulk power system reliability remains adequate. Figure 1 captures the daily SRI²² from 2008 to 2011 including the historic significant events. Based on the SRI values, routine daily performance is consistent across all four years. However, including weather initiated events, 2011 had more “high stress days” (SRI greater than 5.0) with eight days, compared to prior years with averages between two and five days. For SRI values less than 5.0, 2011 had more improved performance days than previous years.

The SRI is a daily, blended metric where transmission loss, generation loss, and load loss events are aggregated into a single value that represents the performance of the system. Accumulated over a year, these daily performance measurements are sorted in descending order to evaluate the year-on-year performance of the system. Since there is significant disparity between normal days and events in terms of SRI values, the curve is depicted using a logarithmic scale.

²² http://www.nerc.com/docs/pc/rmwg/pas/index_team/SRI_Equation_Refinement_May6_2011.pdf

Figure 1: NERC Annual Daily Severity Risk Index (SRI) Sorted Descending with Historic Benchmark Days



As the year-on-year performance in Figure 1 is evaluated, certain portions of the graph become relevant for specific analysis. First, the left side, where the system has been substantially stressed, should be considered in the context of the days which were noteworthy. Next, the slope of the central part of the graph may reveal year-on-year changes in performance for the majority of the days of the year and demonstrate routine system resilience. Finally, the right portion of the curve may also provide useful information about how many best days occurred during the year, contrasted to prior years.

As mentioned earlier, 2011 had more “high stress days” than had been experienced in prior years. However, further examination of the central part of the graph shows that 2011 had improving “day-to-day” performance demonstrated by the more pronounced downward slope than occurred in previous years. Finally examination of the right portion of the curve indicates 2011 shows improvement over prior years. Thus, while more serious days may have occurred in prior years, the majority of the 2011’s performance was improved compared to previous years.

Table 1 lists the highest 10 SRI event dates in 2011. Every event that occurred on the date had DOE OE-417²³ filed. Nine of these 10 events were influenced by weather. The three events that

²³ https://www.oe.netl.doe.gov/docs/OE417_submission_instructions.pdf

required event analysis were the February 2 cold snap event, June 30 disturbance event, and September 8 Arizona-Southern California outage event.

Table 1: 2011 NERC Top 10 SRI Event Days' General Indicators					
Date	NERC SRI Score	Weather Influenced?	Event Analysis?	Highest Event Category ²⁴ on Date	OE-417 ²⁵ Filed?
10/29	12.08	✓		3	✓
2/2	9.70	✓*	✓	4	✓
8/27	9.19	✓		Less than 2	✓
4/27	8.90	✓		3	✓
9/8	8.46		✓	4	✓
8/28	8.16	✓		Less than 2	✓
6/30	4.85	✓*	✓	2	✓
4/4	4.10	✓		Less than 2	✓
7/11	3.51	✓		Less than 2	✓
4/28	3.18	✓		Less than 2	✓

* Indicates partial influence

Transmission System Availability and Metrics Have No Significant Change

Reliability of the transmission system continues to remain high with no statistically significant change in performance from 2008 to 2011, as evidenced in the Reliability Indicator Trends section of this report. AC circuit availability is above 98 percent, and transformer availability is above 96 percent for both 2010 and 2011. These are the first two years for which planned outage data (an integral component in total availability) is available. Planned outages for maintenance and construction have a long-term positive impact on transmission system reliability. AC circuit and transformer unavailability was well below five percent, as shown in Figure 2. The unavailability due to automatic sustained outages was less than one percent. These relative percentages provide an indication of the overall availability of the transmission system operated at 200 kV and above.

In addition to AC circuit and transformer availability and unavailability, the performance indicators include four transmission availability related metrics which are used to measure outage rates for areas deemed important to reliability. Each of the four metrics is statistically analyzed to determine improvement or deterioration.

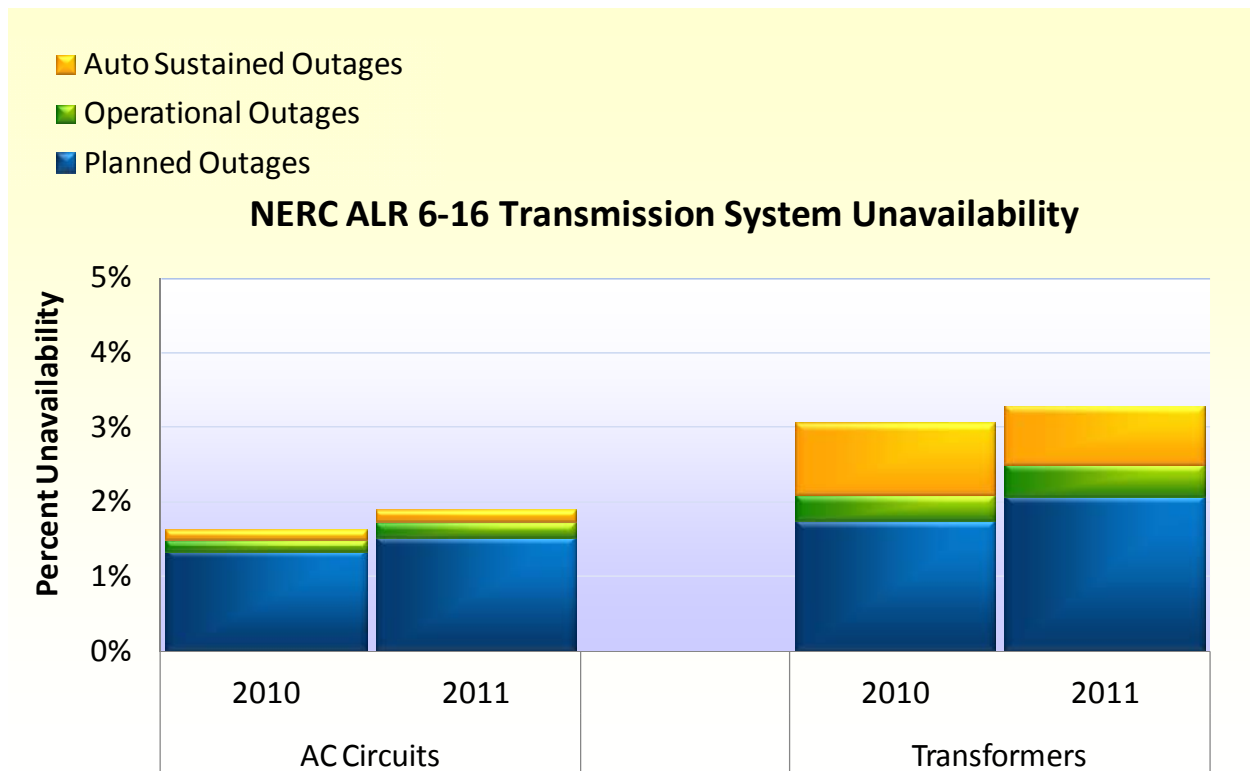
²⁴ http://www.nerc.com/files/ERO_Event_Analysis_Process_Document_Version_1_Feb_2012.pdf

²⁵ https://www.oe.netl.doe.gov/docs/OE417_submission_instructions.pdf

The four metrics are:

- ALR 6-11: Automatic AC transmission outages initiated by failed protection system equipment
- ALR 6-12: Automatic AC transmission outages initiated by human error
- ALR 6-13: Automatic AC transmission outages initiated by failed AC substation equipment, and
- ALR 6-14: Automatic AC Transmission Outages initiated by failed AC circuit equipment.

Figure 2: NERC Transmission System Unavailability by Outage Type (2010- 2011)



Based on the study framework recommended by the United States Department of Energy's Energy Information Administration (EIA),²⁶ the statistical significance of four transmission reliability metrics were tested from year-to-year. Results indicate there are no statistically significant changes in performance of these metrics from 2008 to 2011. Assumptions used and detailed analyses are included in the Transmission Availability Analysis and Reliability Indicator Trends chapters, respectively.

²⁶ http://www.nerc.com/docs/pc/tadswg/07_agenda%20item%20EIA%20Memo.pdf

Generating Unit Availability Supports Adequate Reserve Margin

Based on the 2011 generating unit availability data, generating units continue to be sufficiently reliable to support adequate electric capacity. Individual generating equipment outages did not have any significant impact on bulk power system reliability. Transmission and weather events (tornadoes, lightning, and ice storms) resulted in more multiple unit forced outage trips, hours of down time, and power production lost during 2008 to 2011 than individual unit equipment specific outages.

New generating units are replacing older ones to maintain power production capability to meet load, increase the efficiency of the existing fleet and to address environmental rules. Most new generating units are gas-fired, though new coal-fired capacity is also being added to the system.

Load Loss Events Up from Prior Years

During 2011, the SRI evidenced slightly higher occurrence of load loss events. Further analysis of this data indicates that weather events including tornadoes, hurricanes, ice storms, extreme cold and extreme heat were the predominant causes. Continued investigation into these occurrences is recommended, including post-event review. Further, load loss reporting should be refined to distinguish differences between consequential²⁷ and non-consequential load loss, and include identifications of initiating events.

Key Finding 2: Frequency Response is Stable with No Deterioration

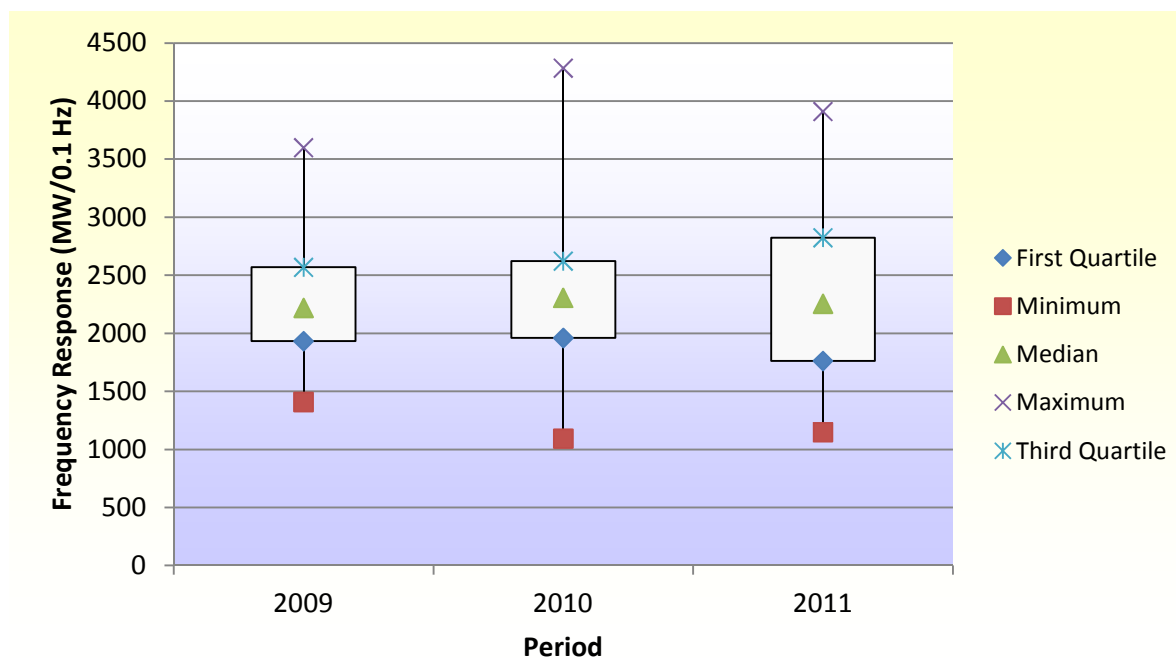
Based on the frequency event data collected from 2009 to 2011, the Frequency Response performance of the Eastern Interconnection (EI) appears relatively stable, as shown in Figure 3. When comparing 2011 performance to 2009 and 2010, the inter-quartile range (the difference between the first and third quartiles) has a greater value. However, the median performance across the time period is consistent. As evidenced in the Reliability Indicator Trends chapter of this report, the wider inter-quartile range is due to more and smaller frequency events captured in 2011. These results are not attributable to deterioration. These events have less Frequency Response due to dead band settings and fewer governors triggered for smaller frequency deviations. Notably, with the more consistent and streamlined data collection procedures developed in 2011, smaller events in EI were captured.²⁸

More data is still needed to apply statistical significance tests and calculate a confidence interval to establish a trend. Also additional analysis on time of year, load levels, generation on-line, and response withdrawal should be considered when interpreting the trend.

Similarly, the Western Interconnection (WI), ERCOT Interconnection, and Québec Interconnection (QI) have shown no changes in Frequency Response performance.

²⁷ http://www.nerc.com/files/Glossary_of_Terms.pdf

²⁸ A historic perspective of the frequency response trend calculations in the Eastern Interconnection can be found in http://web.eecs.utk.edu/courses/spring2012/ece522/D2010_beta.pdf and http://www.truc.org/files/2006/FDA_2006_010.pdf.

Figure 3: Box Plot Analysis for 2009 to 2011 Eastern Interconnection Data

Key Finding 3: Protection System Misoperations are a Significant Reliability Issue

Misoperations Identified in Key Transmission Related Events

Nine transmission related events resulted in loss of firm load in 2011. Events caused by factors other than transmission system performance were not included (such as the cold snap event, tornadoes, etc.). These nine events were due to equipment failures, misoperations, and/or human error. Table 2 summarizes the contribution of their leading causes to these nine events. Definitions of these cause codes are in Table 3.

Protection system misoperations remain a significant reliability issue. As described in the 2011 Post Summer Assessment chapter, on June 6, in the El Paso area of Texas local transmission system protective relaying issues contributed to a service interruption to about 162,000 customers and the loss of 106 MW of generation. On July 13, transmission system protective relaying issues resulted in a loss of 599 MW of generation and the interruption of service to approximately 93,000 customers in the Pueblo area of Colorado. In fact, every major system disturbance since the 1965 Northeast Blackout has been caused or exacerbated by protection system performance ranging from incorrect relay settings to communication failures.²⁹

²⁹ <http://www.nerc.com/docs/docs/blackout/BlackoutTable.pdf>; <http://www.nerc.com/docs/docs/blackout/section5.pdf>

Table 2: Transmission Related Events Resulting in Load Loss from ALR1-4							
Date	Event Category	Generation Loss (MW)	Transmission Loss	Load Loss (MW)	Equipment Failure	Protection System Misoperation	Human Error
1/13/2011	2	0	3 lines	135	✓		
3/27/2011	1	260	13 lines	295	✓		✓
4/25/2011	2	0	5 lines 1 transformer	140		✓	
5/10/2011	2	300	10 lines	462	✓		
6/6/2011	2	106	4 lines	450		✓	
6/30/2011	2	1	3 transformers	797	✓		
7/13/2011	2	599	14 lines 1 back-to-back converter 2 transformers	665	✓	✓	✓
7/22/2011	N/A	0	1 line	206	✓		
9/8/2011 ³⁰	4	*	*	*	*	*	*

NERC is in the process of revising a number of Reliability Standards involving protection system misoperations.³¹ To increase awareness and transparency, NERC has and will continue to conduct industry webinars³² on protection systems and document success stories on how Generator Owners/Transmission Owners are achieving high protection system performance. The quarterly protection system misoperation trending by NERC and the Regional Entities can be viewed on NERC's website.³³

³⁰The 9/8/2011 event analysis is currently underway. On September 8, WECC experienced a widespread power outage affecting portions of Arizona, southern California, and northern Baja California. According to the Department of Energy Form OE-417 report filed for the event, service to approximately 2.8 million customers was interrupted, and seven thousand megawatts of generation tripped offline. The final report regarding this event is not presently available, but it is expected that it will be publicly released in a joint NERC/FERC event analysis report.

³¹http://www.nerc.com/filez/standards/Project2010-05_Protection_System_Misoperations.html

³²http://www.nerc.com/files/misoperations_webinar_master_deck_final.pdf

³³<http://www.nerc.com/page.php?cid=4|331|400>

Misoperations Found in Transmission Common and Dependent Mode Outages

On a NERC-wide basis as shown in Figure 4, an average of two percent of events per year (92 out of 4,185 total events³⁴) contain between three and 14 momentary and sustained automatic element outages, some of which meet the TPL (transmission planning) standards requirements,³⁵ while other events went beyond the Category B events commonly used in planning and daily operations. Additional analysis is needed to improve the understanding of the assumptions used for contingency criteria which form the basis for system planning adequacy studies and daily operations.

A recent survey of 133 of these events (from 2008 to 2011), shows more than a majority of these events (63 percent) includes abnormal clearing of one or more of the element outages, as shown in Table 4.³⁶ A near majority (47 percent) of these events involved element outages initiated by protection system misoperations.

To understand root causes and develop reduction solutions, NERC has collected nearly a year of protection system misoperations data using a uniform misoperations reporting template across the eight Regional Entities. To increase awareness and transparency, the misoperations data aggregated at regional and NERC levels is made available on the public website.³⁷ Focus areas include training on digital relay specifications and settings.

Table 3: Common Cause Codes

Protection System Misoperations

Events caused by relay and/or control initiated operations when not desired or the failure to operate when desired. This category also includes incorrect relay or control settings that do not coordinate with other protective devices.

Equipment Failure

Events caused by the failure of equipment. Use this code only when the equipment failed even though it was operated within design specifications. The failed equipment could be (i) a component of an Element (such as a failed insulator), or (ii) part of an AC Substation (such as a failed circuit breaker).

Human Error

Events caused by any incorrect action traceable to employees and/or contractors for companies operating, maintaining, and/or providing assistance to the Generator Owner/Transmission Owner are reported in this category. Also, any human failure or interpretation of normal industry practices, operating procedures, and guidelines that cause an outage are reported in this category.

³⁴ The detailed 2008-2011 outage information is available in the Transmission Availability Analysis chapter of this report.

³⁵ <http://www.nerc.com/files/TPL-002-0b.pdf>

³⁶ Event Type 60 Breaker Failure: one or more automatic outages with delayed fault clearing due to a 200 kV and above circuit breaker being stuck, slow to open or failure to interrupt current.

Event Type 61 Dependability (failure to operate): one or more automatic outages with delayed fault clearing due to failure of a single protection system (primary or secondary backup) under either of these conditions:

- Failure to initiate the isolation of a faulted power system Element as designed, or within its designed operating time, or
- In the absence of a fault, failure to operate as intended within its designed operating time.

Event Type 62 Security (unintended operation): one or more automatic outages caused by improper operation (e.g. overtrip) of a protection system resulting in isolating one or more TADS elements it is not intended to isolate, either during a fault or in the absence of a fault.

Event Type 90 Automatic Outage(s): event with abnormal clearing not covered by Event Type 60 through 62.

³⁷ <http://www.nerc.com/page.php?cid=4|331|400>

A deeper investigation into the root causes of protection system misoperations which contribute to dependent and common mode events is a high priority. As announced at the March 2012 NERC Planning Committee meeting, a Protection System Misoperation Task Force (PSMTF) has been formed to analyze misoperations.

Figure 4: TO Reported Outages per TADS Event (2008-2011)

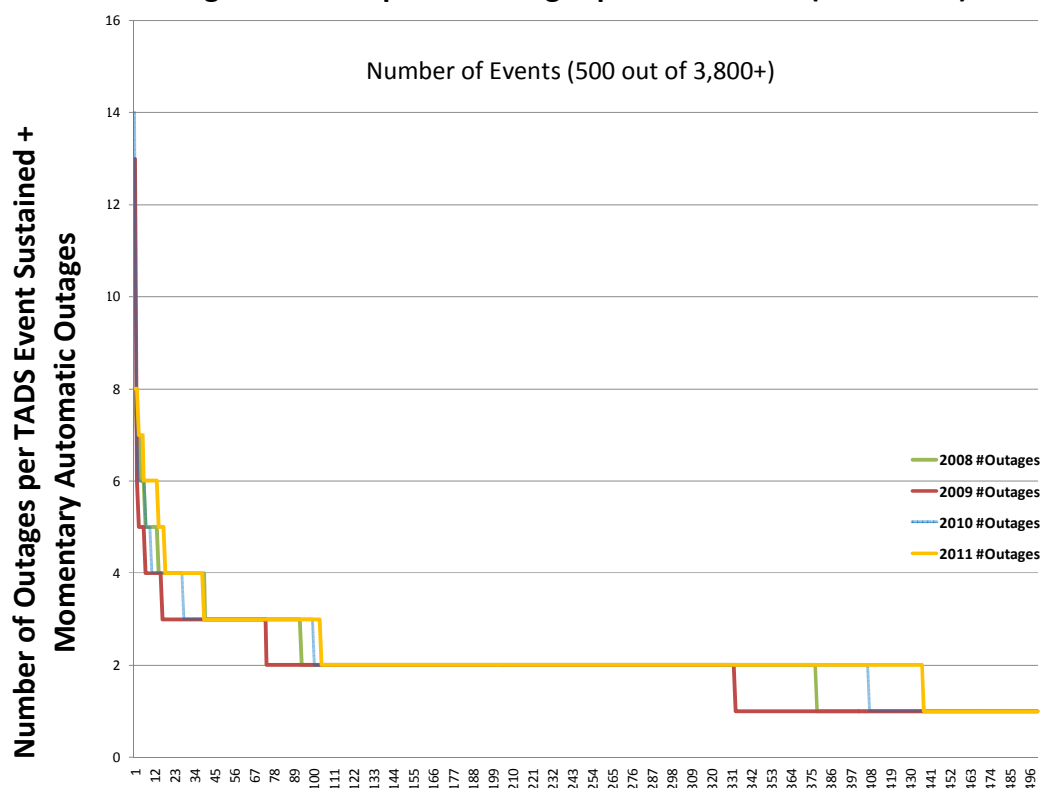


Table 4: Survey Summary - Three Outages or More per TADS Event

Description	TADS Events	Percent
Total Common and Dependent mode events with 3 or more circuit outages	369	100 percent
Survey Responses (Number of Events)	133	36 percent or (133 of 369)
Normal Clearing Events	49	37 percent or (49 of 133)
Abnormal Clearing Events (TADS Event Types 60+61+62+90)	84	63 percent or (84 of 133)
Events with Misoperation Contribution (TADS Event Types 61+62)	63	47 percent or (63 of 133)

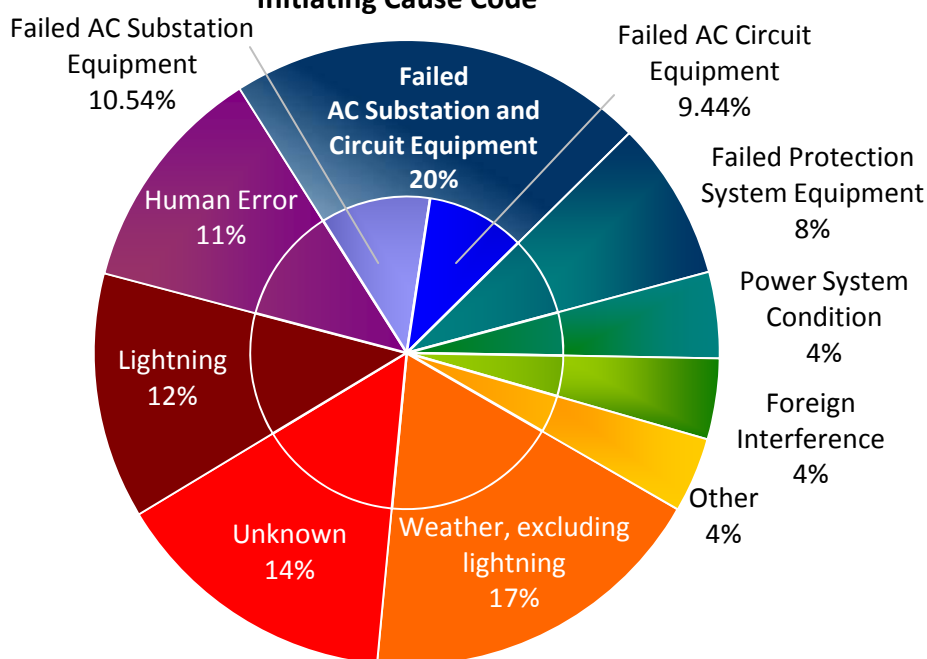
Key Finding 4: Equipment Failure Warrants Further Analysis

As described in Table 2 supporting the discussion of Key Finding 3, equipment failure was involved in six events out of a total of nine transmission related events resulting in loss of firm load. Excluding weather and unknown causes, the transmission availability performance data also indicates equipment failure is one significant contributor to sustained automatic outages, as shown in Figure 5. As detailed in the Transmission Availability Analysis chapter of this report, from 2008 to 2011, nearly 20 percent of automatic sustained outages were initiated by either failed AC substation equipment or failed AC circuit equipment.

The following recommendations will support further risk control analysis:

1. Additional data is needed to investigate and analyze equipment failure. For this purpose, secondary cause codes to gather more insights into each sustained outage event could be developed. This information will provide specific causal factors and identify initiating events, which could support the development of a statistical cause-effect model.
2. A small subject-matter-expert technical group could be formed to further understand the problem of substation and AC circuit equipment failures and provide risk control solutions to improve performance.

Figure 5: NERC 2008 – 2011 AC Circuit Top Ten Sustained Automatic Outage Occurrences by Initiating Cause Code³⁸



³⁸ Percent is out of total number of outages. Remaining 7.40 percent include: Fire, Contamination, Vegetation, etc.

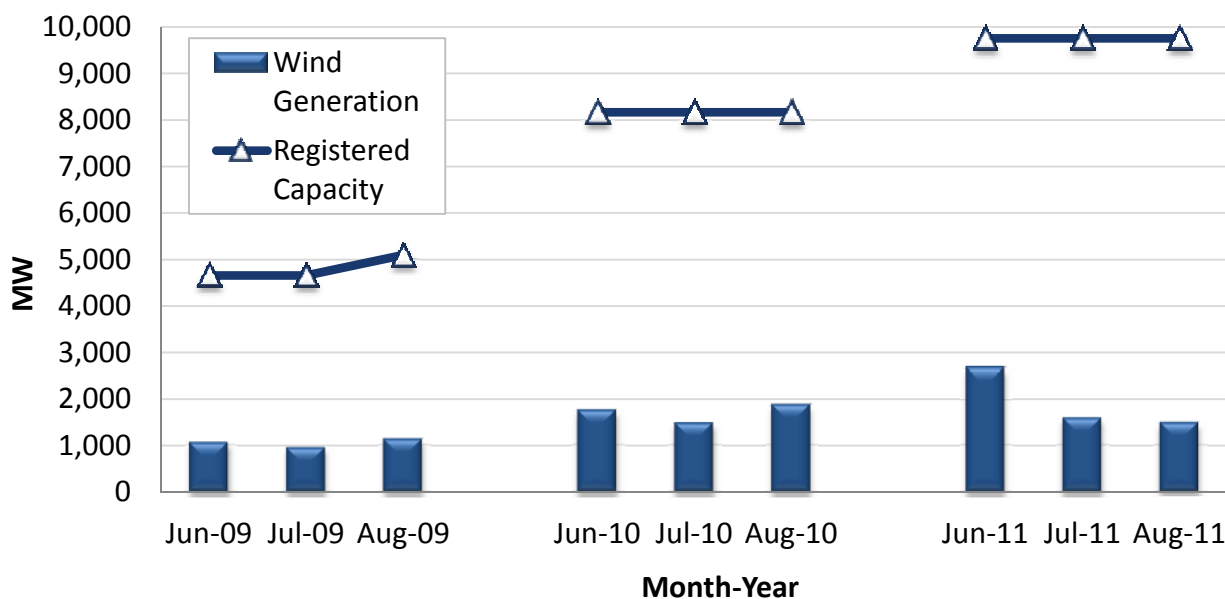
Key Finding 5: Resource Mix Changes Necessitate New Metrics

Resources such as wind generation and demand response are the non-traditional resources that perform differently than conventional generators. New metrics should be developed in order to determine what, if any, impact of these differences have on reliability.

Influence of Wind on Reliability

Wind nameplate capacity has grown in many parts of the bulk power system consistently for past summers. This trend will increase due to state/provincial renewable portfolio energy mandates and potential future Federal mandates.³⁹ The variable and uncertain nature of wind generation complicates the inclusion of wind resources in the calculation of reserve margins. Regional Entities use regionally adjusted percentages of nameplate capacity to estimate the proven capacity of wind. Improvements in wind forecasting are also necessary to assure that adequate resources are in place in operational horizon. In MISO, wind output during the 2011 summer peak month ranged from 13 MW to 4,909 MW, as shown in Figure 6.

Figure 6: MISO Average Wind Generation and Registered Wind Capacity (2009-2011 Summer)



As recommended in NERC's *Accommodating High Levels of Variable Generation* report,⁴⁰ and further developed in the follow-on study *Flexibility Requirements and Potential Metrics for Variable Generations: Implications for System Planning Studies*,⁴¹ reliability metrics are needed to measure flexibility requirements of the bulk power system to address large-scale wind generation integration. Considerations should include ramping requirements, minimum generation levels, required shorter scheduling intervals, equivalent load carrying capability, and transmission interconnections. Additional data is needed to support the bulk power system flexibility and resource adequacy assessment.

³⁹ http://www.nerc.com/files/2011%20LTRA_Final.pdf

⁴⁰ <http://www.nerc.com/files/Special%20Report%20-%20Accommodating%20High%20Levels%20of%20Variable%20Generation.pdf>

⁴¹ http://www.nerc.com/files/IVGTF_Task_1_4_Final.pdf

Demand Response Deployment

As the role of demand response increases, both NERC and stakeholders need to develop metrics and quantify its performance in order to further measure reliability risks from substantial developments. In 2011, NERC collected the first ever reliability related demand response information across 133 entities within North America. This includes enrollment and actual performance data from April 1 to September 30, 2011. With the second warmest North American summer on record at an average temperature of 74.5°F;⁴² the months of June, July, and August had the largest number of demand response events called and also the largest number of enrolled resources and capacity.

August had the largest enrollment out of the six months with a total of 7,360,605 resources and 56,601 MW, close to five percent of 2011 summer generation capacity. There were 664 deployments during this period with July (247 events, 16,283 MW, 70 percent realization rate) and August (153 deployments, 10,896 MW, 77 percent realization rate) being the most active. As evidenced in the 2011 Post Summer Assessment chapter of this report, PJM and ISO-NE both issued energy emergency alerts and called for use of reliability related demand response over peak load conditions.

Key Finding 6: More Data and Research is Needed

Many datasets and performance analyses conducted in this report are still in an early stage. A number of metrics are limited to occurrence count values; no additional details, such as duration and/or intensity are available to provide a better observation of how each occurrence impacts bulk power system reliability.

The PAS recognizes the importance of producing system reliability risks promptly on an annual basis to ensure risks to reliability are identified and actionable steps can be deliberated upon by industry to address these risks. That said, the PAS expects that as it continues its performance analysis and measurement of reliability risks, limitations and enhancements of data and metrics will be identified, which will require review and modification of the reported data. These enhancements will be captured in future reports. Further, when important trends emerge, NERC will highlight concerns swiftly to ensure industry remains informed and can take actions to control risks to reliability.

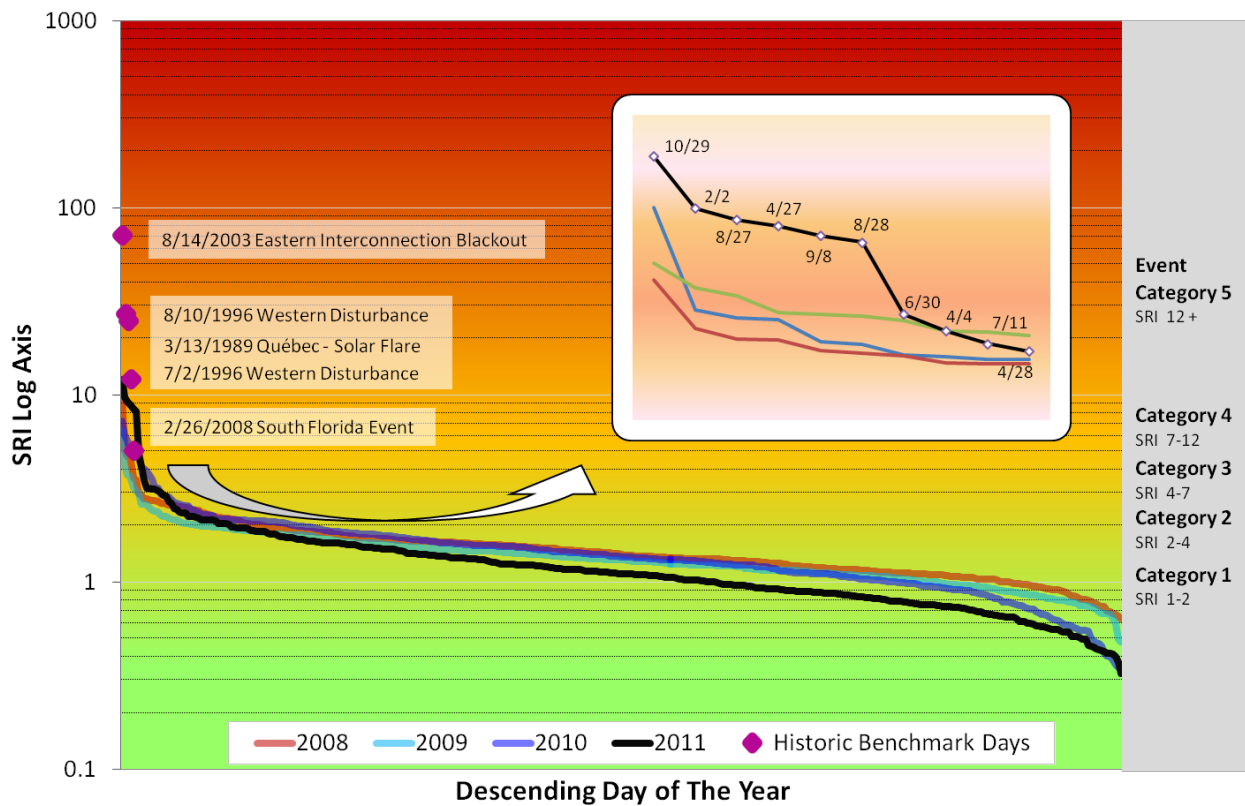
⁴² <http://www.ncdc.noaa.gov/sotc/national/2011/8>

Daily Performance Severity Risk Assessment

NERC Assessment

Figure 7 captures the daily SRI⁴³ value from 2008 to 2011. Other features are also shown on this graphic, including the historic significant events that were used to help substantiate the measurement system. Also, event categories are roughly scaled onto the secondary y-axis. A thumbnail explodes the left side of the curve to further highlight stressed days for the year.

Figure 7: NERC Annual Daily Severity Risk Index (SRI) Sorted Descending with Historic Benchmark Days



As the year-to-year performance is evaluated in Figure 7, certain portions of the graph become relevant for specific analysis. First, the left side of the graph, where the system has been substantially stressed, should be considered in the context of the days which were noteworthy. Next, the slope of the central part of the graph may reveal year-on-year changes in performance for the majority of the days of the year and demonstrate routine system resilience. Finally, the right portion of the curve may also provide useful information about how many stellar days occurred during the year, contrasted to prior years.

The thumbnail shown in Figure 7 indicates 2011 had more “high stress days” experienced in prior years. Table 5 lists the 10 event dates with highest daily SRI values in 2011. Every event

⁴³ http://www.nerc.com/docs/pc/rmwg/pas/index_team/SRI_Equation_Refinement_May6_2011.pdf

occurred on the date had OE-417⁴⁴ filed. Nine of these 10 events were influenced by weather. The three events that required event analysis were the February 2 cold snap event, June 30 disturbance event, and September 8 Arizona-Southern California outage event.

Table 5: 2011 NERC Top 10 SRI Event Days' General Indicators					
Date	NERC SRI Score	Weather Influenced?	Event Analysis?	Highest Event Category ⁴⁵ on Date	OE-417 ⁴⁶ Filed?
10/29	12.08	✓		3	✓
2/2	9.70	✓*	✓	4	✓
8/27	9.19	✓		Less than 2	✓
4/27	8.90	✓		3	✓
9/8	8.46		✓	4	✓
8/28	8.16	✓		Less than 2	✓
6/30	4.85	✓*	✓	2	✓
4/4	4.10	✓		Less than 2	✓
7/11	3.51	✓		Less than 2	✓
4/28	3.18	✓		Less than 2	✓

* Indicates partial influence

However, further examination of the central part of the graph shows that 2011 had improving “day-to-day” performance demonstrated by the more pronounced downward slope than occurred in previous years. Finally, examination of the right portion of 2011 shows improvement over prior years. Thus, while more serious days may have occurred than in prior years, the majority of the year’s performance was a noticeable improvement over other years.

In Figure 8 to Figure 11, additional statistical data is provided to show the trend in median and outlier performance across the years. Generally the median value of daily SRI values ranged from 1.10 to 1.44 with evidence of more outliers occurring in 2011.

⁴⁴ https://www.oe.netl.doe.gov/docs/OE417_submission_instructions.pdf

⁴⁵ http://www.nerc.com/files/ERO_Event_Analysis_Process_Document_Version_1_Feb_2012.pdf

⁴⁶ https://www.oe.netl.doe.gov/docs/OE417_submission_instructions.pdf

Figure 8: 2008 Statistical SRI Summary

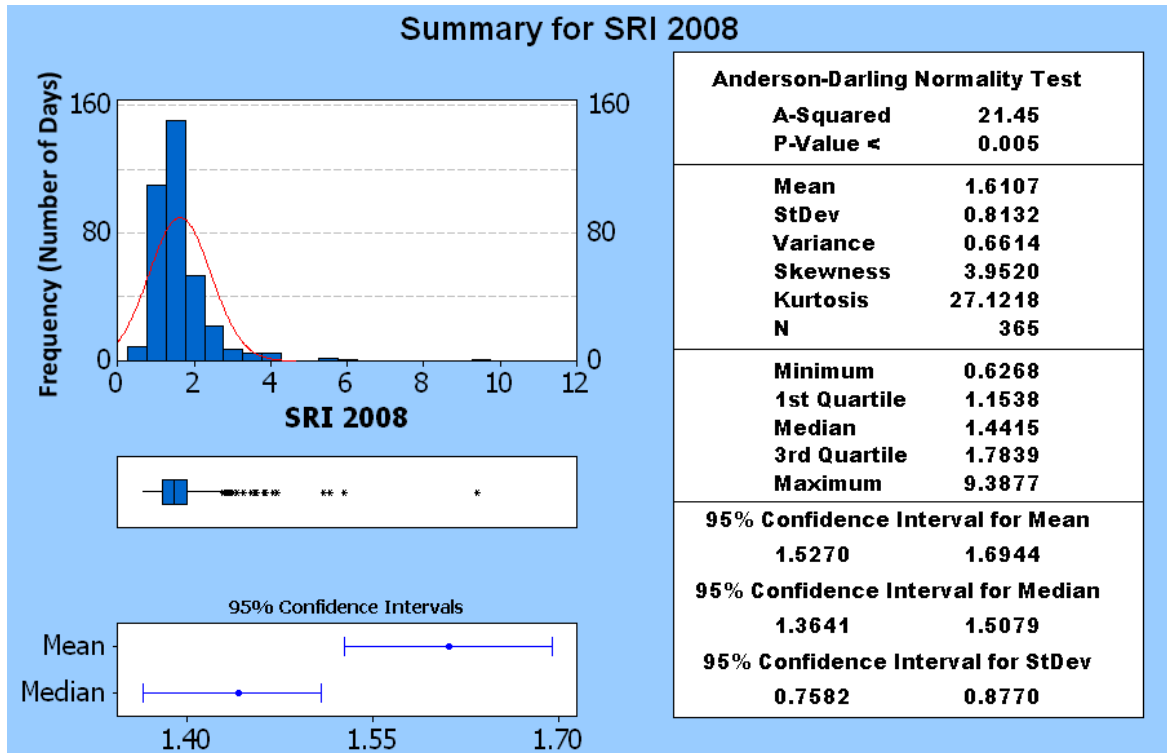


Figure 9: 2009 Statistical SRI Summary

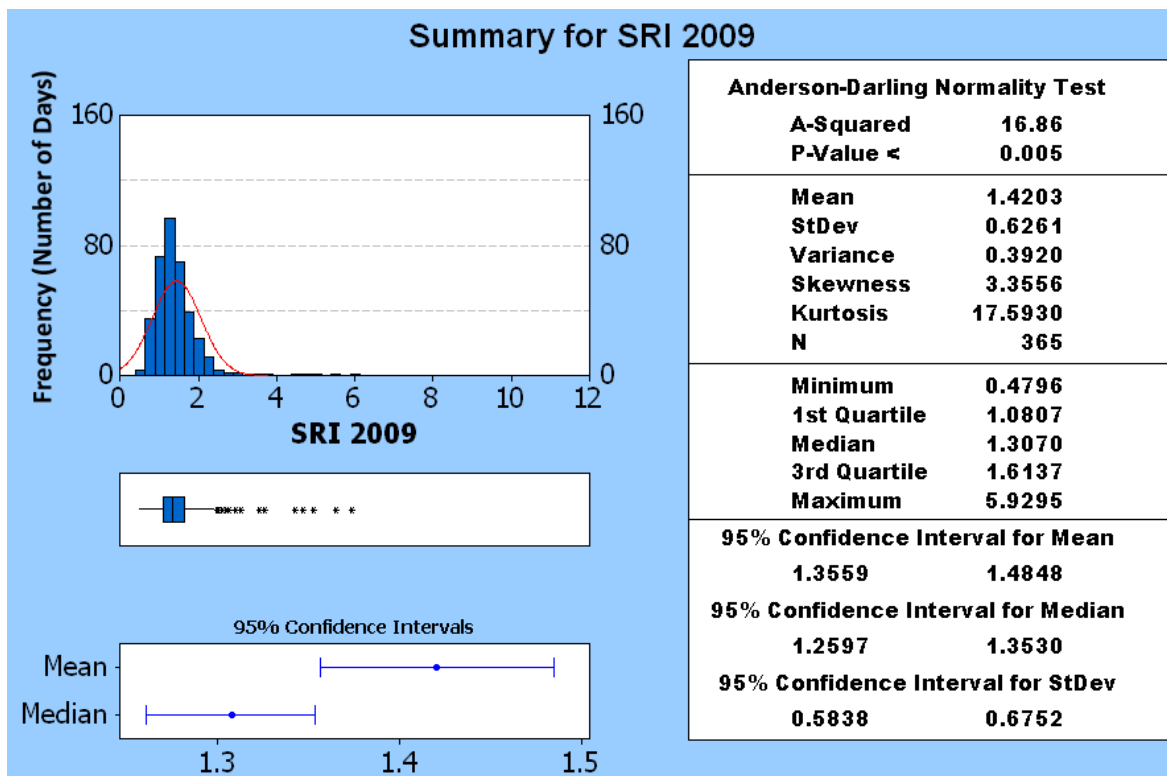


Figure 10: 2010 Statistical SRI Summary

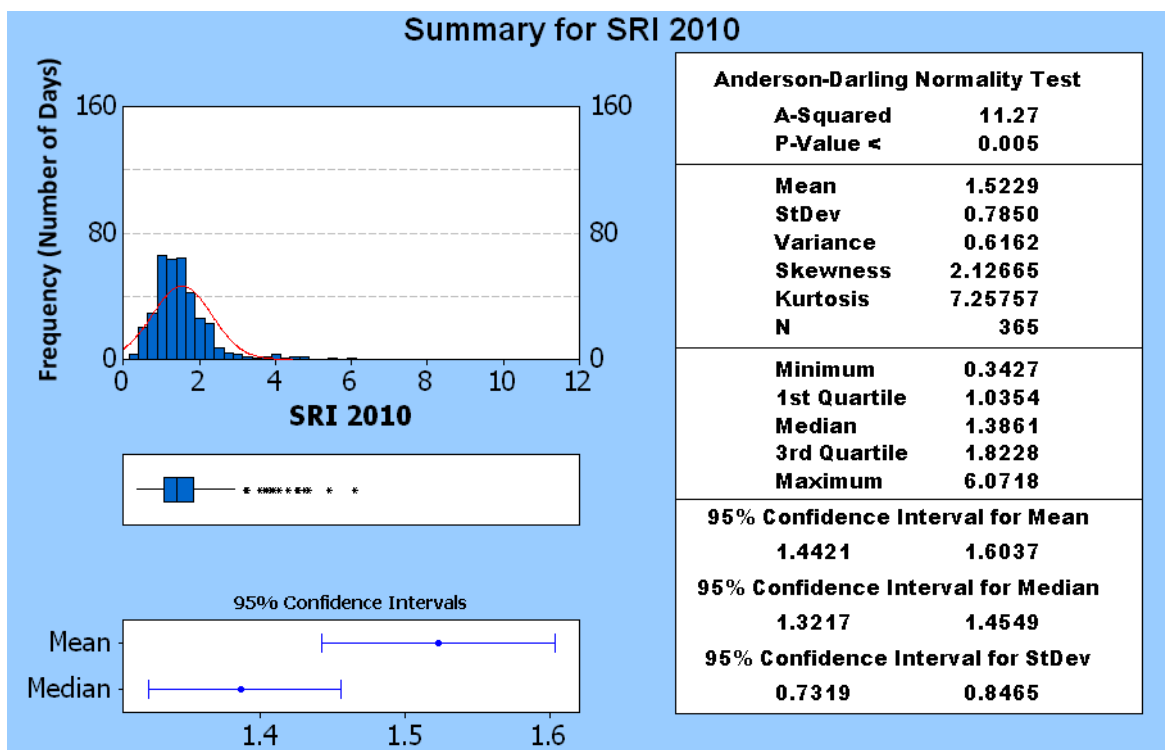
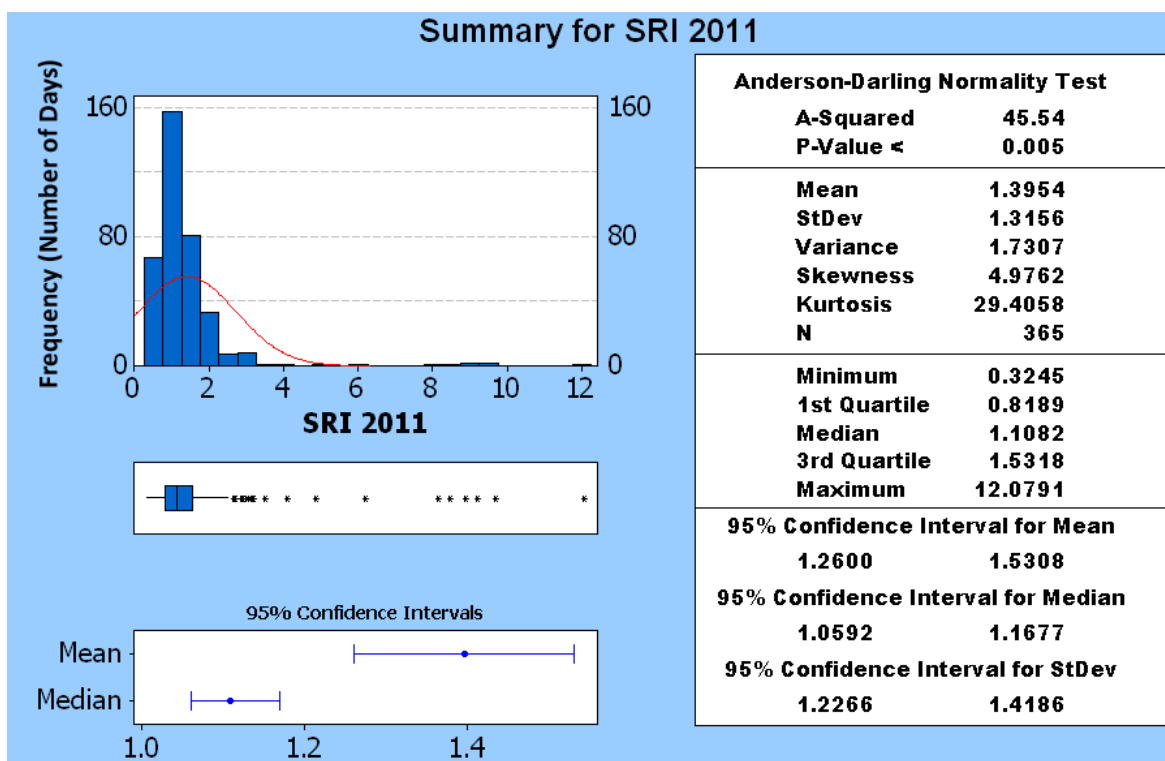


Figure 11: 2011 Statistical SRI Summary



In Figure 12, annual cumulative performance of the bulk power system is shown. The graph can be read by evaluating the lack of significant “steps” that occur on any given day. If a big step happens, it represents a stress day as measured by the SRI. It can be seen the year-end performance of the system improved over prior years but was impacted by several “steps”. These seemed to fall more toward the latter part of the year. However, without additional analysis and review of completed events analyses, no trends about the time of the year could be concluded.

Figure 12: NERC Cumulative SRI Performance History (2008-2011)

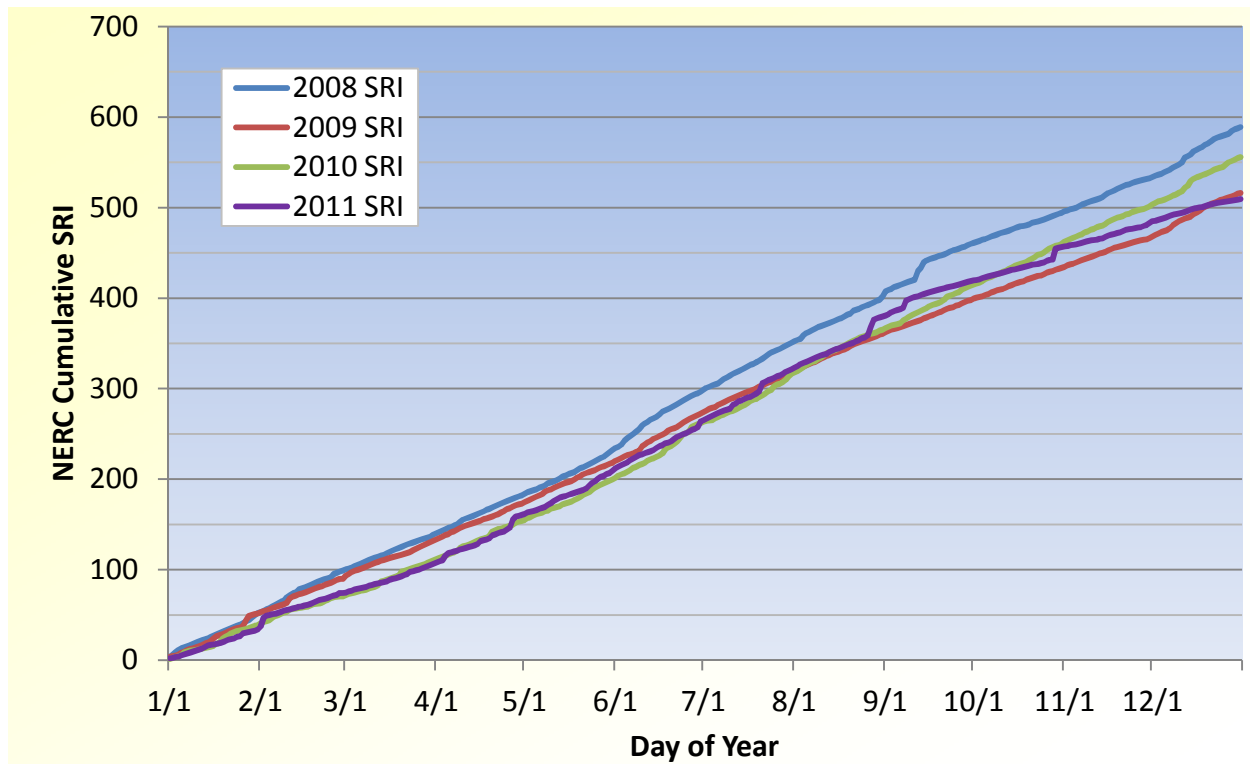
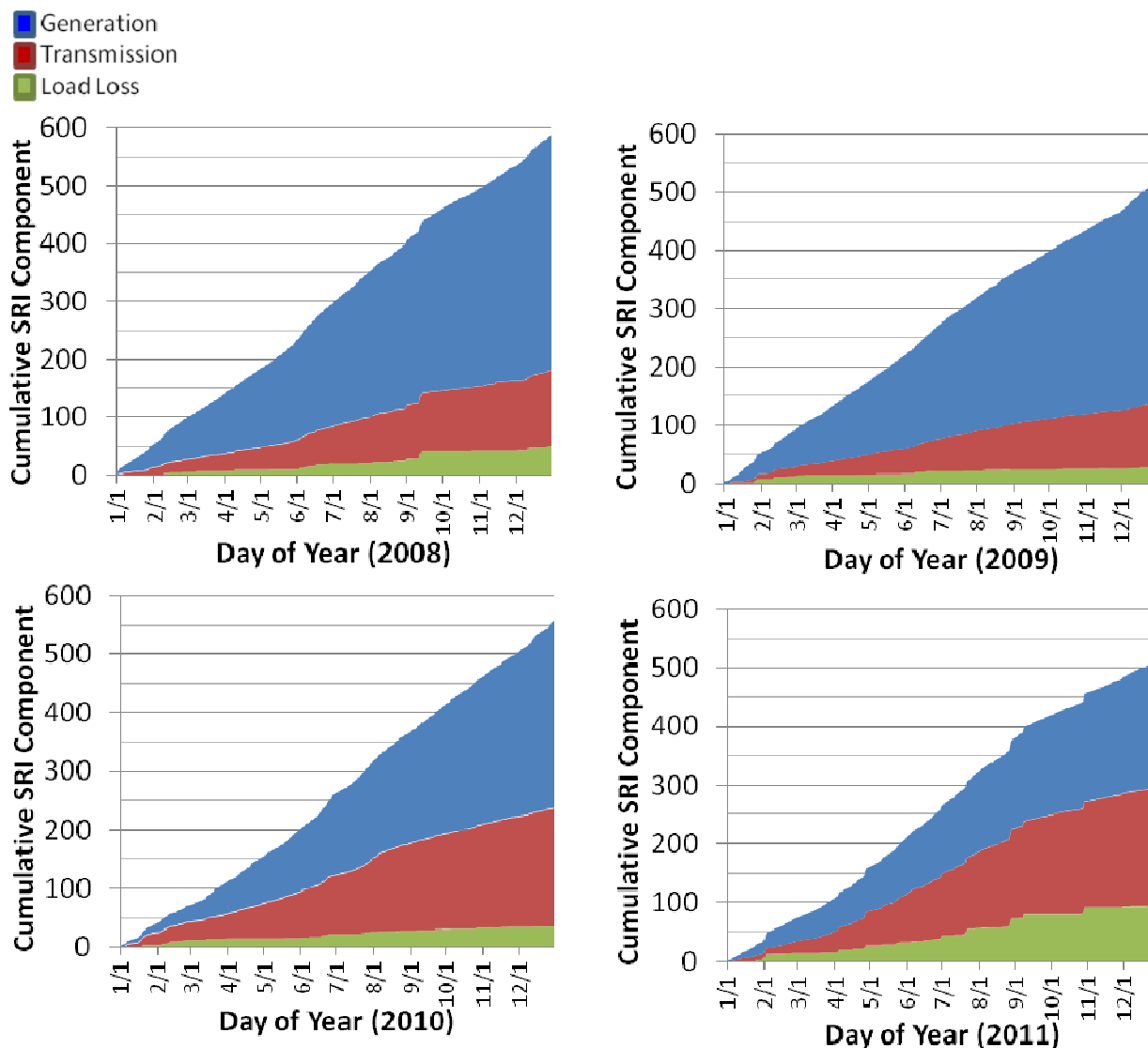


Figure 13 breaks down the cumulative performance by bulk power system segment (generation, transmission, and load loss). From 2008 to 2011, the generation component is the largest followed by the transmission and then the load loss component. Notably, the components of Figure 13 exhibit a choppy characteristic in 2011 compared to prior years, which can be attributed to the higher number of “high stress days” in 2011.

Although 2011 had more “high stress” days, the total cumulative performance remained below 2008, 2009, and 2010. This may be due to a reduction of cumulative slope in all three components starting in mid-September. The change of cumulative slope is caused by a number of days with very good performance from mid-September until the end of 2011.

Figure 13: NERC Cumulative SRI by Bulk Power System Segment (2008-2011)

Eastern Interconnection Assessment

In Figure 14 and Figure 15, SRI performance history and annual cumulative performance of the bulk power system in the Eastern Interconnection are shown, respectively. The graph can be read by evaluating the lack of significant “steps” that occur on any given day. If a big step happens, it represents a stress day as measured by the SRI. Significant stress days for 2011 in the Eastern Interconnection include: the April 27 and 28 Southeastern tornadoes, Hurricane Irene on August 27 and 28, and the Northeastern snowstorm on October 29.

Figure 14: Eastern Interconnection SRI Performance History (2008-2011)

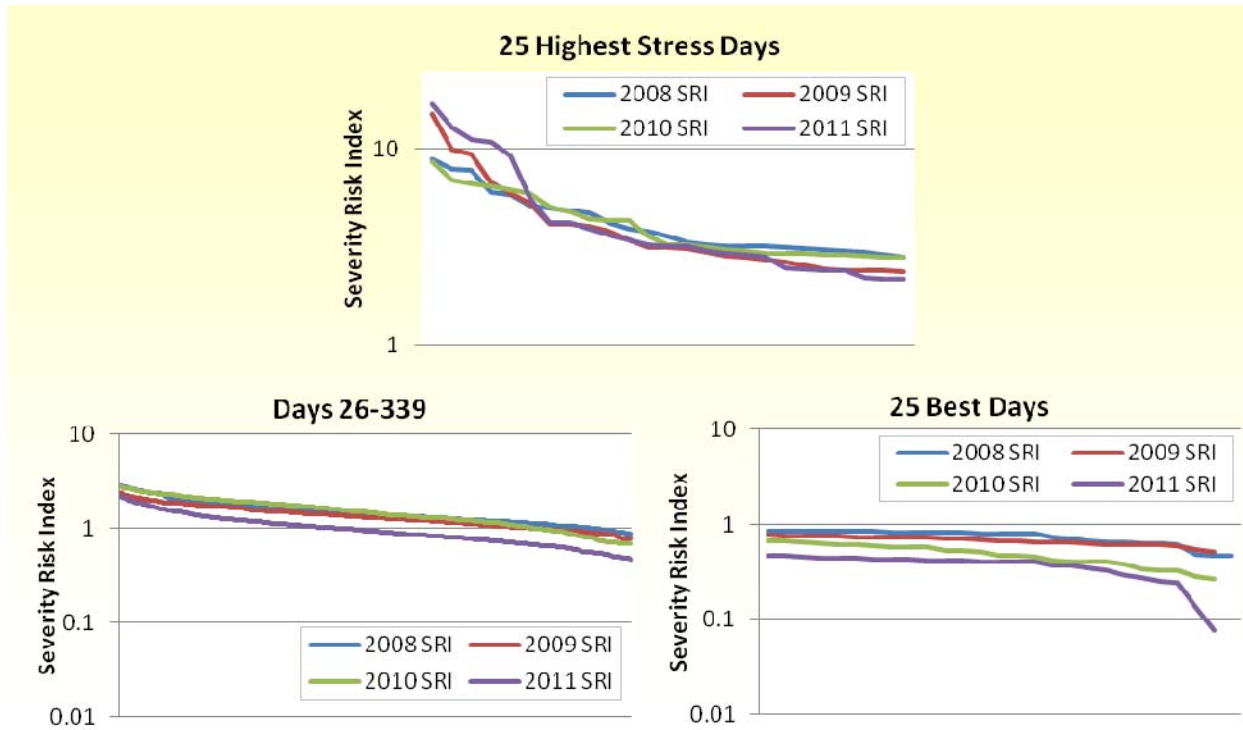


Figure 15: Eastern Interconnection Cumulative SRI Performance History (2008-2011)

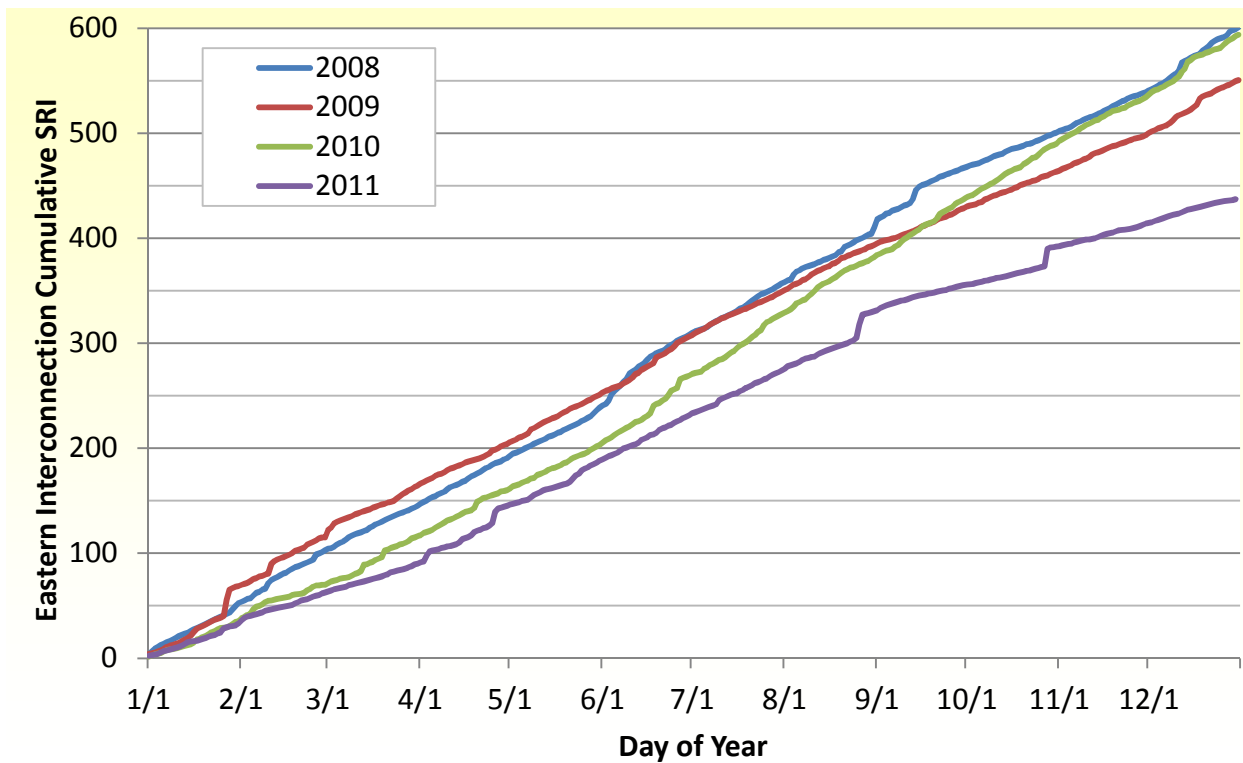
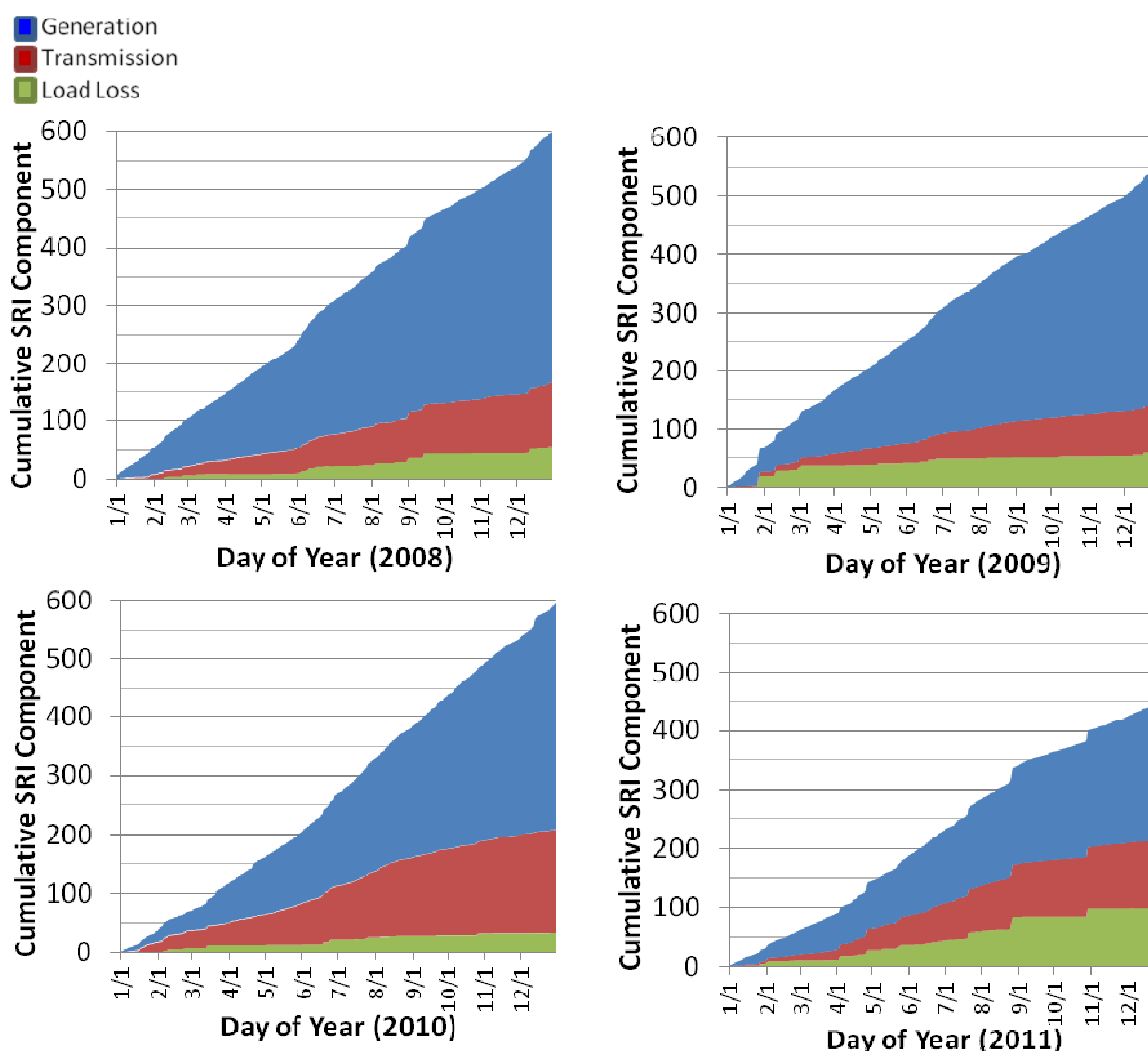


Figure 16 breaks the cumulative SRI performance of Figure 15 into the bulk power system components of generation, transmission, and load loss. In 2011, the ratio between the generation component, transmission, and load loss component shows the load loss and transmission component being proportionally larger than in prior years.

Figure 16: Eastern Interconnection Cumulative SRI by Bulk Power System Segment (2008-2011)



Western Interconnection Assessment

In Figure 17 and Figure 18, SRI performance history and annual cumulative performance of the bulk power system in the Western Interconnection are shown, respectively. The graph can be read by evaluating the lack of significant “steps” that occur on any given day. If a big step happens, it represents a stress day as measured by the SRI. Significant stress days for 2011 in the Western Interconnection include a February 2 generation inadequacy event and a load loss event on September 8.

Figure 17: Western Interconnection SRI Performance History (2008-2011)

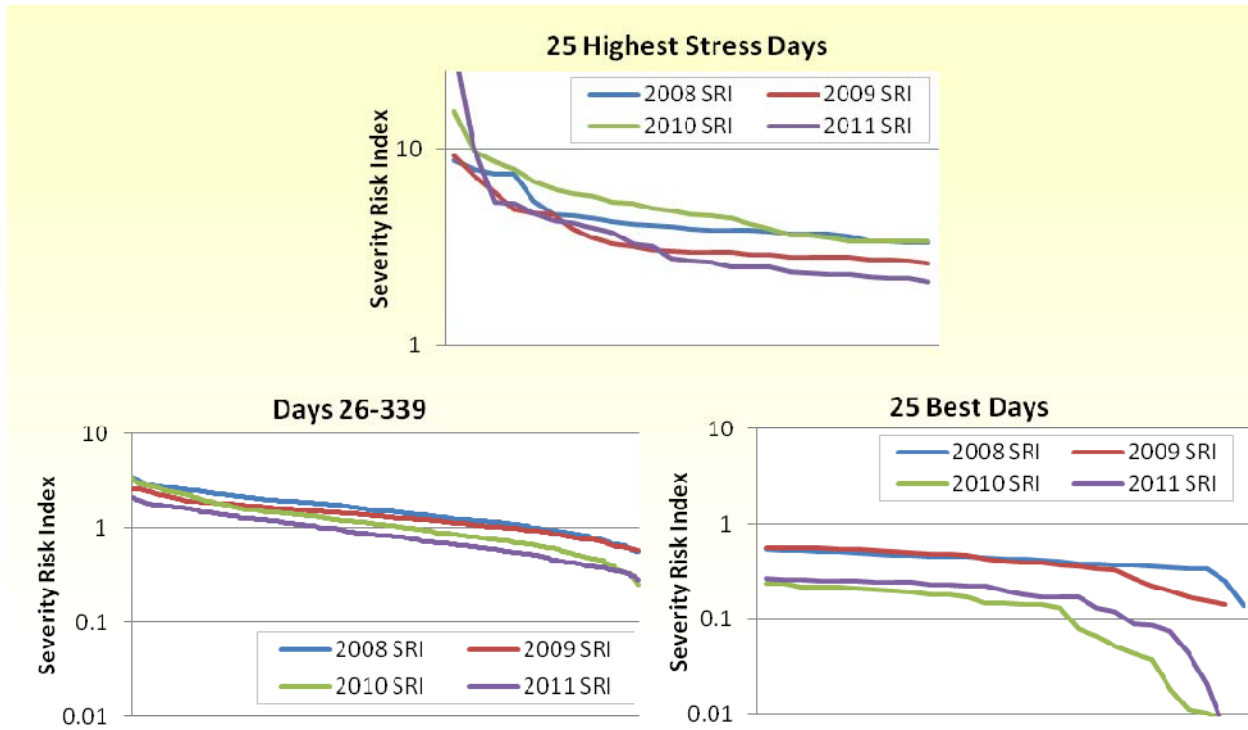


Figure 18: Western Interconnection Cumulative SRI Performance History (2008-2011)

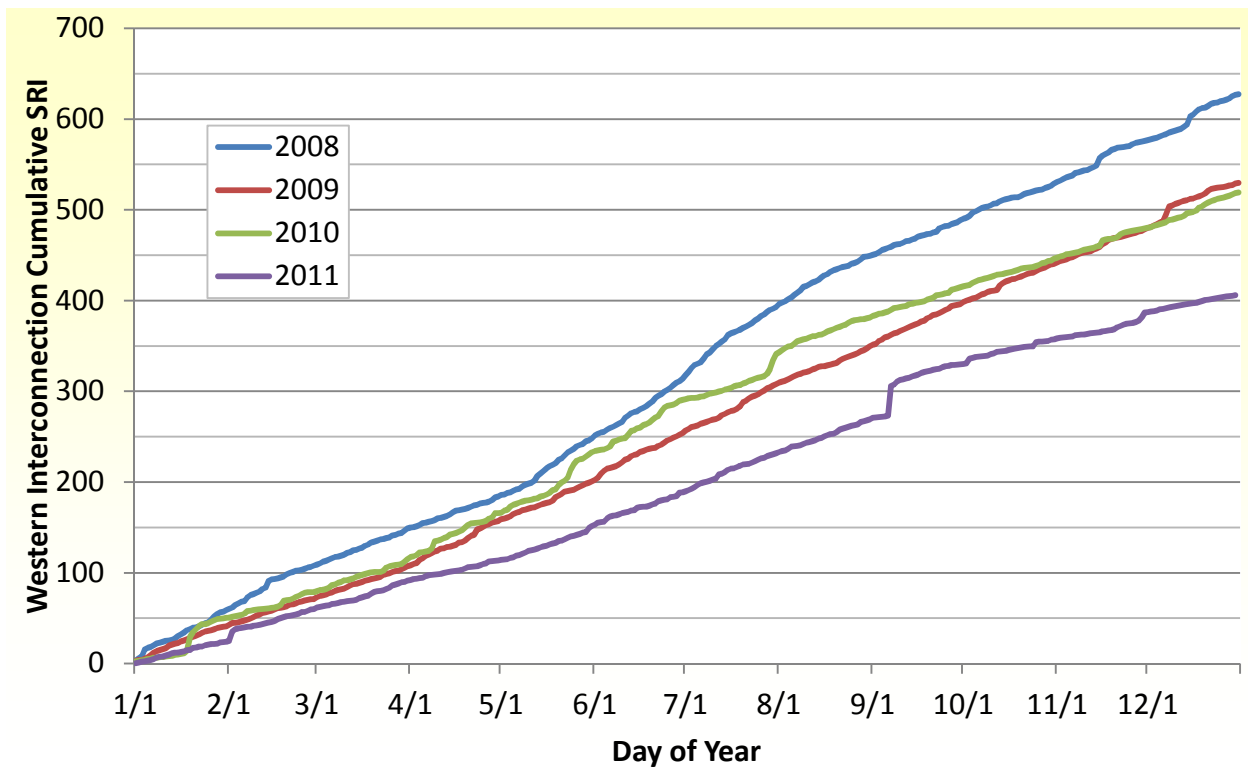
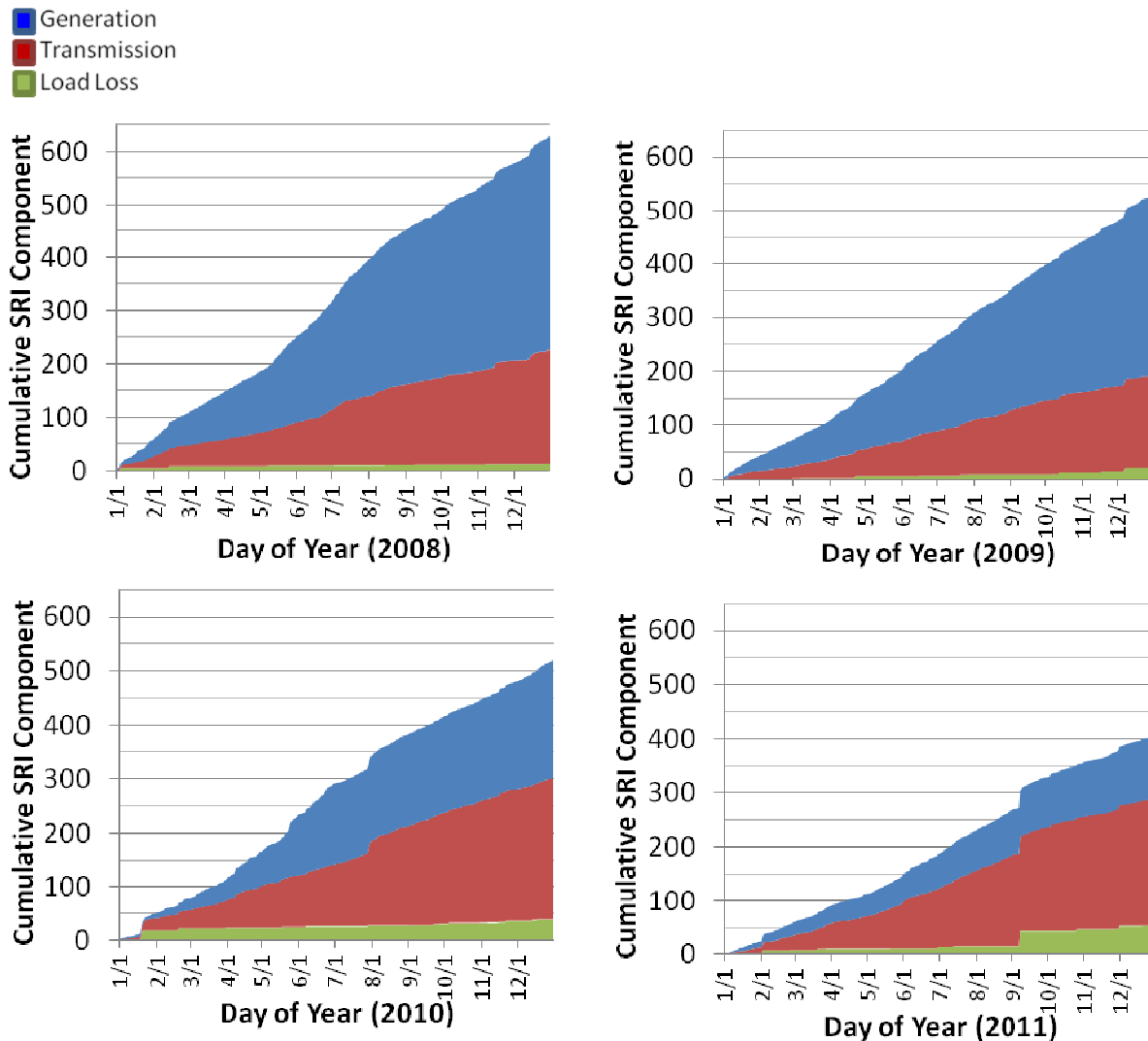


Figure 19 breaks the cumulative SRI performance of Figure 18 into the bulk power system components of generation, transmission, and load loss. In 2011, the ratio between the generation component, transmission, and load loss component shows the generation loss component comprising a much smaller component and the load loss component comprising a larger proportion than in previous years.

Figure 19: Western Interconnection Cumulative SRI by Bulk Power System Segment (2008-2011)



ERCOT Interconnection Assessment

In Figure 20 and Figure 21, SRI performance history and annual cumulative performance of the bulk power system in the ERCOT Interconnection are shown, respectively. The graph can be read by evaluating the lack of significant “steps” that occur on any given day. If a big step happens, it represents a stress day as measured by the SRI. Significant stress days for 2011 in the ERCOT Interconnection include a generation inadequacy event from February 2 to 4.

Figure 20: ERCOT Interconnection SRI Performance History (2008-2011)

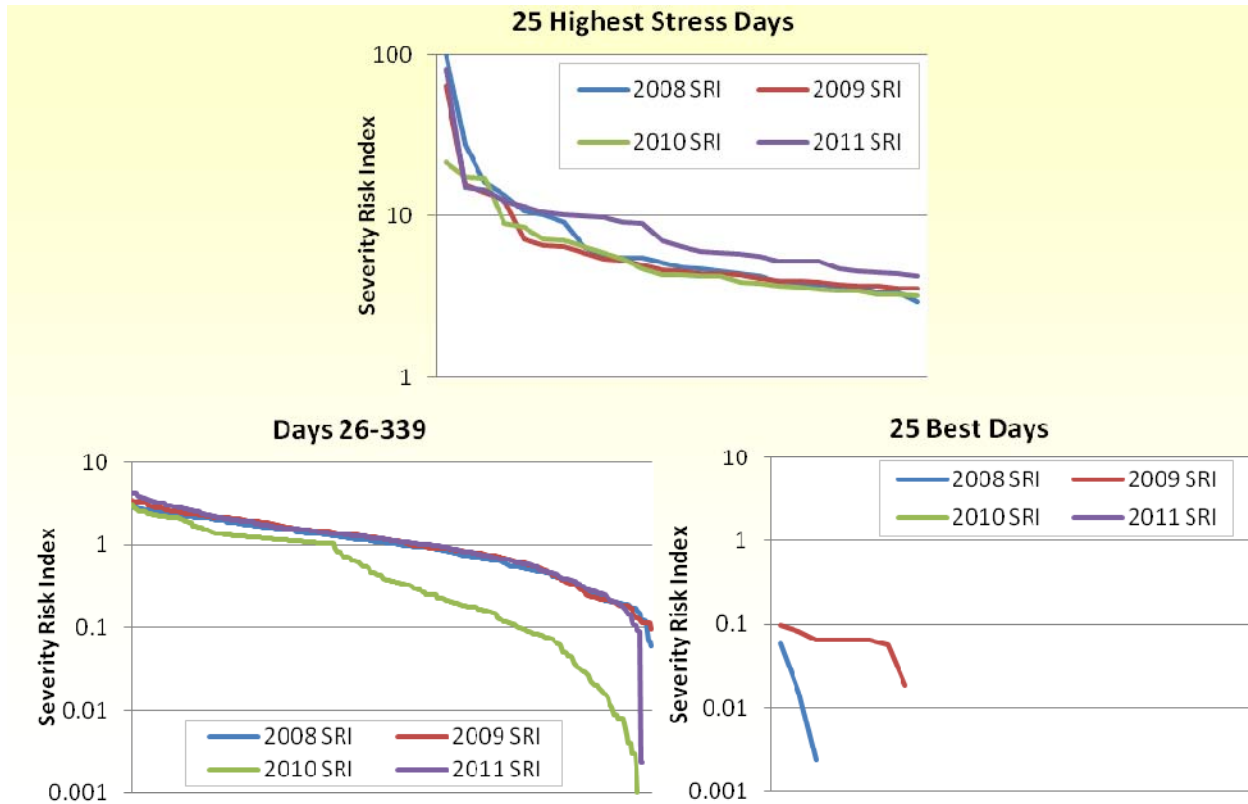


Figure 21: ERCOT Interconnection Cumulative SRI Performance History (2008-2011)

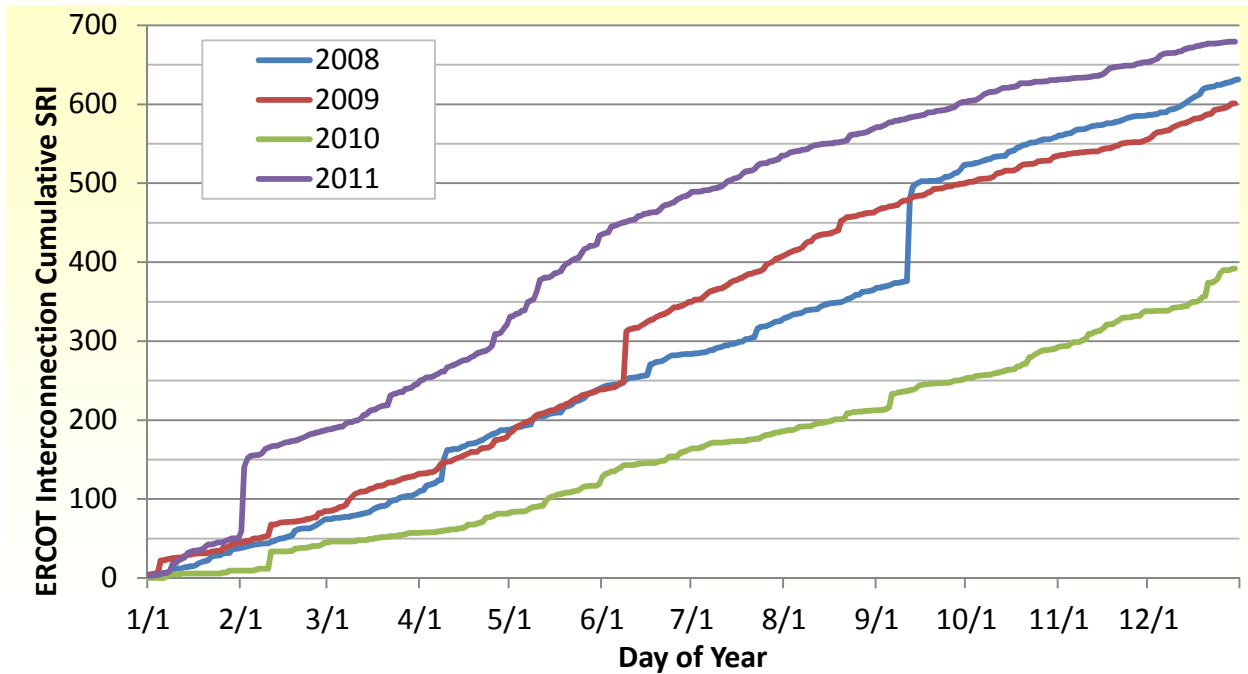
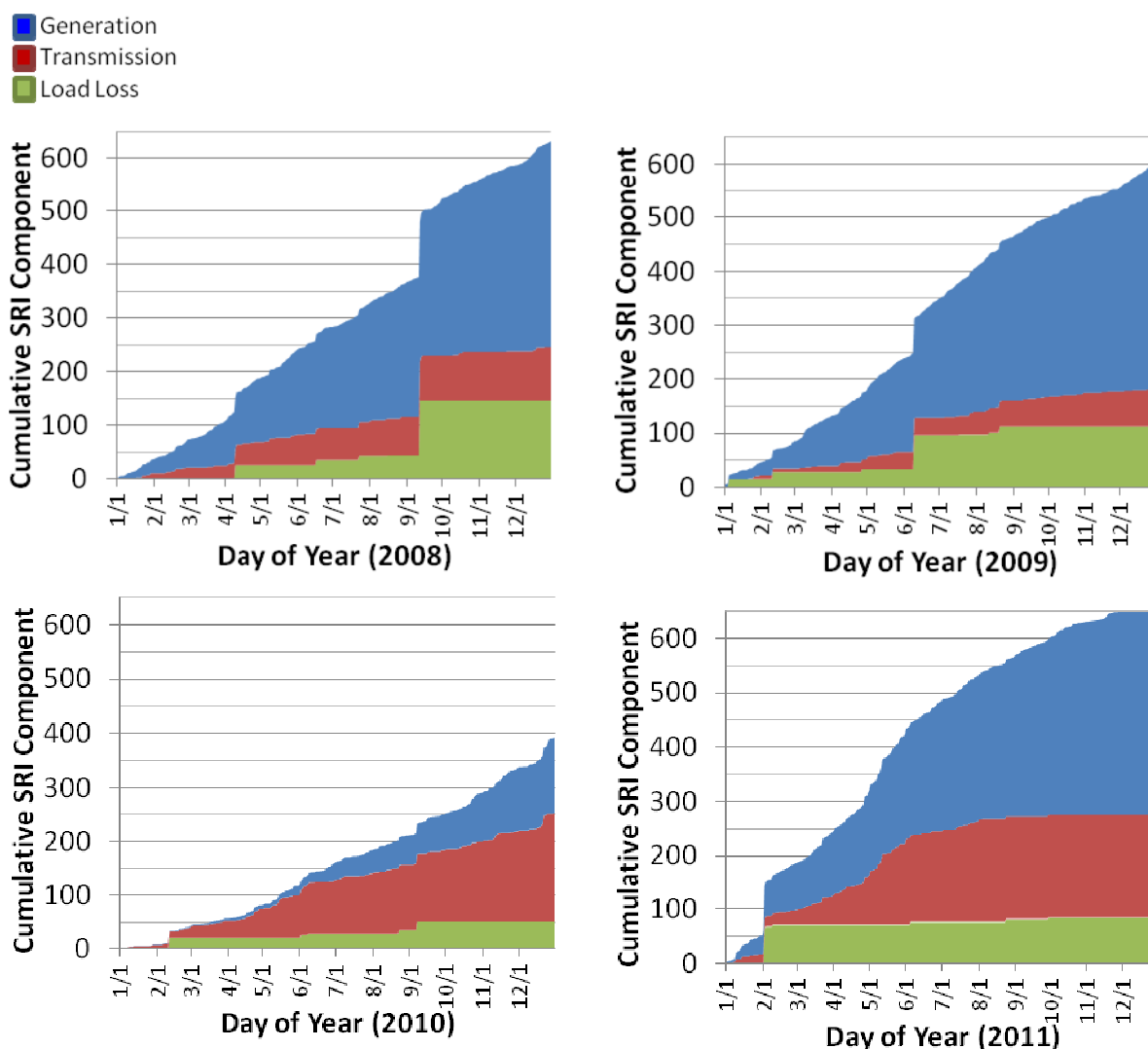


Figure 22 breaks the cumulative SRI performance of Figure 21 into the bulk power system components of generation, transmission, and load loss. In 2011, the ratio between the generation component, transmission, and load loss component shows the generation loss component to be more predominant in 2011 than 2010.

Figure 22: ERCOT Interconnection Cumulative SRI by Bulk Power System Segment (2008-2011)



Québec Interconnection Assessment

There is insufficient historic daily generation outage and event data for Québec Interconnection (QI). The QI SRI assessment will be provided in a future report.

Reliability Indicator Trends

Overview

Building upon last year's metric review, the results of eighteen performance metrics continue to be assessed. Due to data availability, each of the performance metrics does not address the same time periods (some metrics have just been established, while others have data over many years). At this time, the number of metrics is expected to remain constant; however, other metrics may supplant existing metrics which may have more merit.

Each metric is designed to show a measure for a given ALR characteristic. In Table 6, each metric is placed into a grid showing which ALR characteristic that metric represents. Also, the standard objective areas are shown for each ALR metric to provide a connection between standard objectives and ALR characteristics.

Table 6: Adequate Level of Reliability Characteristics ⁴⁷						
Standard Objectives	Boundary	Contingencies	Integrity	Protection	Restoration	Adequacy
Reliability Planning and Operating Performance		ALR1-4	ALR3-5	ALR4-1		ALR1-3 ALR6-1 ALR6-11 ALR6-12 ALR6-13 ALR6-14 ALR6-15 ALR6-16
Frequency and Voltage Performance	ALR1-5 ALR1-12	ALR2-4 ALR2-5		ALR2-3		
Reliability Information						
Emergency Preparation						ALR6-2 ALR6-3
Communications and Control						
Personnel						
Wide-area View						
Security						

⁴⁷ The blank fields indicate no metrics have been developed to assess related ALR characteristics at this time.

These metrics exist within a reliability framework, and, overall, the performance metrics being considered address the fundamental characteristics of an ALR.⁴⁸ Each of the performance categories being measured by the metrics should be considered in aggregate when making an assessment of the reliability of the bulk power system with no single metric indicating exceptional or poor performance of the power system.

Importantly, due to regional differences (size of the Region, operating practices, etc.) comparing the performance of one Region to another would be erroneous and inappropriate. Furthermore, depending on the Region being evaluated, one metric may be more relevant to a specific Region's performance than another, and assessments may be more subjective than a purely mathematical analysis. Finally, choosing one Region's best metric performance to define targets for other Regions is also inappropriate.

Another metric reporting principle is to retain anonymity of any individual reporting organization. Thus, granularity will be attempted only to the point that such action will not compromise anonymity of any individual reporting organization.

An overview of the ALR metric ratings for 2011 is provided in Table 7. Although a number of performance categories have been assessed, some do not have sufficient data to derive conclusions from the metric results. Continued assessment of these metrics should continue until sufficient data is available.

⁴⁸ <http://www.nerc.com/docs/pc/Definition-of-ALR-approved-at-Dec-07-OC-PC-mtgs.pdf>

Table 7: 2011 Metric Trend Ratings		
ALR	Boundary	Trend Rating
1-5	System Voltage Performance	
1-12	Interconnection Frequency Response	
Contingencies		
1-4	BPS Transmission Related Events Resulting in Loss of Load	
2-4	Average Percent Non-Recovery Disturbance Control Standard Events	
2-5	Disturbance Control Events Greater than Most Severe Single Contingency	
Integrity		
3-5	Interconnected Reliability Operating Limit/ System Operating Limit (IROL/SOL) Exceedances	
Protection		
2-3	Activation of Under Frequency Load Shedding	
4-1	Automatic Transmission Outages Caused by Failed Protection System Equipment	
Adequacy		
1-3	Planning Reserve Margin	
6-1	Transmission Constraint Mitigation	
6-2	Energy Emergency Alert 3 (EEA3)	
6-3	Energy Emergency Alert 2 (EEA2)	
6-11	Automatic AC Transmission Outages Initiated by Failed Protection System Equipment	
6-12	Automatic AC Transmission Outages Initiated by Human Error	
6-13	Automatic AC Transmission Outages Initiated by Failed AC Substation Equipment	
6-14	Automatic AC Transmission Outages Initiated by Failed AC Circuit Equipment	
6-15	Element Availability Percentage (APC)	
6-16	Transmission System Unavailability	
Trend Rating Symbols		
Significant Improvement		
Slight Improvement		
No Change / Inconclusive		
Slight Deterioration		
Significant Deterioration		
New Data		

ALR Characteristic: Boundary

ALR1-5 System Voltage Performance

Background

The purpose of this metric is to measure transmission system voltage performance at specific key buses over time. This will be used as an indication of trends in the reactive capability available to the transmission system. The metric is intended to record the amount of time that system voltage is outside a predetermined band around nominal. The band is selected by the transmission owner and retained over time to facilitate trending.

Assessment

Table 8 shows the fourth quarter of 2011 measurement of system voltage performance in minutes above and below the bus's voltage band. These measurements are normalized by the total number of buses. No conclusions should be drawn comparing voltage classes. The value of this metric will come by comparing the average number of minutes buses are outside predetermined ranges over time.

Table 8: ALR1-5 System Voltage Performance by Bus Voltage Class (2011Q4)			
Bus Voltage Class (kV)	Number of Buses	Minutes Below Threshold per Bus	Minutes Above Threshold per Bus
345	86	0	924
500	87	19	133
765	26	4	708

Special Considerations

With a pilot program specified in early 2011, the Operating Reliability Subcommittee (ORS) and the former Reliability Coordinator Working Group (RCWG) provided technical support to identify key buses to monitor. NERC's Operating and Planning Committees subsequently endorsed a voluntary data request letter for respective Transmission Owners (TOs) to submit relevant data on the key buses. More than fifty of the seventy-seven TOs, representing two-thirds of the 296 key buses, voluntarily submitted data for fourth quarter 2011.

The number of buses, the monitored voltage levels, and the voltage ranges vary by reporting entities. Each reporting entity is tasked with determining the voltage range for each bus based on the system configuration near the bus. While the ranges may be similar, they are not the same for all of the key buses. By retaining the same voltage range at each bus over time, comparisons will indicate trends in voltage control, useful to identify reactive power needs for specific areas. Based upon the usefulness of the data collected in the pilot program, additional data needs will be reviewed.

ALR1-12 Interconnection Frequency Response

Background

This metric is used to track and monitor Interconnection Frequency Response. Frequency Response⁴⁹ is a measure of an Interconnection's ability to stabilize frequency immediately following the sudden loss of generation or load. It is a critical component to the reliable operation of the bulk power system, particularly during disturbances and restoration. The metric measures the average Frequency Response for all events where frequency drops more than the Interconnection's defined threshold as shown in Table 9.

Assessment

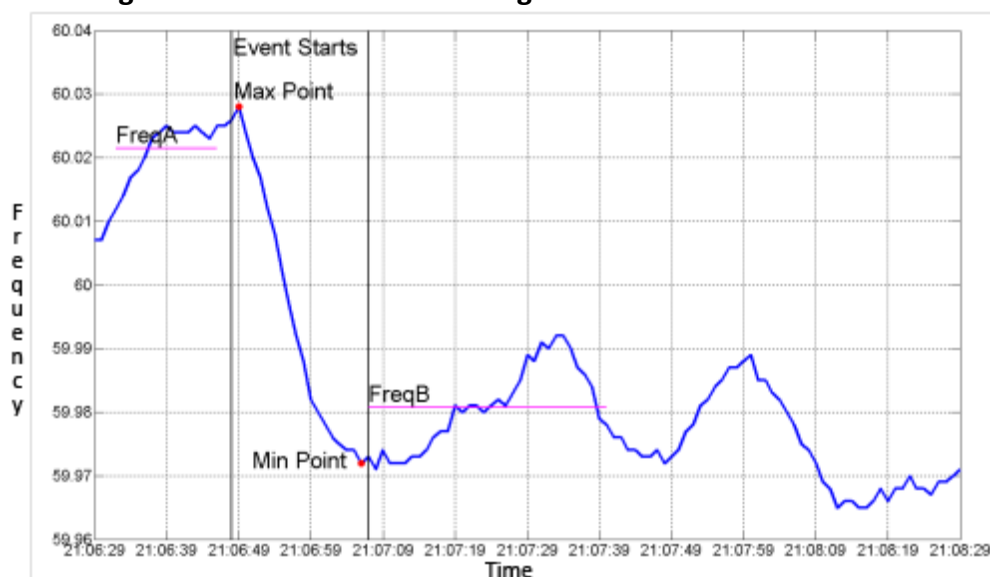
The following are Frequency Response calculations of Eastern Interconnection (EI), Western Interconnection (WI), ERCOT Interconnection and Québec Interconnection. While the calculations may show trends from year to year, no attempt has been made in this analysis to determine or state what indicates an "acceptable" level of Frequency Response for any of the interconnections. Rather, they show the relative performance from year-to-year and can be a basis for further root-cause analysis. Further, the Frequency Response should not be compared between interconnections as their bulk power system characteristics differ significantly in terms of number of facilities, miles of line, operating principles and simple physical, geographic and climatic conditions. Some annualized Frequency Responses are higher due to the large number of disturbances in the dataset where frequency changes were greater than the generator dead-bands. Also, in earlier studies, the capacity of the unit or gross output at the time of the unit trip rather than the net generation⁵⁰ MW loss to the interconnection was reported. No conclusions as to the absolute value of any of these calculations can be drawn at this time.

Figure 23 shows the criteria for calculating average values A and B. The event starts at time $t \pm 0$. Value A is the average from $t - 16$ to $t - 2$ and Value B is the average from $t + 20$ to $t + 52$. The difference of value A and B is the change in frequency⁵¹ used for calculating Frequency Response. These lengths of time used to calculate these values accounts for the variability in System Control and Data Acquisition (SCADA) scan rates that vary from two to six seconds in the multiple-Balancing Authority interconnections.

⁴⁹ Frequency Response is in fact a negative value. However to reduce confusion for the reader, Frequency Response is expressed in this report as positive values (the absolute value of the actual calculated value).

⁵⁰ There could be a coincident loss of load also.

⁵¹ Definitions of Value A and Value B are on Slide 18 of Presentation 1 in:
http://www.nerc.com/docs/oc/rs/RS_Presentation_October_2011.pdf.

Figure 23: Criteria for Calculating Value A and Value B

The frequency events used to calculate the Interconnection Frequency Response are the same events to be used by Balancing Authorities for the calculation of their Frequency Bias and, eventually, compliance with the proposed Frequency Response Standard (FRS) BAL-003. The monthly frequency event candidate lists are posted on the NERC Resources Subcommittee⁵² webpage. The data collection process is described in the BAL-003 Frequency Response Standard Supporting Document.⁵³ The triggers⁵⁴ for significant frequency events are shown in Table 9.

Table 9: Frequency Event Triggers			
Interconnection	Δ Frequency (mHz)	MW Loss Threshold	Rolling Windows (seconds)
Eastern	36	800	15
Western	70	700	15
ERCOT	90	450	15
Québec	140	450	15

The actual MW loss for the flagged frequency events is determined jointly by NERC and Regional Entity situation awareness staff. Both the change in frequency and the MW loss determine whether the event qualifies for further consideration in the monthly frequency event candidate list.

⁵² <http://www.nerc.com/filez/rs.html>

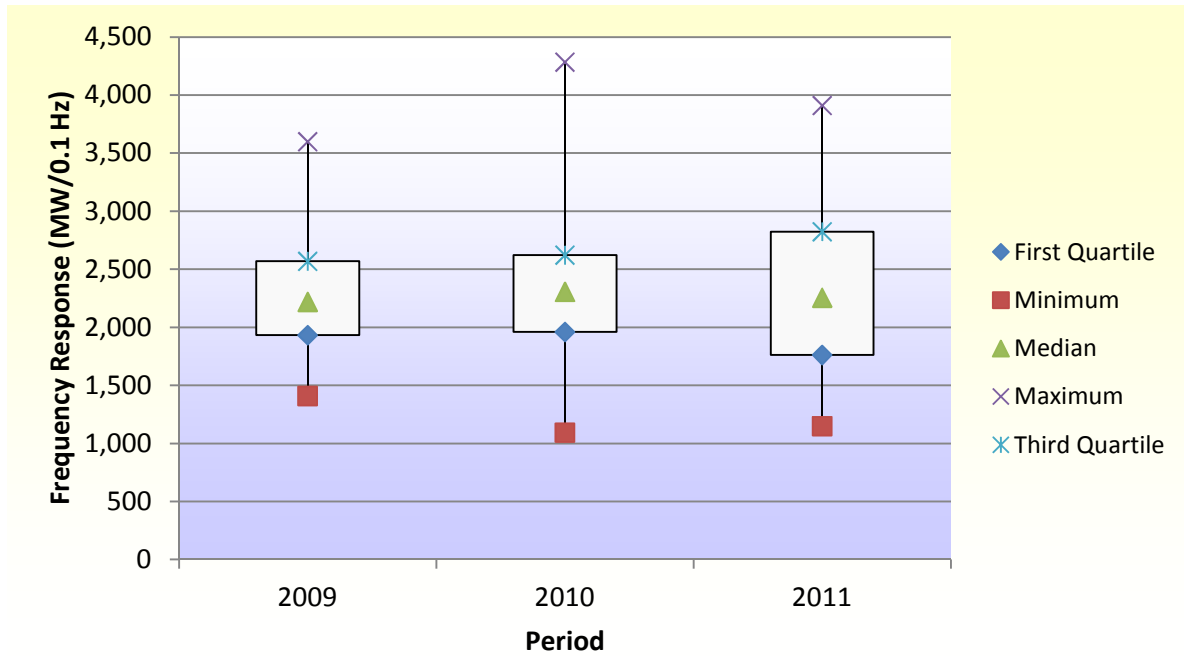
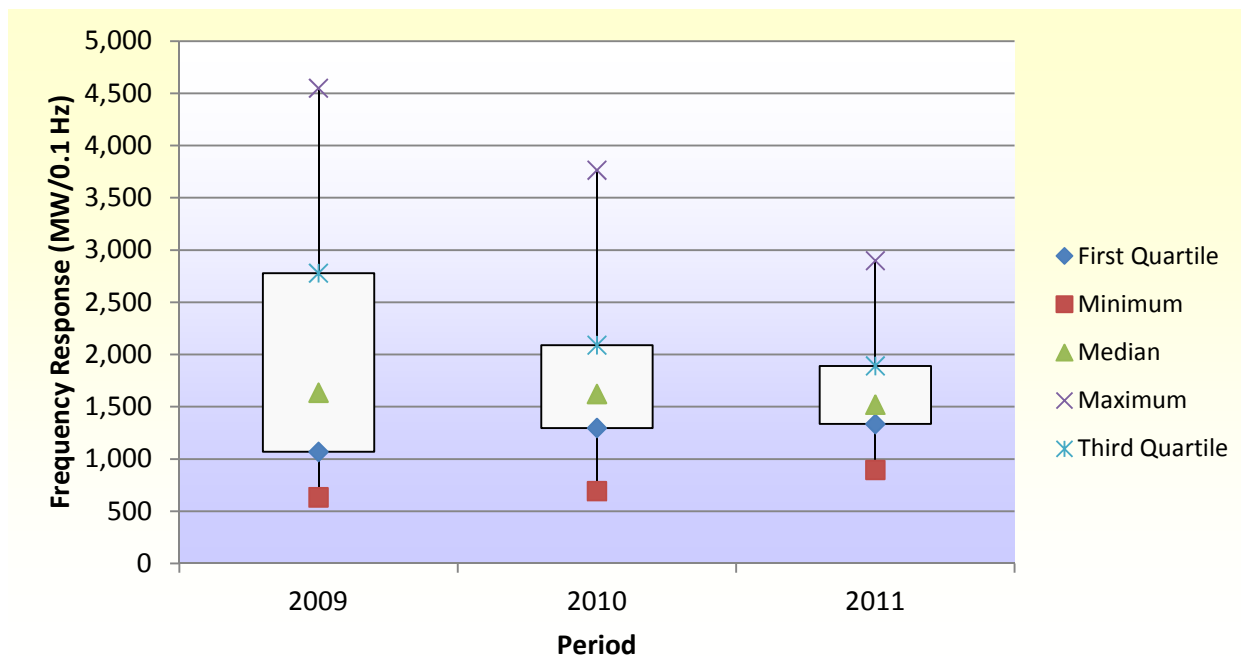
⁵³ <http://www.nerc.com/docs/standards/dt/Attachment%20A%20-%20Frequency%20Response%20Standard%20Supporting%20Document%20-%20RL-%202011%2007%2011.pdf>

⁵⁴ The frequency thresholds were changed to ensure that an appropriate number of significant events are captured for all interconnections. In September 2011, the Québec threshold was changed to 200 mHz. At the beginning of 2012 the Québec threshold was again increased to 300 mHz and the Eastern Interconnection threshold was increased to 40 mHz.

Table 10 shows the number of frequency events per year for each interconnection. In recent years, better tools have been put in place to detect frequency events and their underlying causes. There are also more systematic procedures to document and verify these events. Given that the generation fleet in the EI has not changed much and Frequency Response has been consistent, the number of frequency events that occur would be expected to remain the same for the last several years. The increase in sample size for the EI in 2011 as shown in Table 10 is because more frequency events are captured due to better tools and procedures developed in 2011. This increased sample size leads to increased confidence in the statistics generated by the data.

Table 10: Sample Sizes of Yearly Events			
Interconnection	2009	2010	2011
Western	25	29	25
Eastern	44	49	70
ERCOT	51	67	65
Québec	-	-	20

The Frequency Response box plots for each Interconnection are shown below in Figure 24 to Figure 27. The Québec Interconnection started the data collection process in 2011. Figure 28 to Figure 30 are box plots of the sizes of events as loss in MW. These show that, with the more consistent and streamlined data collection procedures developed in 2011, smaller events in the Eastern Interconnection are being captured. There would be fewer governors triggered due to the dead band for smaller frequency deviations and so these events will have less Frequency Response.

Figure 24: Box Plot Analysis for 2009 to 2011 Eastern Interconnection Data⁵⁵**Figure 25: Box Plot Analysis for 2009 to 2011 Western Interconnection Data**

⁵⁵ A historic perspective of the frequency response trend calculations in the Eastern Interconnection can be found in http://web.eecs.utk.edu/courses/spring2012/ece522/D2010_beta.pdf and http://www.truc.org/files/2006/FDA_2006_010.pdf.

Figure 26: Box Plot Analysis for 2009 to 2011 ERCOT Interconnection Data

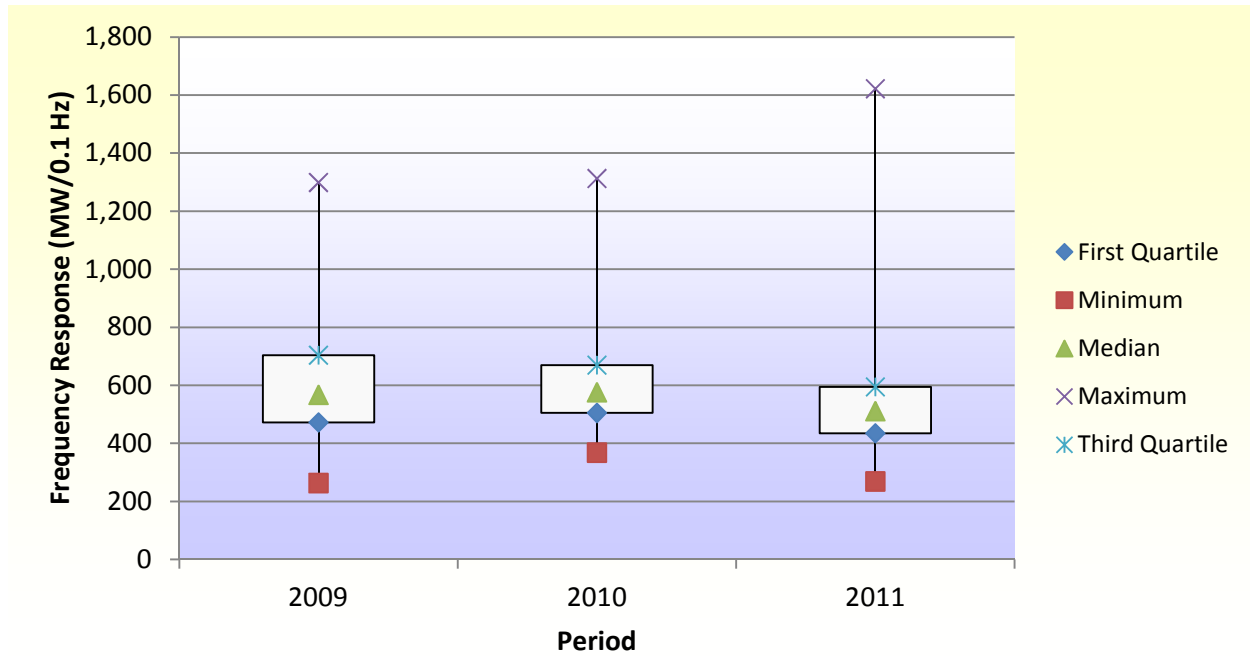


Figure 27: Box Plot Analysis for 2011 Québec Interconnection Data

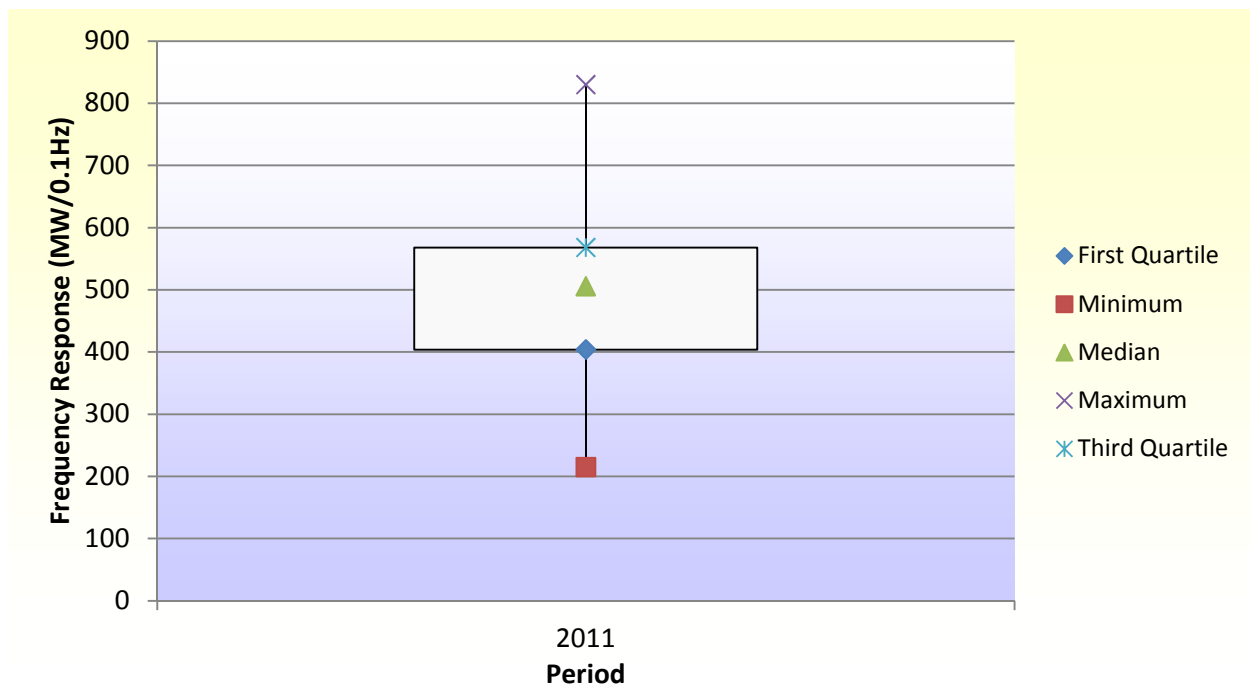


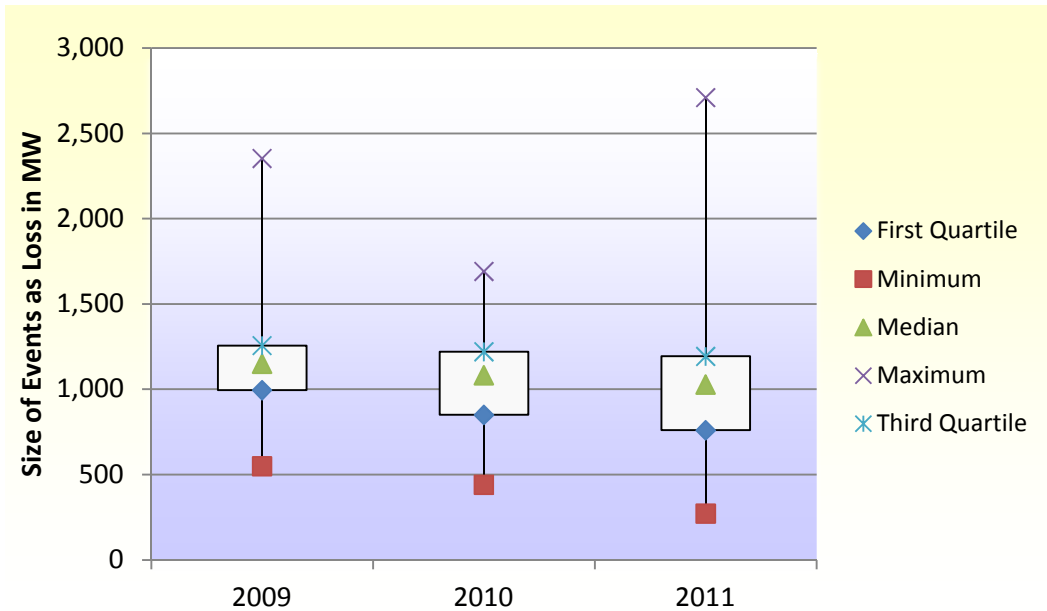
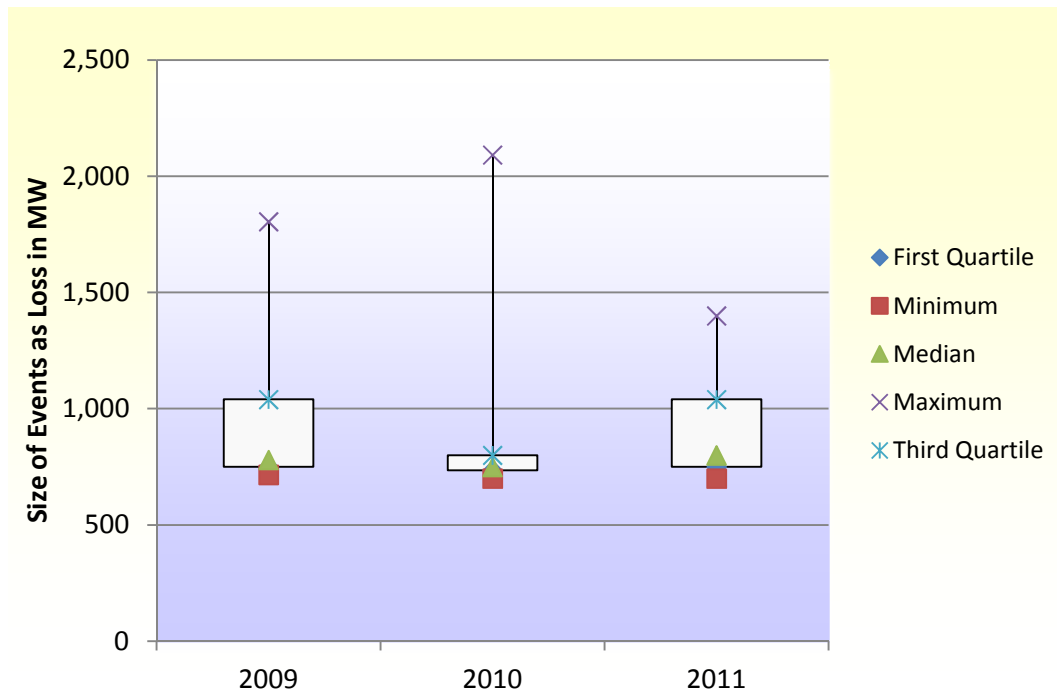
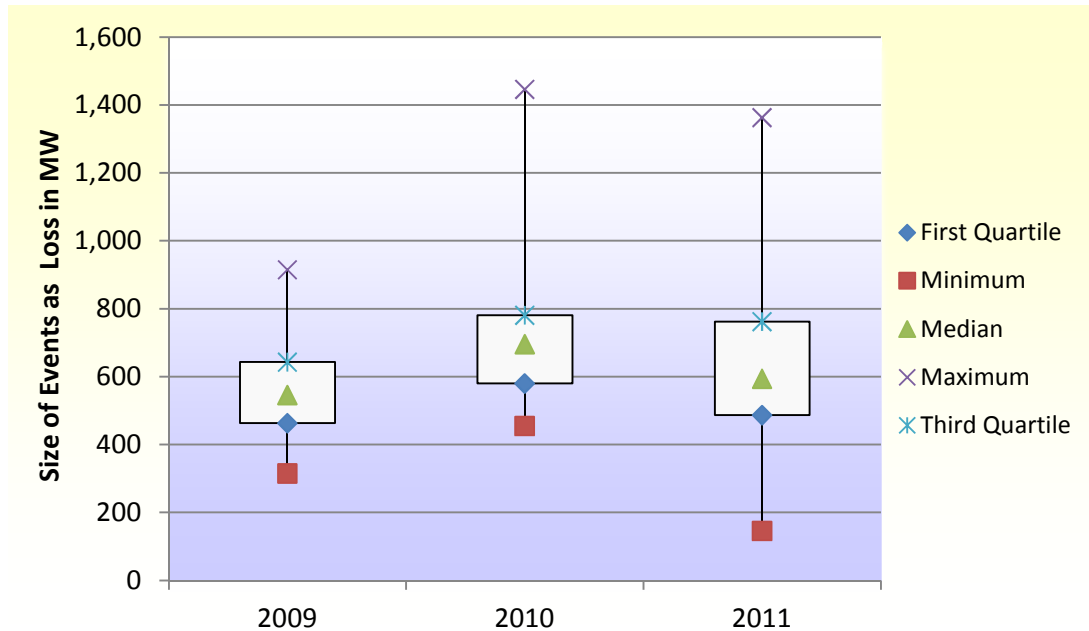
Figure 28: MW Loss Box Plot Analysis for 2009 to 2011 Eastern Interconnection Data**Figure 29: MW Loss Box Plot Analysis for 2009 to 2011 Western Interconnection Data**

Figure 30: MW Loss Box Plot Analysis for 2009 to 2011 ERCOT Interconnection Data***Special Considerations***

There are multiple special considerations in interpreting the data from each event and the calculated Frequency Response performance. The net MW⁵⁶ change to the interconnection versus the capacity of the unit or gross output at the time of the trip is a common reporting error. The process involves manual data collection with multiple handoffs which could result in data transcription errors. Also, in larger interconnections, multiple, nearly simultaneous frequency related events could occur such as multiple generator trips, coincident pumped storage shift from pumping to generating, or a large non-conforming load may cycle on and off. The interaction of these events can drastically alter the calculation of the Frequency Response and must all be addressed. A similar issue is only having one Balancing Authority's share of a Jointly Owned Unit reported as the net MW loss. If one only captures one of the multiple events, one significantly understates or overstates the primary Frequency Response. In summary, one can have high confidence in the median and mean with such a large set of data.

In the WI, Remedial Action Schemes can result in large generation shedding events in which the response is deliberately suppressed. Any extremes should be interpreted with some caution. Additional improvements to the frequency event detection and reporting procedure are proposed to the Frequency Working Group to handle these special cases in order to improve the quality and consistency of this metric.

As a general practice, if a frequency excursion event is recorded in the EI with less than 1,500 MW/0.1 Hz Frequency Response, the event merits further analysis to determine the cause of the low calculated response. There is a good possibility in such cases of a coincident event or a data collection error. Although each NERC Interconnection is inherently different, they share

⁵⁶ Frequency Response events include loss of load or large shifts in pumped storage pumping loads.

similar operating challenges from season to season. Sharing these experiences and subsequent lessons learned with the industry can be helpful in developing solutions to mitigate or otherwise prevent future reliability issues related to Frequency Response.

ALR Characteristic: Contingencies

ALR1-4 BPS Transmission Related Events Resulting in Loss of Load

Background

This metric measures bulk power system transmission-related events resulting in the loss of load, excluding weather-related outages. Planners and operators can use this metric to validate their design and operating criteria by identifying the number of instances when loss of load occurs.

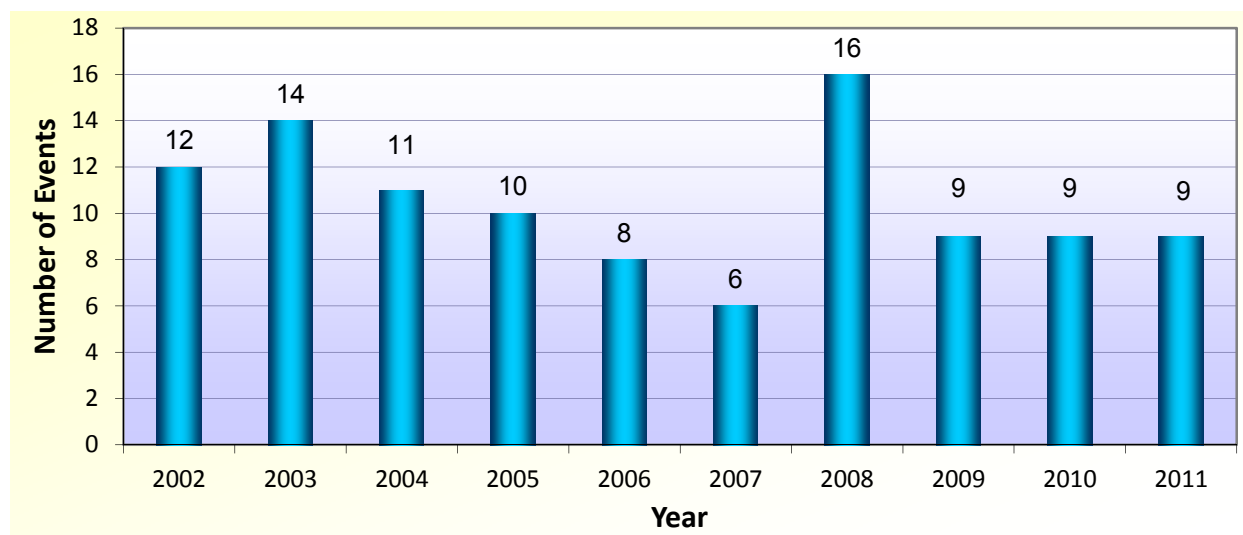
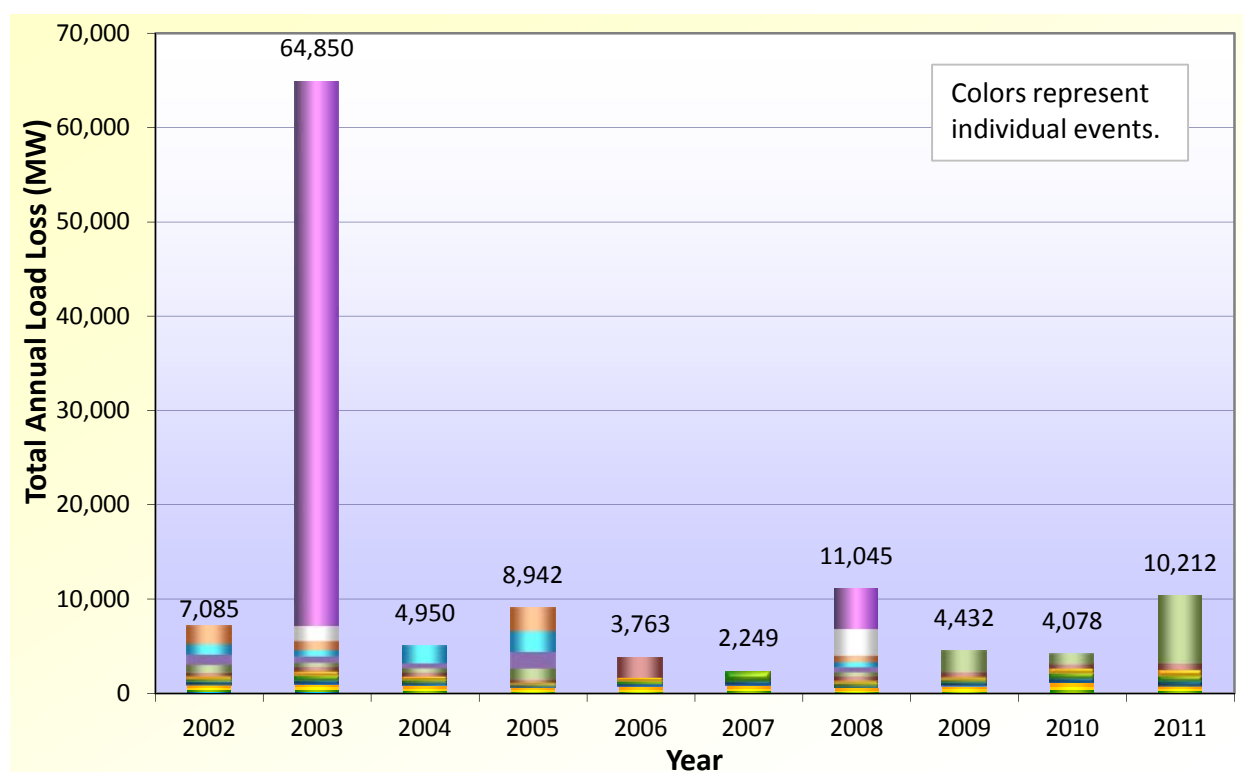
For the purposes of this metric, an “event” is an unplanned transmission disturbance that produces an abnormal system condition due to equipment failures or system operational actions, and results in the loss of firm system demand for more than 15 minutes. The reporting criteria for such events are outlined below:⁵⁷

- Entities with a previous year recorded peak demand of more than 3,000 MW are required to report all such losses of firm demand totaling more than 300 MW.
- All other entities are required to report all such losses of firm demands totaling more than 200 MW or 50 percent of the total customers being supplied immediately prior to the incident, whichever is less.
- Firm load shedding of 100 MW or more used to maintain the continuity of the bulk power system reliability.

Assessment

Figure 31 illustrates that the number of bulk power system transmission-related events resulting in loss of firm load from 2002 to 2011 is relatively constant. On average, eight to 10 events are experienced per year. The top three years in terms of load loss are 2003, 2008, and 2011 as shown in Figure 32. In 2003 and 2011, one event accounted for over two-thirds of the total load loss while, in 2008, a single event accounted for over one-third of the total load loss. Further analysis and continued assessment of the trends over time is recommended.

⁵⁷ Details of event definitions are available at: <http://www.nerc.com/files/EOP-004-1.pdf>.

Figure 31: ALR1-4 BPS Transmission Related Events Resulting in Load Loss (2002-2011)**Figure 32: Bulk Power System Transmission Related Event Related Loss of Load (2002-2011)*****Special Considerations***

The collected data does not indicate whether load loss, during an event, occurred as designed or not as designed. Further investigation into the usefulness of separating load loss as designed and unexpected load loss should be conducted. Also, differentiating between load loss as a direct consequence of an outage compared to load loss as a result of operation action to mitigate an IROL/SOL exceedance should be investigated.

ALR2-4 Average Percent Non-Recovery of Disturbance Control Standard Events

Background

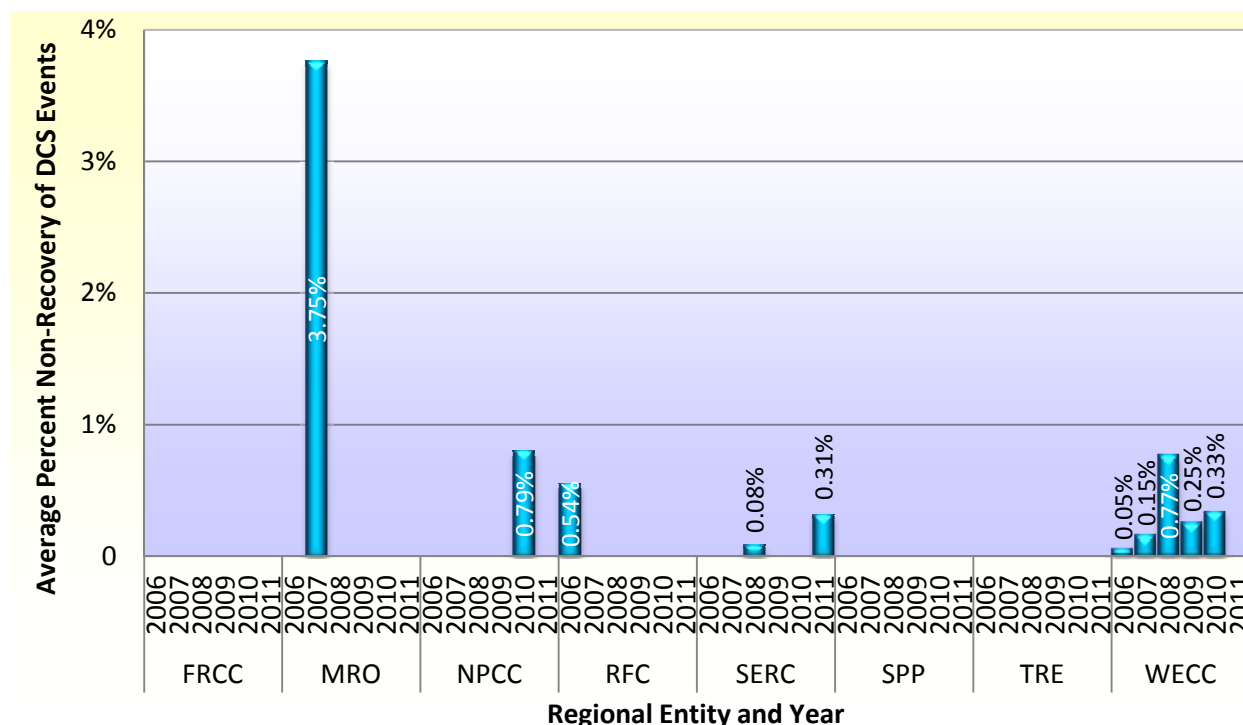
This metric measures the Balancing Authority's or Reserve Sharing Group's (RSG) ability to balance resources and demand with the timely deployment of contingency reserve, thereby returning the Interconnection frequency to within defined limits following a Reportable Disturbance.⁵⁸ The relative percentage provides an indication of performance measured at a Balancing Authority or RSG level.

Assessment

Figure 33 illustrates the average percent non-recovery of Disturbance Control Standard (DCS) events from 2006 to 2011. The graph provides a high-level indication of the performance of each Balancing Authority or RSG within the different Regional Entities. However, a single event may not reflect all the reliability issues within the given Region. In order to understand the reliability aspects, it may be necessary to request individual Regional Entities to further investigate and provide a more comprehensive reliability report. Further investigation may indicate that sufficient contingency reserves were available, but, through their implementation process, failed to meet DCS recovery.

Continued trend assessment is recommended. Where trends indicated potential issues, the Regional Entity will be requested to investigate and report their findings.

Figure 33: Average Percent Non-Recovery of DCS Events by Regional Entity and Year



⁵⁸ Details of the Disturbance Control Performance Standard and Reportable Disturbance definitions are available at: <http://www.nerc.com/files/BAL-002-0.pdf>.

Special Considerations

This metric aggregates the number of events based on reporting from individual Balancing Authorities or RSGs. It does not capture the severity of the DCS events. Most Regional Entities use 80 percent of the Most Severe Single Contingency to establish the minimum threshold for reportable disturbance, while others use 35 percent.⁵⁹

ALR2-5 Disturbance Control Events Greater Than Most Severe Single Contingency

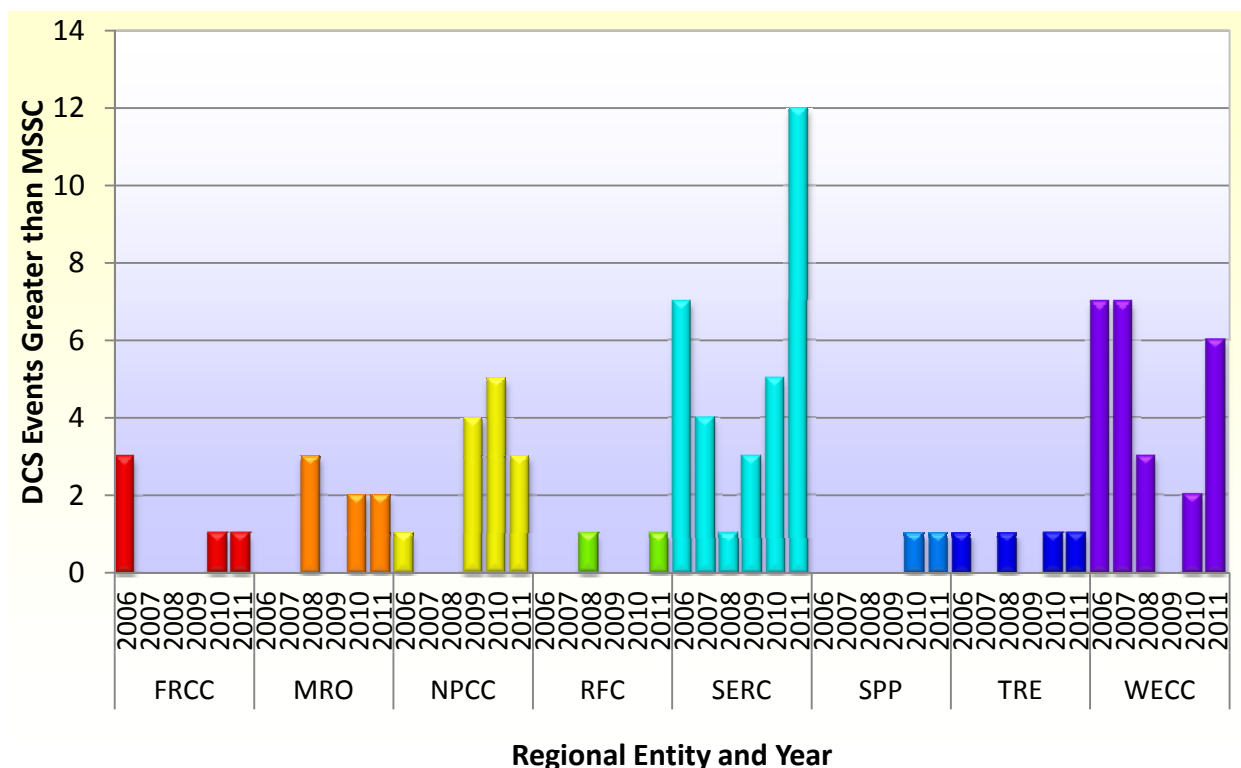
Background

This metric represents the number of disturbance events that exceed the Most Severe Single Contingency (MSSC) and is specific to each Balancing Authority or RSG. Each Balancing Authority reports disturbances greater than the MSSC on behalf of the Balancing Authority or RSG. The MSSC is determined based on the specific configuration of each Balancing Authority or RSG and can vary in significance and impact on the bulk power system.

Assessment

Figure 34 represents the number of DCS events within each Regional Entity that are greater than the MSSC from 2006 to 2011. This metric and any resulting trends could provide insight regarding the risk of events greater than the MSSC on adequate operating reserves or the frequency control performance.

Figure 34: Disturbance Control Events Greater Than Most Severe Single Contingency by Regional Entity and Year (2006-2011)



⁵⁹ <http://www.wecc.biz/Standards/Development/Lists/Request%20Form/DispForm.aspx?ID=69&Source=/Standards/Development/Pages/WECCStandardsArchive.aspx>

Special Considerations

The metric reports the number of DCS events greater than MSSC, most severe single contingency, without regards to the size of a Balancing Authority or RSG and without respect to the number of reporting entities within a Regional Entity. Because of the potential for differences in the magnitude of MSSC and the resultant frequency of events, trending should be conducted within each Regional Entity to provide any potential reliability indicators. Each Regional Entity should investigate the cause and relative effect on reliability of the events within their footprints.

A small Balancing Authority or RSG may have a relatively small MSSC. As such, a high number of DCS events greater than MSSC may not indicate a reliability problem for the reporting Regional Entity, but may indicate an issue for the respective Balancing Authority or RSG. In addition, events greater than MSSC may not cause a reliability issue for a BA, RSG or Regional Entity if they have more stringent standards which require contingency reserves greater than MSSC.

ALR Characteristic: Integrity**ALR3-5 Interconnection Reliability Operating Limit/ System Operating Limit (IROL/SOL) Exceedances*****Background***

This metric measures the number of times that a defined Interconnection Reliability Operating Limit (IROL) or System Operating Limit (SOL) was exceeded and the duration of these events. Exceeding IROL/SOLs could lead to outages if prompt operator control actions are not taken to return the system to within normal operating limits. Also, exceeding the limits may not directly lead to an outage, but it puts the system at unacceptable risk if the operating limits are exceeded beyond T_v .⁶⁰

With the Operating Reliability Subcommittee's and former Reliability Coordinator Working Group's technical support, this metric was endorsed by NERC's Operating and Planning Committees in June 2010 and a data request was subsequently issued in August 2010. The reporting of IROL/SOL exceedances became mandatory in 2011. While the IROL is used in the Eastern, ERCOT and Québec Interconnections, there are no pre-identified IROLs in the Western Interconnection.

Assessment

Figure 35 and Figure 36 show the number of IROL/SOL exceedances separated by quarter and duration for the Eastern and Western Interconnections, respectively. The second quarter of 2011 shows the most exceedances for the Eastern Interconnection. For the Western Interconnection, the third and fourth quarter of 2011 show a marked increase in the number of SOL exceedances that lasted between 10 seconds and 10 minutes. There is insufficient data to assess any trends in IROL/SOL exceedances.

⁶⁰ T_v is the maximum time that an Interconnection Reliability Operating Limit can be violated before the risk to the interconnection or other Reliability Coordinator Area(s) becomes greater than acceptable. Each Interconnection Reliability Operating Limit's T_v shall be less than or equal to 30 minutes.

**Figure 35: 2011 Eastern Interconnection ALR3-5 IROL Exceedances
by Quarter and Duration**

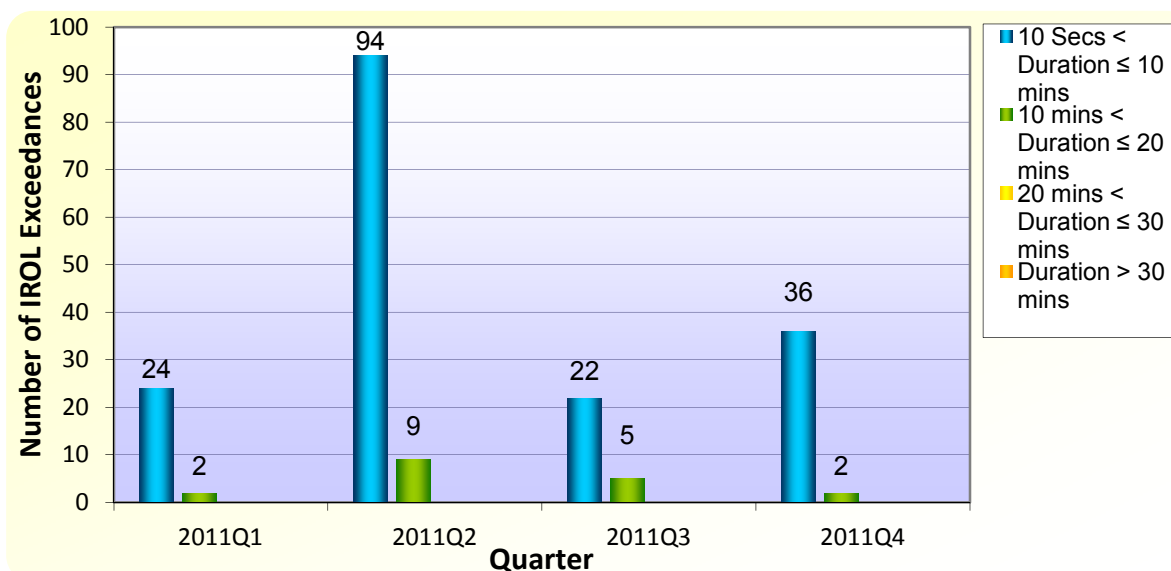


**Figure 36: Western Interconnection ALR3-5 SOL Exceedances
by Quarter and Duration**

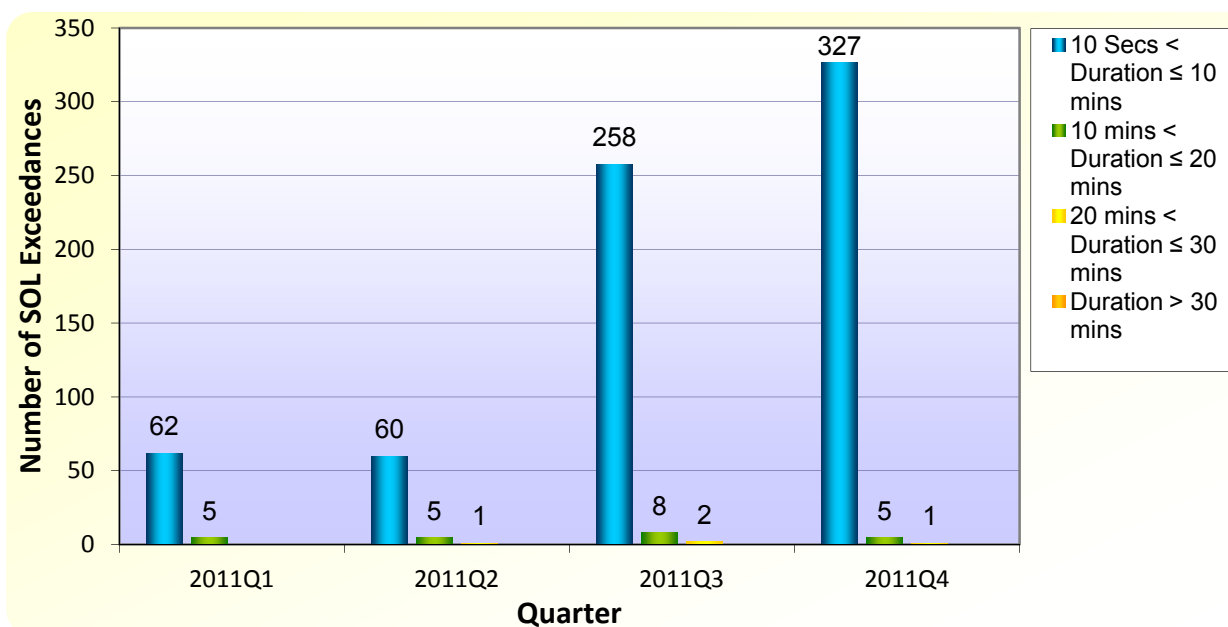
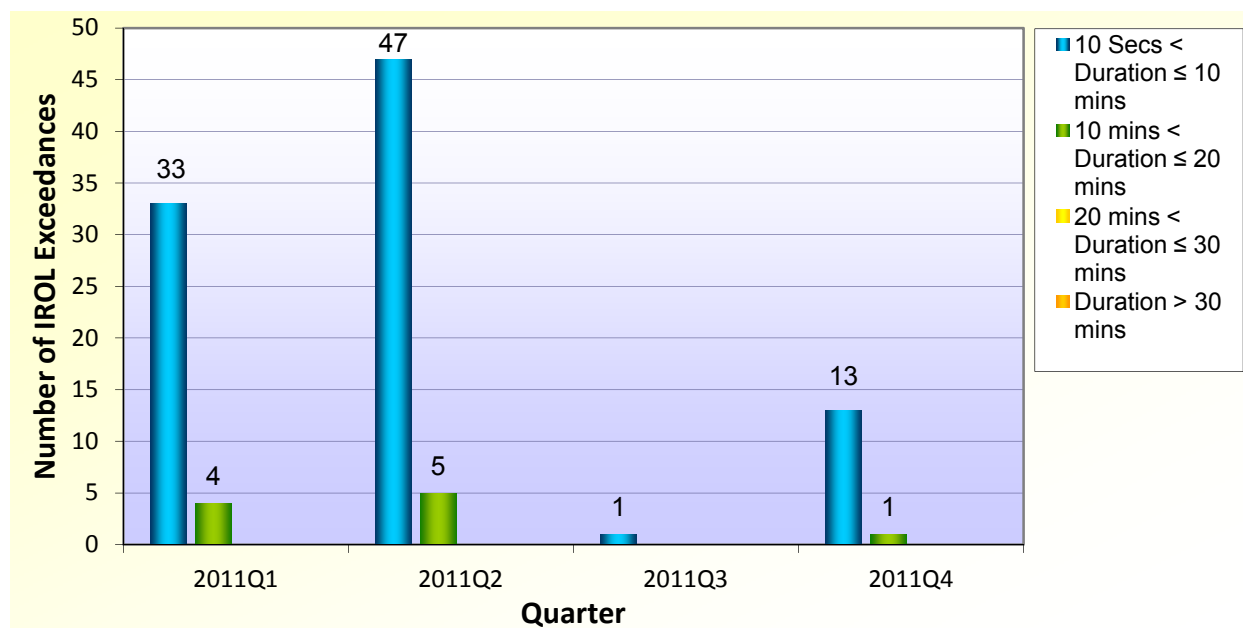


Figure 37: ERCOT Interconnection ALR3-5 IROL Exceedances by Quarter and Duration (2011)

ALR Characteristic: Protection

ALR2-3 Activation of Under Frequency Load Shedding

Background

The purpose of Under Frequency Load Shedding (UFLS) is to balance generation and load when an event causes a significant drop in frequency of an interconnection or islanded area. The UFLS activation metric measures the number of times it is activated and the total MW of load interrupted in each Regional Entity and NERC-wide.

Assessment

Table 11 illustrates a history of UFLS events from 2001 through 2011. Notably, single events had a load shedding range from 24 MW to 17,644 MW. The activation of UFLS is the last automated reliability measure associated with a decline in frequency in order to rebalance the system. Further assessment of the MW loss for these activations is recommended.

Because of the large range of load lost in UFLS events, the need to establish a UFLS total load loss threshold is under evaluation. The significance of a UFLS activation compared to the total activation load loss will be assessed over time.

Table 11: ALR2-3 Under Frequency Load Shedding MW Loss⁶¹

	2003	2004	2005	2006	2007	2008	2009	2010	2011
FRCC						1,273			
MRO					486				
NPCC	17,644	24				48			
RFC	6,105								176
SPP						673 (2 Events)			
SERC									
TRE	1,549								
WECC									

ALR4-1 Automatic AC Transmission Outages Caused by Protection System Equipment-Related Misoperations

Background

Originally titled *Correct Protection System Operations*, this metric has undergone a number of changes since its initial development. To ensure that it best portrays how misoperations affect transmission outages, it was necessary to establish a common understanding of misoperations and the data needed to support the metric. NERC's ERO-Reliability Assessment and Performance Analysis (ERO-RAPA) group evaluated several options of transitioning from existing procedures for the collection of misoperations data to a consistent approach which was introduced at the beginning of 2011. With the NERC System Protection and Control Subcommittee's (SPCS) technical guidance, NERC and the Regional Entities have agreed upon a set of specifications for misoperations reporting including format, categories, event cause codes, and reporting period to have a final, consistent reporting template.⁶² Based on the standardized misoperations reporting, two quarters of data in 2011 have been collected.

To calculate the metric, the Transmission Availability Data System (TADS) is used to find the total number of automatic outages. Currently, TADS only collects data for transmission outages on elements greater than 200 kV. Therefore, only automatic transmission outages 200 kV and above, including AC circuits and transformers, will be used in the calculation of this metric.

⁶¹ MW loss due to Under Frequency Load Shedding Misoperations have been removed from the Table. Except for SPP in 2008, all MW loss was in a single UFLS event.

⁶² The current Protection System Misoperations template is available at:
http://www.nerc.com/docs/pc/rmwg/Protection_System_Misoperation_Reporting_Template_Final.xlsx.

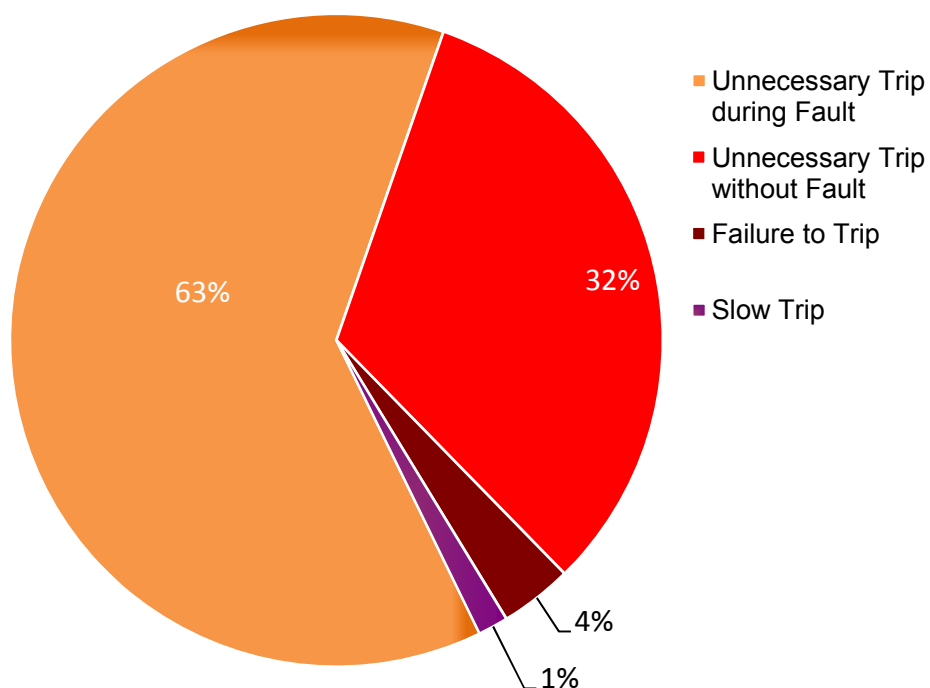
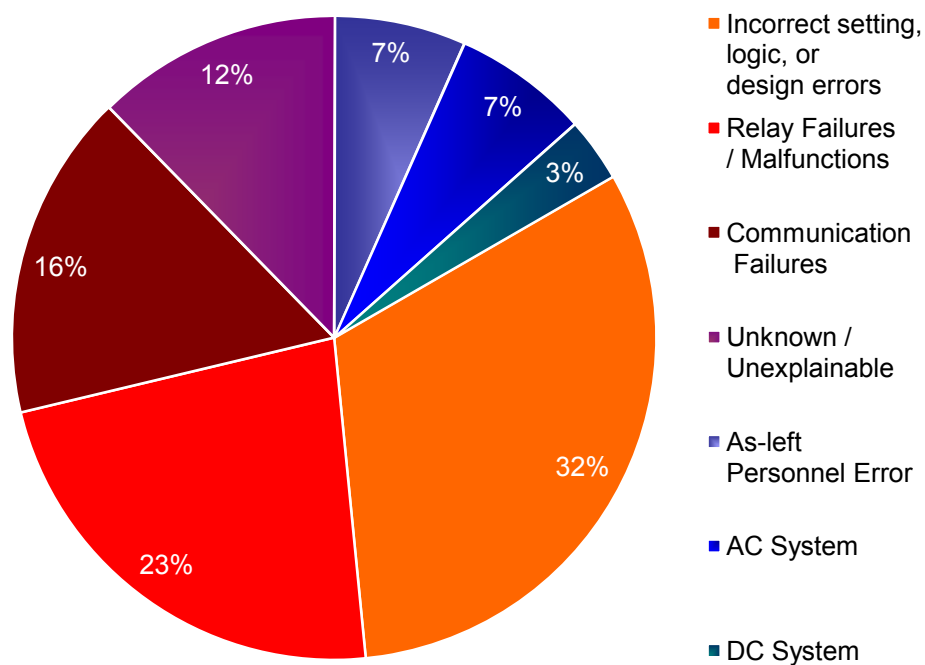
Assessment

Currently, efforts are underway to reconcile misoperation reporting with TADS event reporting. Therefore, the values for this metric are based on preliminary, not final data. However, based on the preliminary misoperations reporting, some observations can be made.

With less than a full year's data, a full assessment for protection system misoperation trending is not possible. The decrease in misoperations from the second to third quarter, as shown in Table 12, is notable, and a year-to-year quarterly comparison would provide a better insight into how the numbers of misoperations are changing over time.

Table 12: Protection System Misoperations by Regional Entity and Quarter		
Regional Entity	2011Q2 Misoperations	2011Q3 Misoperations
FRCC	23	18
MRO	77	51
NPCC	45	52
RFC	170	141
SERC	209	68
SPP RE	115	68
TRE	70	28
WECC	114	87

Although it is too early to trend misoperation counts, there are other interesting observations. The vast majority of misoperations in both quarters, shown in Figure 38, are categorized as unnecessary trips. Also, Figure 39 illustrates the top three cause codes assigned to misoperations in both quarters: incorrect setting, logic, or design error; relay failures/malfunction; and communication failure. To further investigate the root causes of protection system misoperations, NERC's Planning Committee has formed a task force known as the Protection System Misoperation Task Force (PSMTF). The PSMTF will investigate protection system misoperations in order to improve performance and mitigate risks due to misoperations.

Figure 38: NERC-wide Misoperations by Category (2011Q2 and 2011Q3)**Figure 39: NERC-wide Misoperations by Cause Code (2011Q2 and 2011Q3)**

ALR Characteristic: Adequacy

ALR1-3 Planning Reserve Margin

Background

The Planning Reserve Margin⁶³ is a measure of the relationship between the amount of resource capacity forecast and the expected demand in the planning horizon.⁶⁴ Planning Reserve Margins have been used by system planners for decades as an industry standard indication of system resource adequacy.

Planning Reserve Margin is the difference between forecast capacity and projected peak demand (50/50 forecast⁶⁵), normalized as a percentage of projected peak demand. Based on experience, for portions of the bulk power system that are not energy-constrained, Planning Reserve Margin indicates the amount of capacity available to maintain reliable operation, while meeting unforeseen increases in demand (e.g., extreme weather) and unexpected unavailability of existing capacity (e.g., long-term generation outages). Further, from a planning perspective, Planning Reserve Margin trends identify whether capacity additions are projected to keep pace with demand growth.

The North American bulk power system is divided into four distinct Interconnections. These Interconnections are loosely connected with limited ability to share capacity or energy across the Interconnections. To reflect this limitation, the Planning Reserve Margins are calculated in this report based on Interconnection values rather than by national boundaries as is the practice of the NERC Reliability Assessment Subcommittee (RAS).

Assessment

Planning Reserve Margins, considering anticipated capacity resources and adjusted potential capacity resources,⁶⁶ decrease in the latter years of the 10-year forecasts in each of the four Interconnections for both the 2010⁶⁷ and 2011 resource projections. Typically, the early years provide more certainty since new generation is either in-service or under construction with firm commitments. In the later years, there is less certainty about the resources that will be needed to meet peak demand. Therefore, declining Planning Reserve Margins are expected in a conventional forecast (assuming load growth) and do not necessarily indicate a trend of a degrading resource adequacy. Rather, they are an indication of the potential need for additional resources. In addition, key observations can be made about the Planning Reserve Margin forecast, such as short-term assessment comparison to target margins, rate of margin change through the assessment period, identification of margins that are approaching or below a target requirement, and comparisons from year-to-year forecasts.

⁶³ Detailed calculations of Planning Reserve Margin are available at: <http://www.nerc.com/page.php?cid=4|331|333>.

⁶⁴ The Planning Reserve Margin indicated here is not the same as an operating reserve margin that system operators use for near-term operations decisions.

⁶⁵ These demand forecasts are based on methods used in the 2011 Long Term Reliability Assessment, pp. 43-44.

⁶⁶ Please see 2011 Long-Term Reliability Assessment, http://www.nerc.com/files/2011%20LTRA_Final.pdf, pp. 356-396 for definitions.

⁶⁷ 2010 Long-Term Reliability Assessment, http://www.nerc.com/files/2010_LTRA_v2-.pdf.

While resource planners are able to forecast the need for resources, the type of resource that will actually be built or acquired to fill the need is less certain. For example, in the northeast U.S. markets, with a three to five year forward capacity market, firm commitments are not made in the long-term. Proposed resources are included in a generator interconnection queue in order to study the potential transmission requirements for facility interconnection. Since much of the generation in an interconnection queue will not be constructed as originally proposed, these queues are then adjusted to reflect a forecast of resources. The adjustment can reduce the forecast of new generation to 20 percent or less of the capacity rating in the queue, depending on the assessment area.

In the Eastern Interconnection, planning reserve margins were on the rise between 2008 and 2010 as shown in Figure 40. However, the 2011 forecast shows a decrease when compared to last year's forecast. Since the demand forecast is in line with last year's forecast, the decrease indicates a decreased supply projection. While the 2011 reserve margin forecast stays above the 15 percent NERC reference reserve margin and does not indicate major supply issues at this time.

A decrease in projected future and conceptual generation resources leads to declining Planning Reserve Margins in some areas. Declining resource adequacy in the ERCOT Interconnection is somewhat of a concern. However, the majority of areas appear to have adequate resource plans to meet projected peak demands.⁶⁸

This conclusion results from slightly higher capacity forecasts and slightly lower demand forecasts. Importantly, the pace of any economic recovery will affect future comparisons.⁶⁹ This metric can be used by NERC to assess the individual Interconnections in the ten-year long-term reliability assessments. If a noticeable change occurs, further investigation is necessary to determine the causes and likely effects on reliability, and the potential need for additional resources.

The increase in 2011 Reserve Margin projections in the 2008 and 2009 Long-Term Reliability Assessments are primarily the result of different interpretations and modifications to the data request form, specifically for the CA-MX subregion, which had applied special conditions to the generation queue prior in 2008. In 2009, the entire generation queue was included, and this caused what appeared to be a jump in Future-Planned capacity projections. This change was to ensure WECC's data collection definitions were consistent with other Regions/Assessment Areas.

Special Considerations

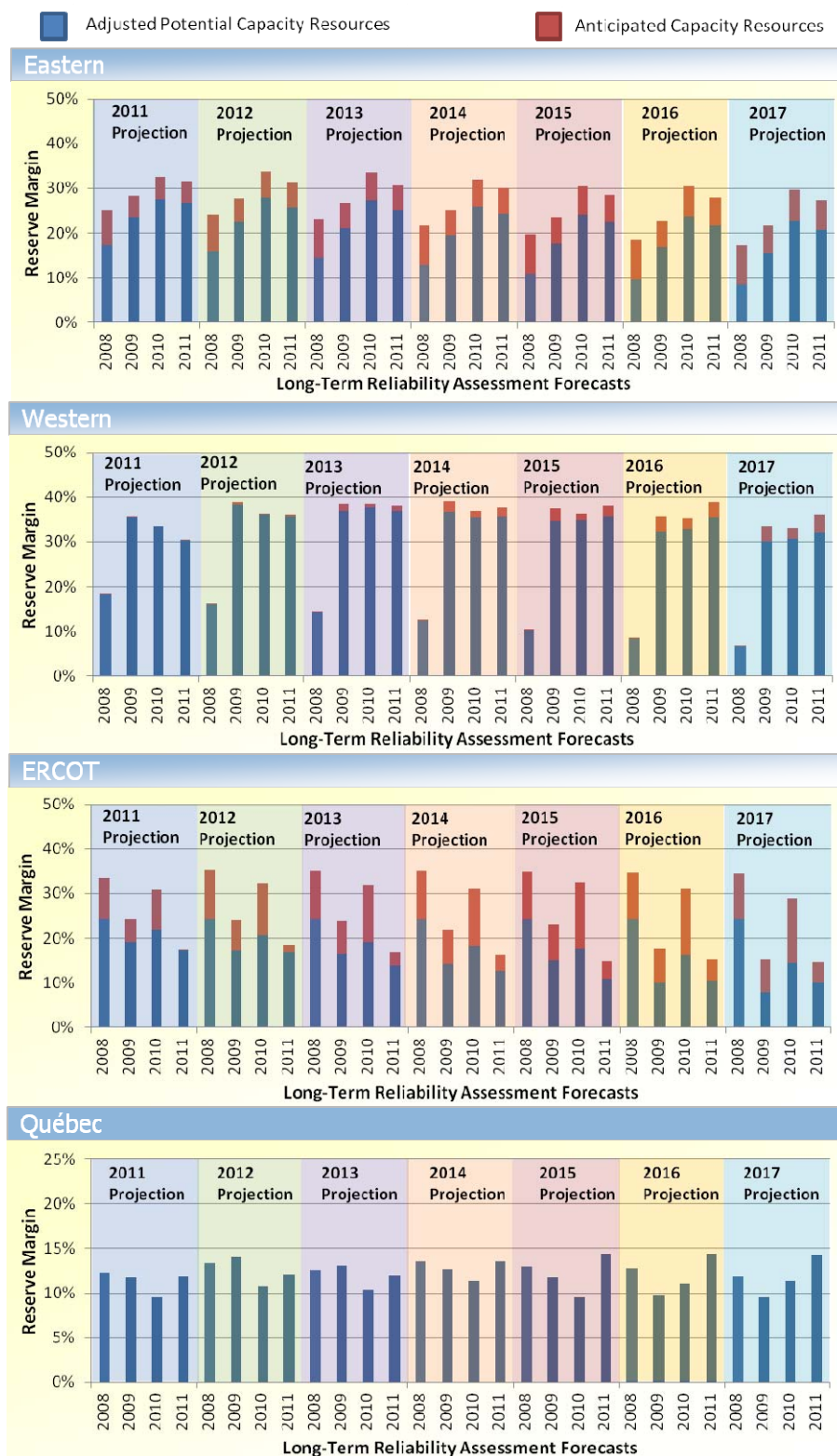
The Planning Reserve Margin is a capacity-based metric. Therefore, it does not provide as accurate assessment of performance in energy-limited systems (e.g., hydro capacity with limited water resources). Systems with significant penetration of variable generation or other

⁶⁸ 2011 Long Term Reliability Assessment, http://www.nerc.com/files/2011%20LTRA_Final.pdf, pp. 8-10.

⁶⁹ Potential Reliability Impacts of Swift Demand Growth after a Long-Term Recession, http://www.nerc.com/files/NERC_Swift_Scenario_Aug_2010.pdf.

resources that cannot be dispatched will need to review the equivalent capacity assigned to these non-traditional resources.

Figure 40: ALR1-3 2011 Planning Reserve Margin by Interconnection and Year



ALR6-1 Transmission Constraint Mitigation

Background

The intent of this metric is to identify trends in the number of mitigation measures (Special Protection Schemes (SPS), Remedial Action Schemes (RAS), and Operating Procedures) required to meet Transmission Planning (TPL)⁷⁰ reliability requirements. By their nature, SPSs and RASs do not indicate an inherent weakness in the bulk power system. However, SPSs and RASs do indicate that in some operating scenarios there may be corrective actions required to maintain a reliable operating state.

For ALR6-1 SPS and RAS counts, the Regional Entities report the total number of SPS or RAS involving systems or system elements at 100 kV or greater (or the bulk electric system as defined by the Regional Entity) as recorded in the respective Regional Entity's SPS database. This database is established according to the PRC-013-000 standard, Special Protection System Database. Data for future planning years may be obtained from TPL studies.⁷¹ The following types of systems should be reported:

- Generation rejection or reduction schemes;
- Load rejection schemes;
- Line tripping schemes;
- Acceptable voltage and power flow adjustment schemes; and
- And all schemes necessary to meet the requirements of the TPL-001 to TPL-004 standards.

No SPS should be reported where it is installed solely for economic purposes. Also, Under Voltage Load Shedding, UVLS, or UFLS, installations should not be reported.

The operating procedures counts are the total number of operating procedures involving systems or system elements at 100kV or greater (or the bulk electric system as defined by the Region) as recorded in the planning studies aggregated at a regional level. The operating procedures are also called remedies as included in the planning studies to ensure performance per the TPL series of standards. The following types of operating procedures performed on the bulk electric system are including in ALR6-1:

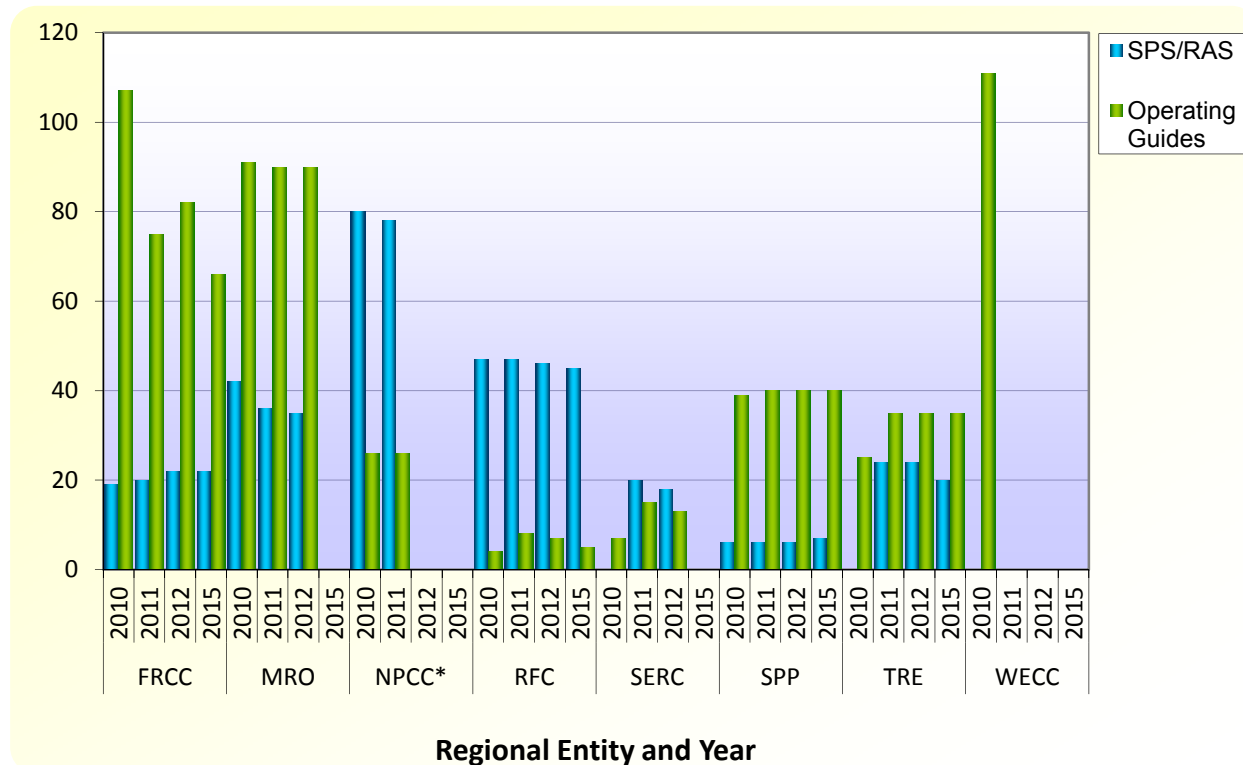
- Generation reduction or redispatch procedures;
- Opening breaker(s) to sectionalize portions of the transmission system; and
- Other operator actions required to return equipment loadings and system voltages within planning reliability criteria.

Assessment

As shown in Figure 41 per Regional Entity, there is a relatively constant number of regional mitigation measure plans over the data collection time period.

⁷⁰ <http://www.nerc.com/files/TPL-005-0.pdf>

⁷¹ Other data source for planning years includes the Transmission Planner's or Planning Coordinator's FERC Form 715 filing.

Figure 41: ALR6-1 Transmission Constraint Mitigation Count by Regional Entity and Year

**NPCC separates Special Protection Schemes into 3 distinct types.⁷²*

Special Considerations

This metric is only intended to evaluate the trend in the future use of these plans, and whether the metric indicates robustness of the transmission system is increasing, remaining static, or decreasing. A certain number of SPS mitigation plans may be necessary to support reliable operation of the system. An increase of SPSs may indicate additional transmission capacity is required. Correspondingly, a reduction in the number of SPSs may be an indicator of increased generation or transmission facilities being placed in-service, which may imply greater robustness of the bulk power system.

At this time, identifying the number of operating procedures is still a manual process and prone to error. One procedure may be provided for multiple contingencies. No automatic tool is available to avoid double counting of the procedures.

In general, mitigation plans are a viable, effective tool for the bulk power system operation. In power system planning, reliability, operability, capacity and cost-efficiency are simultaneously considered through a variety of system scenarios. Mitigation measures are a method for optimizing a power system across these scenarios.

⁷² <https://www.npcc.org/Standards/Directories/NPCC%20Directory%207%20-%20Special%20Protection%20System%20RCC%20Endorsed%20Nov%2028%202007rev4--new%20NERC%20hyperlinks.pdf>

ALR6-2 Energy Emergency Alert 3 (EEA3)

Background

This metric identifies the number of times Energy Emergency Alert Level 3 (EEA3) is issued. EEA3 events are firm-load interruptions imminent or in progress due to capacity and/or energy deficiencies. EEA3 events are currently reported, collected and maintained in NERC's Reliability Coordinator Information System (RCIS), defined in the NERC Standard EOP-002.⁷³ The number of EEA3s per year provides a relative indication of performance measured at a Balancing Authority or Interconnection level. As historical data is gathered, trends provide an indication of either decreasing or increasing use of EEA3s, signaling real-time adequacy of the electric supply system. This metric can also be considered in the context of the Planning Reserve Margin. Significant increases or decreases in EEA3 events with relatively constant ALR1-3 Planning Reserve Margins could indicate changes in the adequacy of the bulk power system requiring review of resources. However, lack of fuel and dependence on transmission for imports into constrained areas can also contribute to increased EEA3 events.

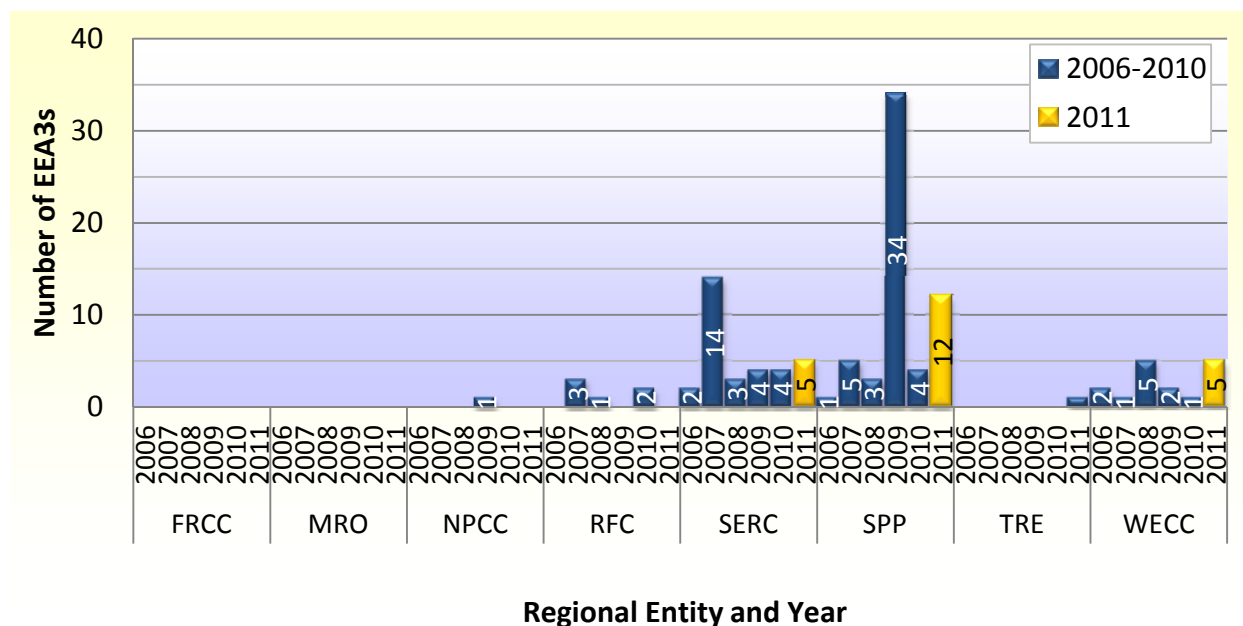
Assessment

Figure 42 shows the number of EEA3 events from 2006 to 2011 at a Regional Entity level. An interactive presentation is available at the Reliability Indicator's page.⁷⁴ Due to the large number of EEA3s in the Acadiana Load Pocket (ALP) region, the SPP RC coordinated an operating agreement in 2009 with the five operating companies in the ALP to improve reliability performance as an interim step while a \$200 million transmission construction program was initiated by Cleco Power, Entergy, and Lafayette Utilities. The addition of two 230 kV lines, one in spring 2011 and another in fall 2011, alleviated a portion of the most limiting elements. An additional 230 kV line was energized in February 2012 and two other 230 kV lines are expected to be energized by the summer of 2012. Completion of these projects should further alleviate transmission congestion in this area and will conclude the planned ALP projects.

SPP RTO continues to coordinate operating plans with the operating entities in this area. Mitigation plans and local operating guides in place are expected to provide sufficient flexibility should issues arise. NERC will continue to monitor this area for reliability impacts and coordinate any actions with the SPP Reliability Coordinator and SPP Regional Entity.

⁷³ The latest version of EOP-002 is available at: http://www.nerc.com/files/EOP-002-3_1.pdf.

⁷⁴ The EEA3 interactive presentation is available on the NERC website at: <http://www.nerc.com/page.php?cid=4|331|335>.

Figure 42: ALR6-2 Energy Emergency Alert 3 (EEA3) by Regional Entity and Year (2006-2011)***Special Considerations***

The need to include the magnitude and duration of the EEA3 declarations in this metric is under evaluation.

ALR6-3 Energy Emergency Alert 2 (EEA2)***Background***

The Energy Emergency Alert 2 (EEA2) metric measures the number of events declared for deficient capacity and energy during peak load periods. The number of EEA2 events, and any trends in their reporting, indicates how robust the system is in supplying aggregate load requirements. The EEA2 declarations may also serve as a leading indicator of energy and capacity shortfall in the adequacy of the electric supply system. EEA2 declarations provide a sense of the frequency of precursor events to more severe EEA3 declarations. This metric measures the number of events declared for deficient capacity and energy during peak load periods. At this time, however, this data reflects inclusion of demand side resources that would not be indicative of inadequacy of the electric supply system.

Demand response is a legitimate resource to be called and does not indicate a reliability concern. The historical record may include demand response activations and non-firm load interruptions, per applicable contracts, within the EEA alerts.⁷⁵ EEA2 events called solely for activation of demand response or interruption of non-firm load per applicable contracts should be excluded from this metric.

This metric can also be considered in the context of the planning reserve margin. Significant increases or decreases in EEA2 events with relatively constant planning reserve margins could

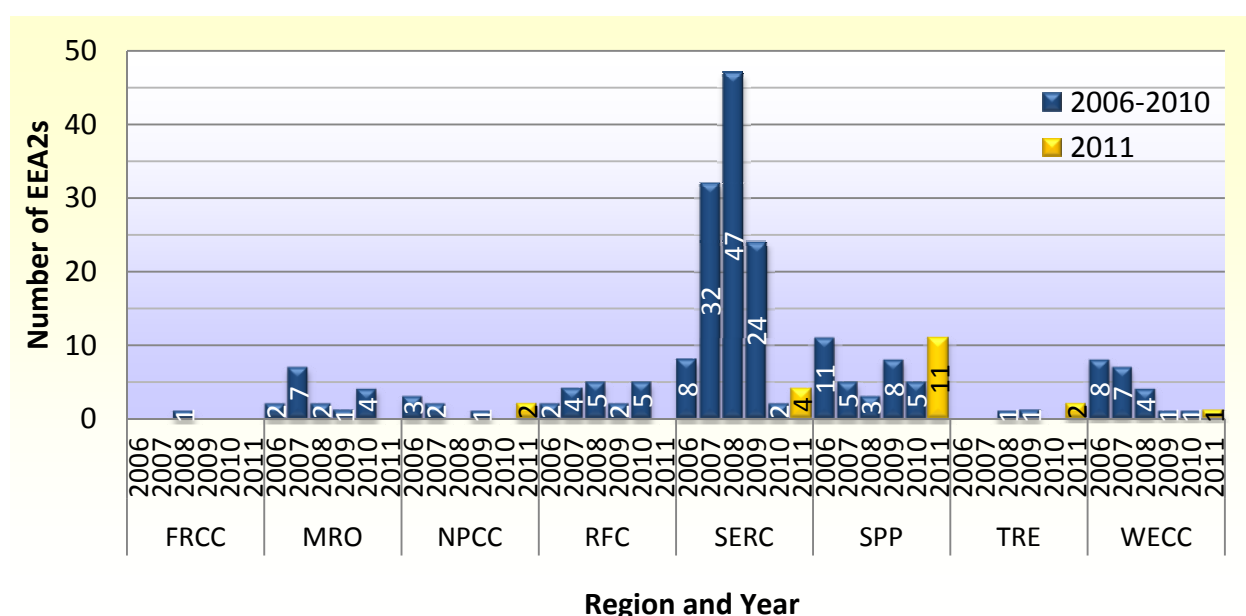
⁷⁵ The EEA2 is defined at <http://www.nerc.com/files/EOP-002-3.pdf>.

indicate volatility in the actual loads compared to forecasted levels or changes in the adequacy of the bulk power system required to meet load demands. As more data is gathered, there might be an indication of either decreasing or increasing adequacy in the electric supply system's Planning Reserve Margins.

Assessment

Figure 43 shows the number of EEA2 events within a Regional Entity from 2006 to 2010 from the EEA2 interactive reports available online.⁷⁶ The general trend continues to show improved performance which may have been influenced by the overall reduction in demand throughout NERC caused by the economic downturn.

Figure 43: ALR6-3 Energy Emergency Alert 2 (EEA2) by Regional Entity and Year (2006-2011)



There are two issues that should be assessed further for the EEA2 metric. To begin, specific performance for any one Region should be investigated for issues or events that may affect the results. Secondly, determining whether reported performance includes those events resulting from the economic operation of DSM and non-firm load interruption should also be investigated.

⁷⁶ EEA2 interactive version is located at: <http://www.nerc.com/page.php?cid=4|331|341>.

ALR6-11 – ALR6-14

ALR6-11	Automatic AC Transmission Outages Initiated by Failed Protection System Equipment
ALR6-12	Automatic AC Transmission Outages Initiated by Human Error
ALR6-13	Automatic AC Transmission Outages Initiated by Failed AC Substation Equipment
ALR6-14	Automatic AC Transmission Outages Initiated by Failed AC Circuit Equipment

Background

These metrics evolved from the original ALR4-1 metric for correct protection system operations and now illustrate a normalized count (on a per element basis) of AC transmission element outages (i.e., TADS momentary and sustained automatic outages)⁷⁷ that were initiated by: Failed Protection System Equipment, (ALR6-11); Human Error (ALR6-12); Failed AC Substation Equipment (ALR6-13); and Failed AC Circuit Equipment (ALR6-14). These metrics are all related to the non-weather related initiating cause codes for automatic outages of AC circuits and transformers operated 200 kV and above.

Assessment

Figure 44, Figure 45 and Figure 46 show the normalized automatic outages per AC circuit or per 100 circuit-miles and automatic outages per transformer for facilities operated at 200 kV and above. As shown in these charts, there are some regional trends in the four years of outage data. However, some Regional Entity values have increased from one year to the next, stayed the same, or decreased with no discernible regional trends.

In last year's annual report, confidence intervals were introduced as a means of weighing the significance of the data and trends. However, applying this confidence interval method to ALR6-11 to ALR6-14 raised the question whether the observable decreases or increases between three annual data points constituted a statistically significant trend. With the EIA's recommendations,⁷⁸ the TADSWG decided to use the Unpaired Poisson method to evaluate ALR6-11 to ALR6-14 in this report. A brief description and the assumptions used in the method are included in the Transmission Availability Analysis chapter of this report.⁷⁹

The statistical testing shows no significant trend changes in ALR6-11 to ALR6-14 performance during 2008 to 2011. In other words, whether observed year-to-year outage rates moved up or down is uncertain.

⁷⁷ Definitions for TADS outages are located on page 4 of <http://www.nerc.com/docs/pc/tadswg/Appendix%207%2020101202a%20clean.pdf>. TADS Initiating Cause Code definitions are located at: http://www.nerc.com/docs/pc/tadswg/TADS_Definitions_Appendix_7_092909.pdf.

⁷⁸ http://www.nerc.com/docs/pc/tadswg/07_agenda%20item%20EIA%20Memo.pdf

⁷⁹ To evaluate annual changes in the metrics, NERC wide metrics ALR6-11 – ALR6-14 for Single Mode Outages of AC Circuits only were analyzed using the Unpaired Poisson method. This method makes the following assumptions:

1. Assume the outages for each circuit in year 1 comes from identical but independent Poisson distributions.
2. Assume the outages for each circuit in year 2 comes from identical but independent Poisson distributions.
3. Assume the number of outages in year 1 and the numbers of outages in year 2 are independent.

ALR 6-11 – Automatic Outages Initiated by Failed Protection System Equipment

Figure 44 shows the automatic outages with an initiating cause code of failed protection system equipment. This code covers automatic outages initiated by any relay and/or control misoperations except those that are initiated by incorrect relay settings or design logic errors.

Figure 44: ALR6-11 Automatic Outages Initiated by Failed Protection System Equipment by Regional Entity (Includes NERC-Wide)



**Note: TRE has no transformers with low-side voltages at 200 kV and above.*

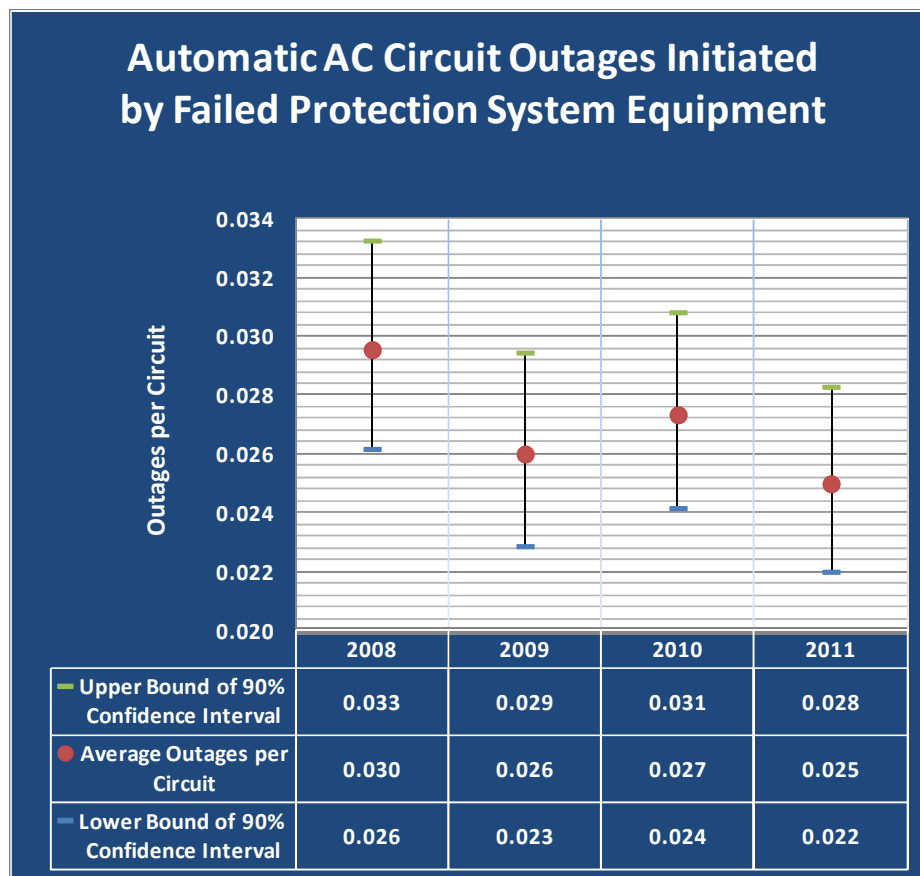
***Note: MRO has no transformer outage occurrences.*

As depicted Figure 45 and Figure 46, NERC-wide analysis of Single Mode Automatic AC Circuit Outages per circuit Initiated by Failed Protection System Equipment (ALR 6-11) using the Unpaired Poisson method shows that there is no statistically significant change from 2008 to 2011.

Figure 45: NERC Single Mode AC Circuit Outages Year to Year Comparison for ALR6–11

	2009-2008	2010-2009	2010-2008	2011-2008	2011-2009	2011-2010
Estimated Mean Percent Change in Number of Outages per Year per Circuit	-12%	5%	-7%	-15%	-4%	-9%
Significance of Mean Change in Number of Outages per Year per Circuit	NS	NS	NS	NS	NS	NS

Key to Significance Labels	
NS	Not Significant
*	90% Confident

Figure 46: NERC Single Mode AC Circuit Unpaired Poisson Analysis for ALR6-11

ALR6-12 – Automatic Outages Initiated by Human Error

Figure 47 shows the automatic outages with an initiating cause code of human error. This code covers automatic outages caused by any incorrect action traceable to employees and/or contractors for companies operating, maintaining, and/or providing assistance to the Transmission Owner.

Figure 47: ALR6-12 Automatic Outages Initiated by Human Error by Regional Entity (Includes NERC-wide)



*Note: TRE has no transformers with low-side voltages at 200 kV and above.

**Note: SPP has no transformer outage occurrences.

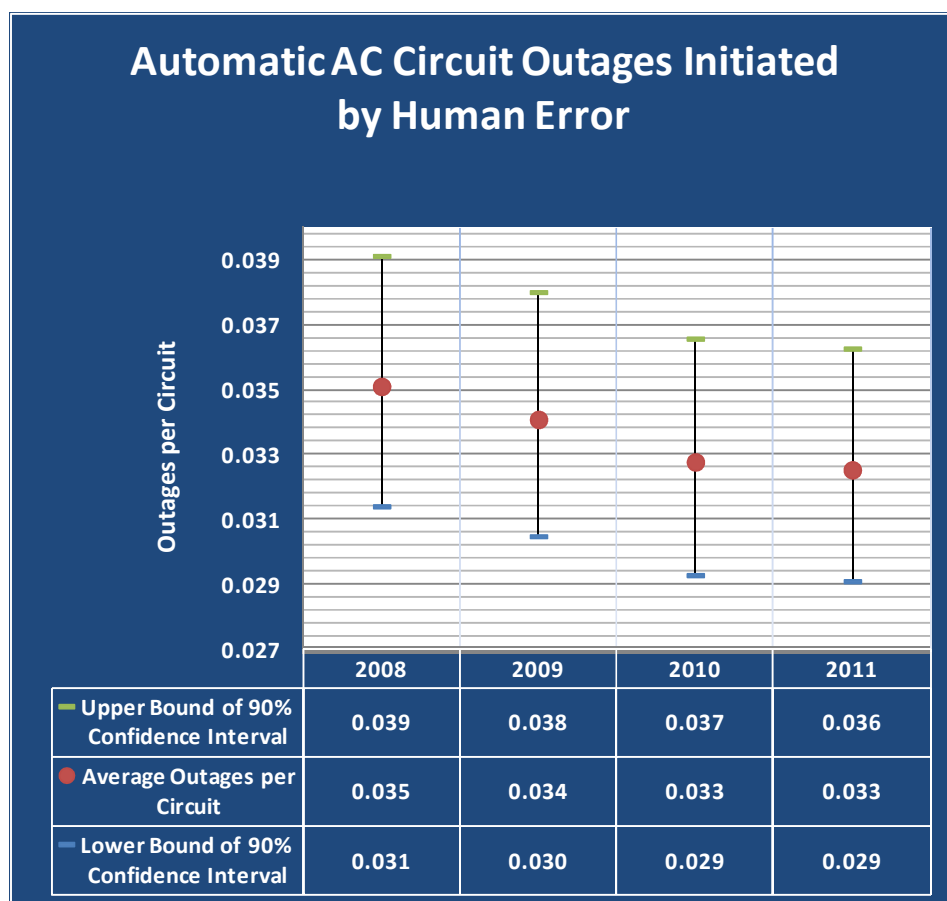
As depicted in Figure 48 and Figure 49, NERC-wide analysis of Single Mode Automatic AC Circuit Outages per circuit Initiated by Human Error (ALR 6-12) using the Unpaired Poisson method shows that there is no statistically significant change between the years 2008 to 2011.

Figure 48: NERC Single Mode AC Circuit Outages Year to Year Comparison for ALR 6 – 12

	2009-2008	2010-2009	2010-2008	2011-2008	2011-2009	2011-2010
Estimated Mean Percent Change in Number of Outages per Year per Circuit	-3%	-4%	-7%	-7%	-5%	-1%
Significance of Mean Change in Number of Outages per Year per Circuit	NS	NS	NS	NS	NS	NS

Key to Significance Labels	
NS	Not Significant
*	90% Confident

Figure 49: NERC Single Mode AC Circuit Unpaired Poisson Analysis for ALR 6 – 12



ALR6-13 – Automatic Outages Initiated by Failed AC Substation Equipment

Figure 50 shows the automatic outages with an initiating cause code of failed AC substation equipment. This code covers automatic outages caused by the failure of AC Substation; i.e., equipment “inside the substation fence” including Transformers and circuit breakers but excluding Protection System equipment.

Figure 50: ALR6-13 Automatic Outages Initiated by Failed AC Substation Equipment by Regional Entity (Includes NERC-Wide)



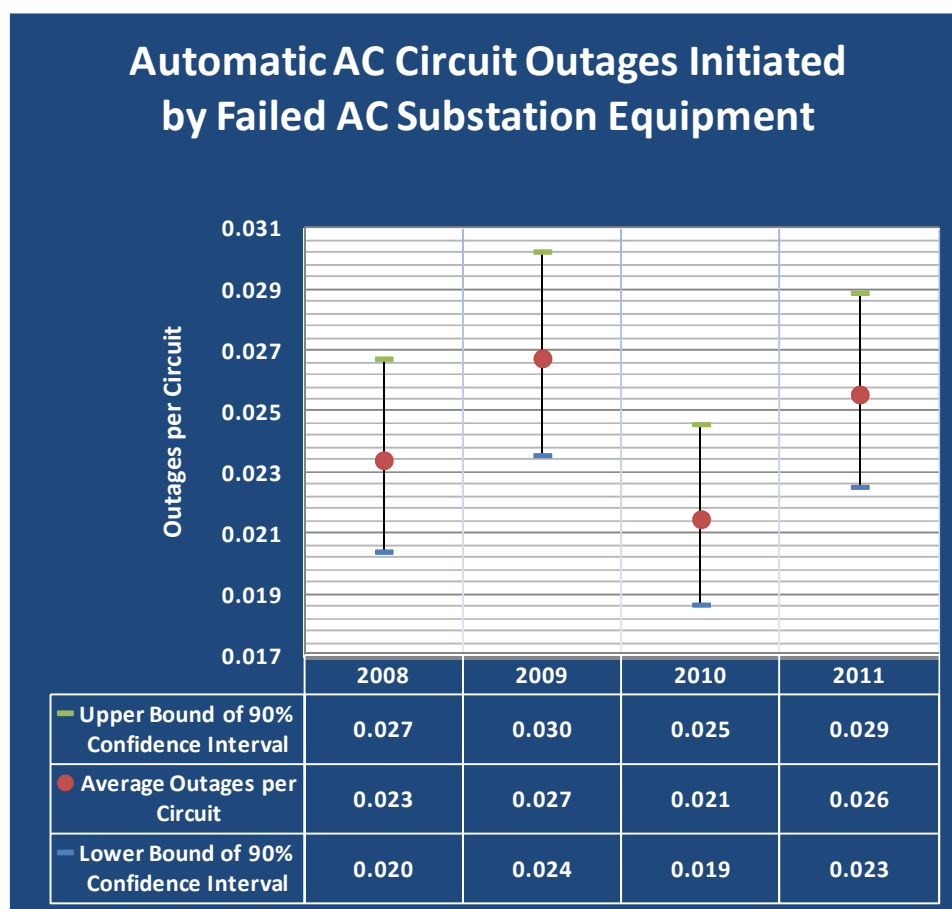
**Note: TRE has no transformers with low-side voltages at 200 kV and above.*

As depicted in Figure 51 and Figure 52, NERC-wide analysis of Single Mode Automatic AC Circuit Outages per circuit Initiated by Failed AC Substation Equipment (ALR 6-13) using the Unpaired Poisson method shows that there is a 90 percent confidence level of statistically significant change between the years 2009 and 2010. Other years do not show statistically significant change.

Figure 51: NERC Single Mode AC Circuit Outages Year to Year Comparison for ALR 6 – 13

	2009-2008	2010-2009	2010-2008	2011-2008	2011-2009	2011-2010
Estimated Mean Percent Change in Number of Outages per Year per Circuit	14%	-20%	-8%	9%	-4%	19%
Significance of Mean Change in Number of Outages per Year per Circuit	NS	*	NS	NS	NS	NS

Key to Significance Labels	
NS	Not Significant
*	90% Confident

Figure 52: NERC Single Mode AC Circuit Unpaired Poisson Analysis for ALR 6 – 13

ALR6-14 Automatic AC Transmission Outages Initiated by Failed AC Circuit Equipment

Figure 53 shows the automatic outages with an initiating cause code of failed AC circuit equipment. This code covers automatic outages related to the failure of AC circuit equipment, i.e., overhead or underground equipment “outside the substation fence.”

Figure 53: ALR6-14 Automatic AC Transmission Outages Initiated by Failed AC Circuit Equipment by Regional Entity (Includes NERC-Wide)



*Note: TRE has no transformers with low-side voltages at 200 kV and above.

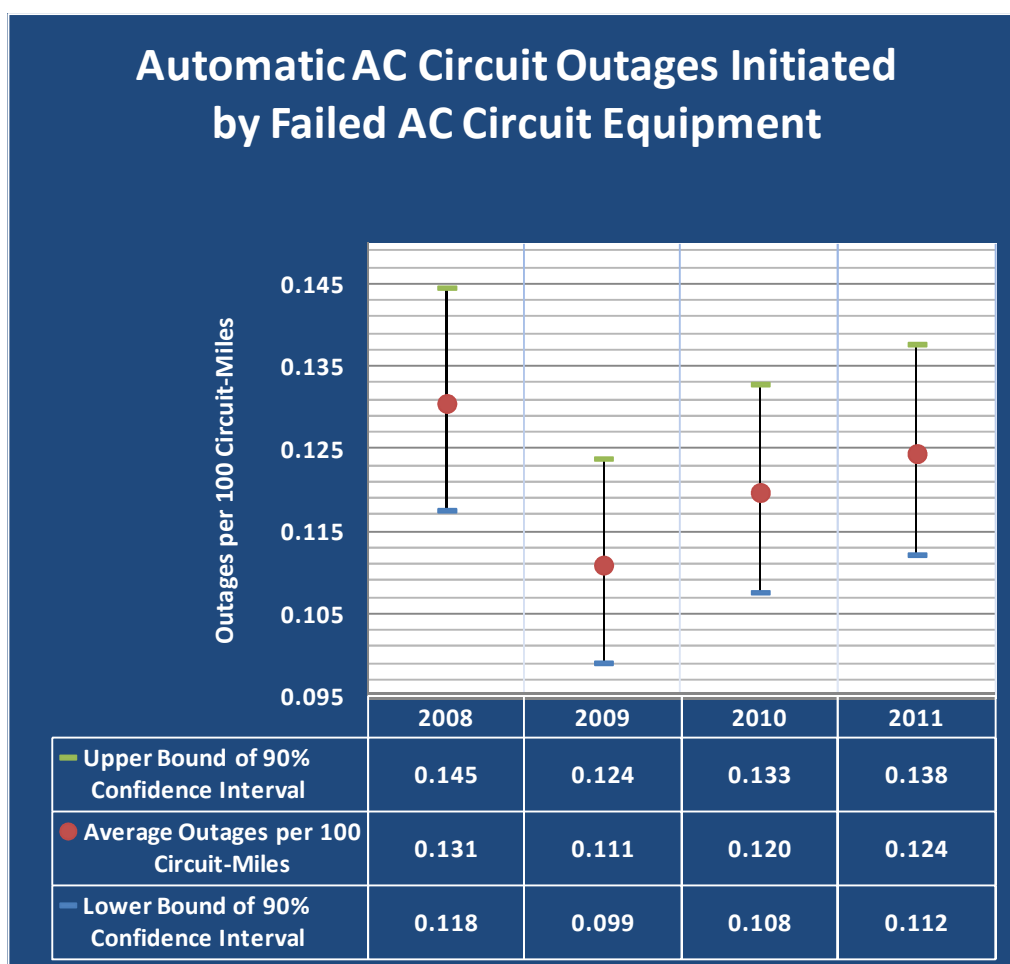
**Note: SPP have no transformer outage occurrences.

As depicted in Figure 54 and Figure 55, NERC-wide analysis of Single Mode Automatic AC Circuit Outages per 100 circuit miles Initiated by Failed AC Circuit Equipment (ALR 6-14) using the Unpaired Poisson method shows that there is a 90 percent confidence level of statistically significant change between the years 2008 and 2009. Other years do not show statistically significant change.

Figure 54: NERC Single Mode AC Circuit Outages Year to Year Comparison for ALR 6 – 14

	2009-2008	2010-2009	2010-2008	2011-2008	2011-2009	2011-2010
Estimated Mean Percent Change in Number of Outages per Year per 100 Circuit-Miles	-15%	8%	-8%	-5%	12%	4%
Significance of Mean Change in Number of Outages per Year per 100 Circuit-Miles	*	NS	NS	NS	NS	NS

Key to Significance Labels	
NS	Not Significant
*	90% Confident

Figure 55: NERC Single Mode AC Circuit Unpaired Poisson Analysis for ALR 6 – 14

ALR 6-15 – Element Availability Percentage (APC)

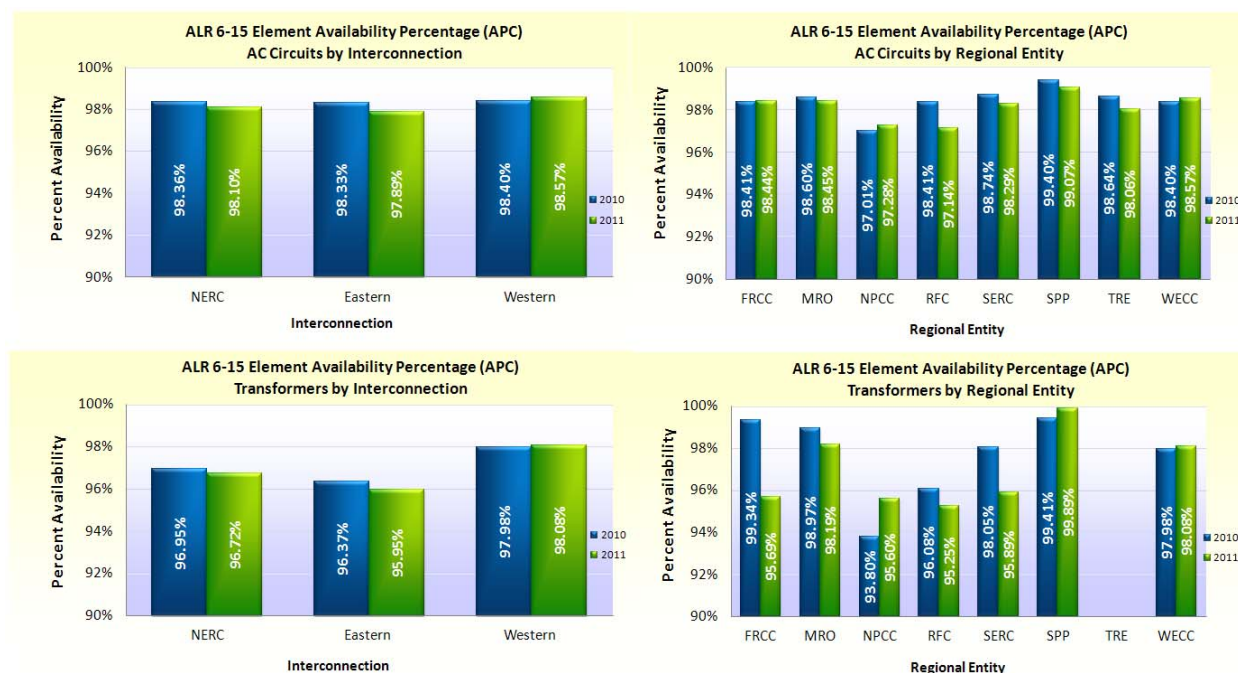
Background

This metric uses data and calculations directly from the NERC TADS effort and shows the overall percent of time that AC circuits and transformers are available and in service. This value is calculated for each element type using sustained outages (automatic and non-automatic) for AC circuits and for transformers operated at 200 kV and above for each Regional Entity, Interconnection, and consolidated values for NERC.

Assessment

Figure 56 shows the 2010 and 2011 element availability percentage (APC) for AC circuits and for transformers operated at 200 kV and above. The values are all over 90 percent. Continued metric data collection for this metric is required for at least a few more years in order to assess the value of this metric.

Figure 56: ALR6-15 Element Availability Percentages (2010-2011)



**Note: TRE has no transformers with low-side voltages at 200 kV and above.*

Special Considerations

The non-automatic outage data needed to calculate this metric was first collected for the calendar year 2010 as part of the TADS process.

ALR 6-16 – Transmission System Unavailability

Background

This metric uses data directly from the NERC TADS effort and shows the overall percent of time that AC circuit and transformer TADS elements are unavailable due to sustained automatic and non-automatic outages. The value is calculated for each element type using sustained outages for AC circuits and for transformers operated at 200 kV and above for each Regional Entity, Interconnection, and consolidated values for NERC.

Assessment

Figure 57 and Figure 58 illustrate the 2010 and 2011 unavailability percentages for AC circuits and for transformers operated at 200 kV and above. The values for AC circuits by Interconnection and Region are all under three percent. Continued data collection for this metric is recommended for at least a few more years in order to assess the value of this metric.

Figure 57: ALR6-16 Transmission System Unavailability (2010 - 2011)

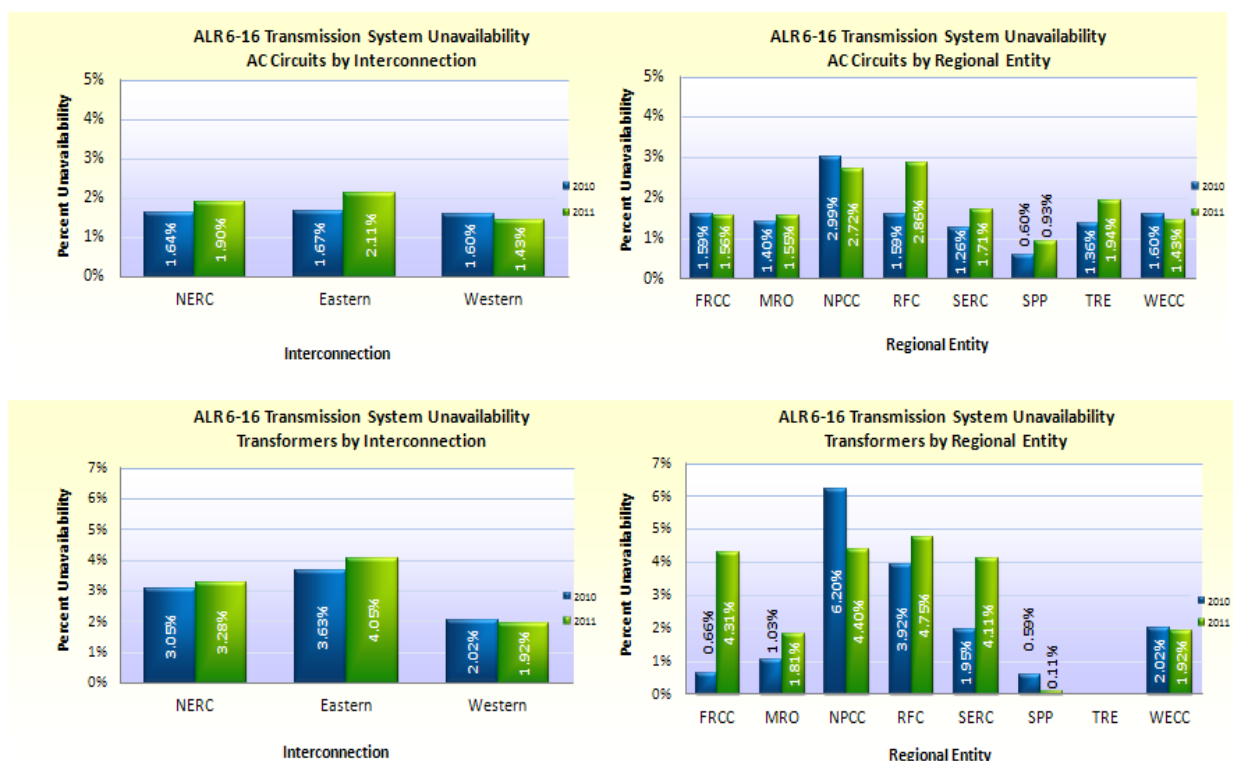
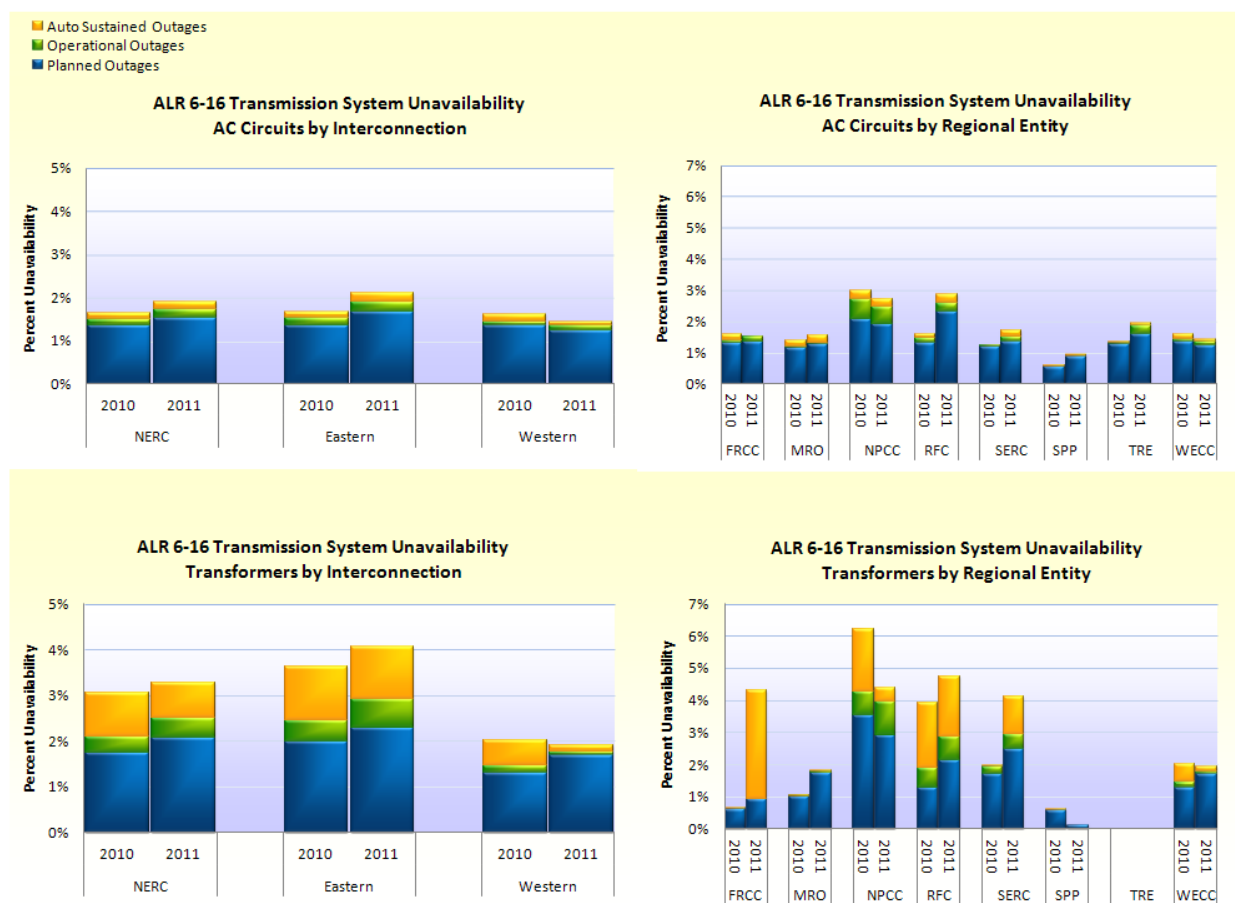


Figure 58: ALR6-16 Transmission System Unavailability by Outage Type (2010- 2011)

Special Considerations

The non-automatic outage data needed to calculate this metric was first collected for the calendar year 2010 as part of the TADS process.

Disturbance Event Analysis

Introduction

Since becoming the Electric Reliability Organization (ERO), NERC has had the need for a systematic, predictable and transparent event analysis process to review bulk power system events based on risk, significance and prioritization. Additionally, NERC needed a consistent and timely reporting of event information so that sharing of valuable reliability information takes place:

- Identify what transpired – sequence of events.
- Understand the cause of events.
- Identify and ensure timely implementation of corrective actions or evaluation of recommendations.
- Develop and disseminate valuable lessons learned to the industry to enhance operational performance and avoid repeat events.
- Develop the capability to integrate risk analysis into the event analysis process.
- Share key results to facilitate enhancements and support of NERC programs and initiatives (e.g., performance metrics, standards, compliance monitoring and enforcement, training and education, etc.)

Starting in October 2010, NERC staff and the Events Analysis

Figure 59: Event Categories

Category 1: An event that results in one or more of the following:

- a. An unexpected outage, contrary to design, of three or more BPS elements caused by a common disturbance. For example:
 - i. The loss of a combination of NERC-defined elements or facilities.
 - ii. The loss of an entire generation station of three or more generators (aggregate generation of 500 MW to 1,999 MW); combined cycle units are represented as one unit.
- b. Intended and controlled system separation by the proper operation of a Special Protection System Scheme (SPS) or Remedial Action Scheme (RAS) in Alberta from the Western Interconnection, New Brunswick or Florida from the Eastern Interconnection.
- c. Failure or misoperation of BPS SPS/RAS.
- d. System-wide voltage reduction of 3% or more that lasts more than 15 continuous minutes due to a BPS emergency.
- e. Unintended BPS system separation that results in an island of 100 MW to 999 MW. Excludes BPS radial connection, and non-BPS (distribution) level islanding.
- f. Unplanned evacuation from a control center facility with BPS SCADA functionality for 30 minutes or more.
- g. In ERCOT, the loss of generation of 1,000 MW - 1,399 MW.

Category 2: An event resulting in one or more of the following:

- a. Complete loss of all BPS control center voice communication system(s) for 30 minutes or more.
- b. Complete loss of SCADA, control or monitoring, functionality for 30 minutes or more.
- c. Voltage excursions equal to or greater than 10% lasting more than five minutes.
- d. Loss of off-site power (LOOP) to a nuclear generating station.
- e. Unintended system separation resulting in an island of 1,000 MW to 4,999 MW.
- f. Unintended loss of 300MW or more of firm load for more than 15 minutes.
- g. Violation of an Interconnection Reliability Operating Limit (IROL) for more than 30 minutes.

Category 3: An event resulting in one or more of the following:

- a. The loss of load or generation of 2,000 MW or more in the Eastern Interconnection or Western Interconnection, or 1,000 MW or more in the ERCOT or Québec Interconnections.
- b. Unintended system separation resulting in an island of 5,000 MW to 10,000 MW.
- c. Unintended system separation resulting in an island of Florida from the Eastern Interconnection.

Category 4: An event resulting in one or more of the following:

- a. The loss of load or generation from 5,001 MW to 9,999 MW.
- b. Unintended system separation resulting in an island of more than 10,000 MW (with the exception of Florida as described in Category 3c).

Category 5: An event resulting in one or more of the following:

- a. The loss of load of 10,000 MW or more.
- b. The loss of generation of 10,000 MW or more.

Working Group (EAWG) developed Phase 1 of an event analysis field trial process and further enhanced this process with the release of Phase 2 in May 2011. As part of this field trial, qualified events were placed into one of five categories based on the severity of the event.

Registered entities were also requested to perform compliance self assessments. Then, in October 2011, NERC and the EAWG completed the field trial process, and implemented the formal process in February 2012.⁸⁰

Also during 2011, NERC's Reliability Risk Management (RRM) Group developed a new NERC Cause Code Analysis Program to guide, assist, and inform industry, and to share data across NERC. The program was based on the Department of Energy's Occurrence Reporting Causal Analysis Guide.⁸¹ It provides the opportunity to collect and disseminate reliability data and fosters collaboration between NERC, Regional Entities, and the registered entities. Events to be cause-coded include human error, EMS, equipment failure, protection system misoperation, and a multitude of other causes. Cause code assignments follow a three-tiered approach to determine root and contributing causes. This process not only identifies human performance and equipment failures, but communication, management, training and design related problems as well. Information from event analysis reports (EAR) has been placed into the Events Analysis Database to track and identify the trends in bulk power system events, in conjunction with other databases (TADS, GADS, metric and benchmarking database). As 2011 came to a close, EAWG was still striving towards an integrated approach to analyzing data, assessing trends and communicating the results to the industry.

Event Analysis (EA) Process

The EA Process (*Electric Reliability Organization Event Analysis Process*, February 2012) was approved following two phases of field trials (Oct 2010 - May 2011, May 2011-February 2012), and is now in place as a voluntary process. This process provides a method by which entities document information concerning:

- What happened during an event and why
- How the event happened, including causal factors
- What corrective actions were taken
- Whether there were any recommendations for preventing reoccurrence
- Whether there were lessons learned to be shared with the industry

Performance Trends

Event categories are classified in Figure 59. Figure 60 depicts trends in qualified events (Category 1 to 5) from January 1, 2011 to December 31, 2011. All weather-related occurrences are included. Table 13 illustrates all qualified events Category 2 or higher. The impact (generation loss, transmission loss, or load loss) is also indicated. April had the highest number

⁸⁰ For additional details, the Events Analysis Process document is located at:
http://www.nerc.com/files/ERO_Event_Analysis_Process_Document_Version_1_Feb_2012.pdf.

⁸¹ For additional details, the DOE Causal Analysis Guide is located at:
<https://www.directives.doe.gov/directives/0232.2-BOrder/view>.

of qualified events in 2011. April's increase in events can be attributed to tornados that occurred in the Southeast. The most severe events recorded in 2011 were two Category 4 events recorded in February and September respectively. The first was a winter storm that caused many generating units forced outages. These forced outages greatly impacted the ERCOT and WECC Regions. A second event occurred when a 500 kV line was lost in the WECC Region.

Figure 60: Event Category by Month (January 1, 2011 – December 31, 2011)

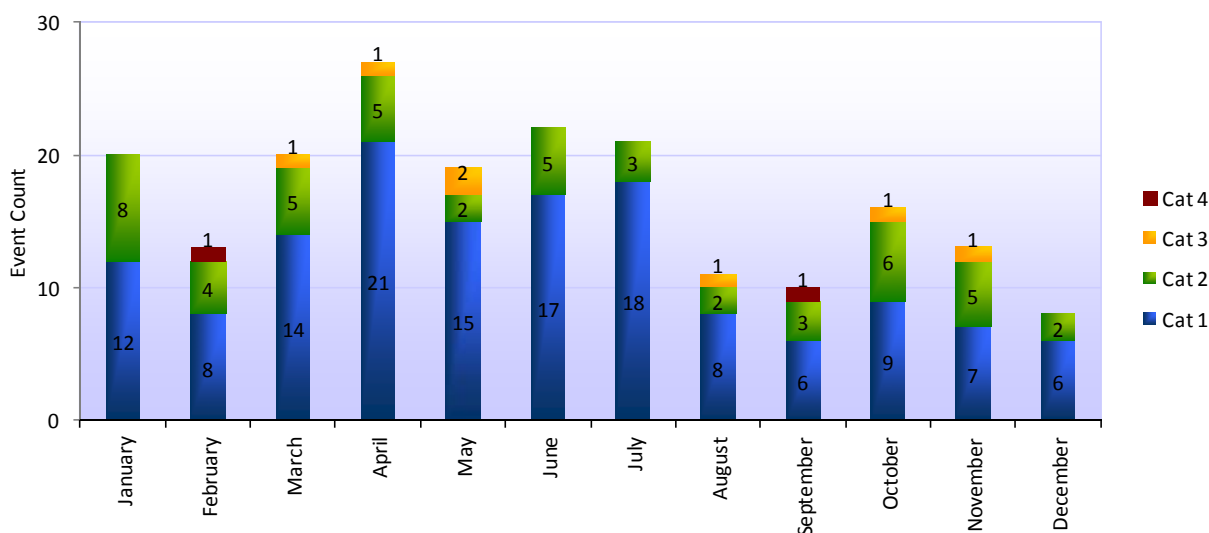


Table 13: 2011 Event Impact

Regional Entity	Date	Event Category	Generation Impact	Transmission Impact	Load Loss Impact
RFC	1/4	2a			
FRCC	1/5	2a		✓	
FRCC	1/13	2f.1			
MRO	1/18	2a			
FRCC	1/24	2a			
FRCC	1/24	2a			
SERC	1/26	2h.2	✓		✓
RFC	1/28	2a			
TRE	2/2	4a	✓		✓
NPCC	2/17	2a			
SERC	2/18	2i			
MRO	2/26	2a			

Table 13: 2011 Event Impact					
Regional Entity	Date	Event Category	Generation Impact	Transmission Impact	Load Loss Impact
WECC	3/2	2a			
WECC	3/7	2d	✓	✓	
MRO	3/9	2a			
SERC	3/15	2b			
TRE	3/23	3a	✓	✓	
WECC	3/29	2a			
WECC	4/8	2a			
SPP RE	4/15	2a			
SERC	4/25	2f.1			✓
SERC	4/26	2f.1			
SERC	4/27	3a			
WECC	4/28	2d	✓		
WECC	5/6	3a	✓	✓	
MRO	5/10	2f	✓	✓	✓
NPCC	5/11	2f		✓	✓
TRE	5/19	3a	✓		
WECC	6/6	2f	✓	✓	✓
WECC	6/7	2b			
WECC	6/14	2b			
SPP RE	6/26	2c	✓		
WECC	6/30	2f	✓		✓
WECC	7/1	2b			
WECC	7/13	2f			
RFC	7/17	2b			
WECC	8/4	2b			
WECC	8/8	2b			
SERC	8/23	3a			

Table 13: 2011 Event Impact					
Regional Entity	Date	Event Category	Generation Impact	Transmission Impact	Load Loss Impact
NPCC	9/2	2b			
WECC	9/8*	4a	*	*	*
WECC	9/18	2b			
NPCC	9/18	2b			
NPCC	10/1	2b			
WECC	10/5	2b			✓
WECC	10/11	2b			
MRO	10/12	2b			
MRO	10/20	2b			
MRO	10/27	2b			
NPCC	10/29	3a	✓	✓	✓
MRO	11/1	2c	✓		
WECC	11/9	2b			
WECC	11/13	2b			
FRCC	11/13	2b			
TRE	11/29	3a	✓		
WECC	11/30	2b			
WECC	12/12	2b			
WECC	12/31	2c	✓		✓

✓ indicates a particular event had generation, transmission, or load loss.

* The 9/8 event is currently under analysis.

In the first 16 months of the Event Analysis field trial, one common failure or trend was observed immediately in the trending and analysis process. During the period of the Event Analysis Field Trial, 28 Category 2b events had occurred where a complete loss of Supervisory Control and Data Acquisition (SCADA) or Energy Management System (EMS) lasted for more than 30 minutes. Further analysis of 24 of these events has revealed three common themes:

1. EMS Software Failure, 52 percent;
2. Inadequate testing of EMS Equipment and Software, 38 percent; and
3. Change Management, 38 percent for EMS systems.

An advisory alert was published in 2012 intended to highlight some of the most common EMS reliability issues and identify opportunities for registered entities to reduce or avoid the complete loss of SCADA/EMS events.⁸² The alert included examples taken from events that illustrate these issues. As a result of this close collaborative discussion within the industry, the alert was also able to provide some practices that industry is applying or could apply in maintaining and testing EMS systems. Employing these or similar practices could help registered entities reduce the risks of EMS interruptions. These events reinforce the need for a well-written detailed test, change management, and change control plan. Most of these events may have been avoided with proper testing using a representative EMS quality assurance test system, with the associated hardware configuration.

One of the ultimate goals of the Event Analysis Program is to enhance reliability and serve as a learning initiative by providing the industry timely lessons learned from system events, conditions, and trends.⁸³ Figure 61 presents the number of lessons learned that have been published since the first quarter of 2011 by theme. For the category 4 winter weather event, a total of 55 lessons learned were submitted, and eight were eventually published by January 2012. The industry indicated that they believe in the Events Analysis process by submitting such a large quantity of lessons learned on one event. This was a very encouraging outcome even if the documents were consolidated into only eight publications in comparison to the count submitted. Events Analysis will continue to present the industry with helpful lessons learned in regards to themes like bulk power operations, transmission facilities, protection systems, and communication.

⁸² The alert can be found at:

http://www.nerc.com/fileUploads/File/Events%20Analysis/Preventable_EMS_and_SCADA_Events_FINAL_20120410.pdf.

⁸³ For additional details, information regarding the Events Analysis Program can be found here: <http://www.nerc.com/page.php?cid=51321>.

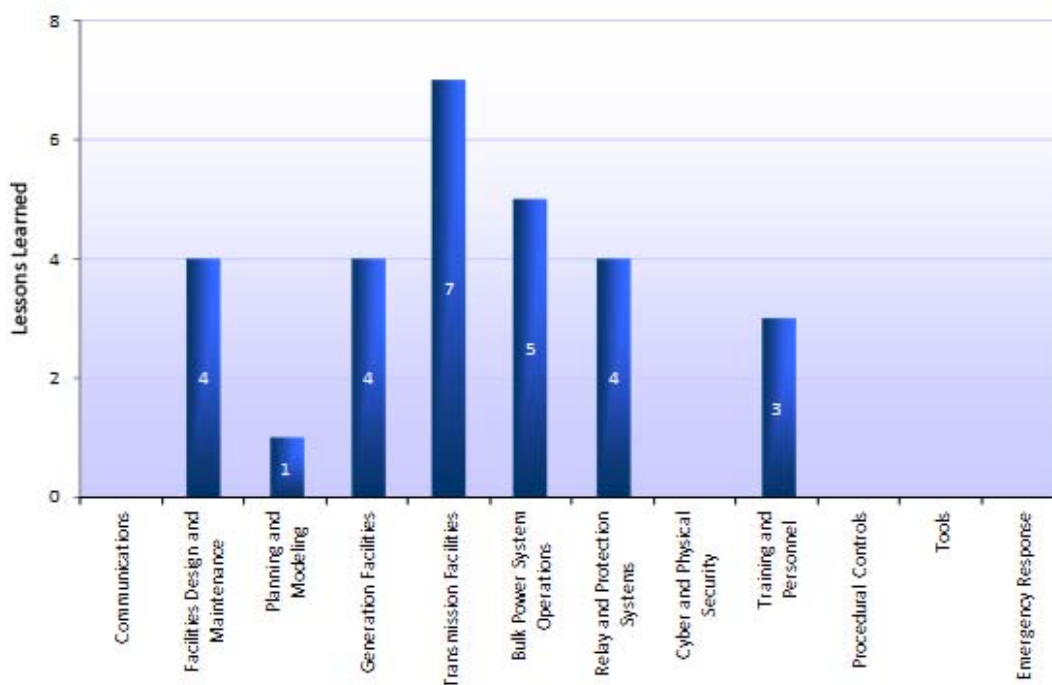
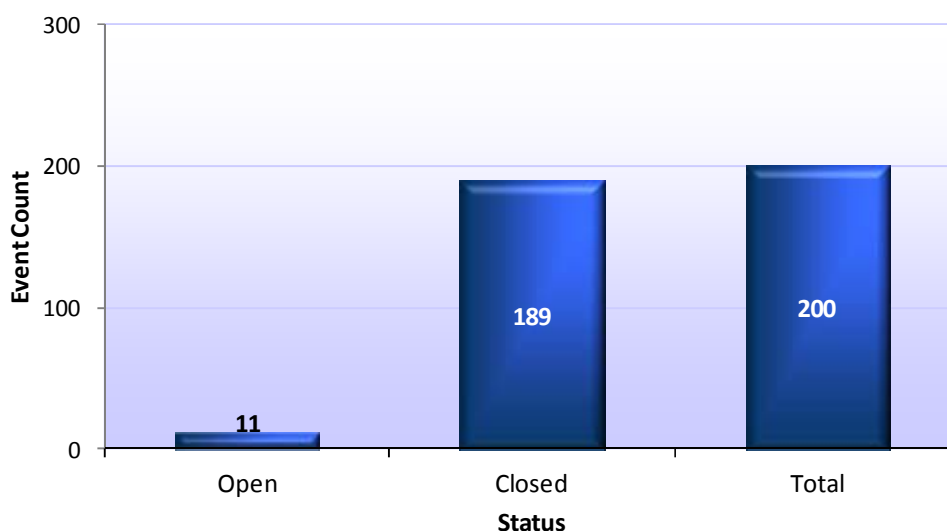
Figure 61: Published Lessons Learned by Theme (Q1 2011 – Q1 2012)

Figure 62 shows 95 percent of 2011 events have been closed as of December 31, 2011. A closed event indicates that the category, root cause, and other important information have been sufficiently advanced in order for analysis to be accurate for each event. In December, NERC events analysis database began capturing the date of closure for all events which have sufficient information to be closed. This date will be used in future analyses to calculate the throughput of event investigations, the rate at which events are opened and closed.

At this time, there is not enough data to draw any long-term conclusions about event analysis performance. Further trending of event categories for closed events and the development of a larger dataset is needed to assess trends between event categories and event counts.

Figure 62: Event Count by Status (January 1, 2011 - December 31, 2011)

Conclusions

The 2011 calendar year was a transitional one for the NERC Event Analysis Working Group (transitioning to EAS). NERC implemented its Event Analysis field trial program and developed a new cause coding analysis process. The cause coding analysis process provides information on the root and contributing factors for events and makes this information available to registered entities through lessons learned, NERC Alerts and other means. The NERC Cause Code Process is still relatively new and is improving each month. Once more data has been collected from events over a longer timeframe; reliability trending and subsequent recommendations will become more readily available to share with Industry. NERC will continue the cause analysis training and offer the course to the industry each quarter of 2012 to ensure the expectations of the process are articulated and to introduce the skills necessary to perform a cause analysis on an event. Additionally, a process will be developed to proactively provide feedback to entities on the completeness of their report and with the maturation of the process, share trending and analysis from across North America.

Transmission Availability Analysis

Introduction

The Transmission Availability Data System (TADS) was launched with the establishment of a TADS task force by the NERC Planning Committee in October 2006.⁸⁴ On October 27, 2007, the NERC Board of Trustees approved the collection of automatic transmission outage data beginning in calendar year 2008 (Phase I). Subsequently, on October 29, 2008, the NERC Board of Trustees approved the collection of non-automatic outage data beginning in calendar year 2010 (Phase II).

This chapter focuses on automatic outage information from calendar year 2008 to 2011. Since only two years of non-automatic outages were collected, insufficient information is available for use in this report.

When calculating bulk power system performance, care must be exercised when interpreting results. Misinterpretation can lead to erroneous conclusions regarding system performance. The unpaired Poisson statistical method was applied to determine the relevance of statistically significant change of transmission metrics ALR 6-11 – 6-14 from year to year.⁸⁵ On a regional basis, there was not enough data to perform statistically relevant analysis. On a NERC-wide basis, however, there is enough information to accurately determine whether the yearly outage variation compared to another year is due to random statistical variation, or the particular year in question is statistically different in performance.

Performance Analysis

Transmission performance information has been provided by Transmission Owners (TOs) within NERC through the NERC TADS process. The data presented in the Performance Analysis section includes momentary and sustained AC automatic outages of AC circuits (overhead and underground) that operate at voltages greater than or equal to 200 kV with the criteria specified in the TADS process. The data presented in the Transmission Outage Events section includes AC circuits, transformers, DC circuits, and AC/DC back-to-back converters with criteria specified in the TADS process.

Unpaired Poisson Analysis of Metrics ALR6-11 to ALR6-14

It is relatively straightforward to calculate the observed rate of failure for each AC circuit from year to year for each ALR metric. However, it is much more challenging to determine whether the changes in these rates are due to improvements in reliability, if the changes are due to other factors that are not the target of interest, or if they are simply due to random fluctuations. By making some assumptions about the number of outages that occur each year it may be possible to draw some conclusions about whether observed changes are signs of actual changing reliability.

⁸⁴For additional details on TADS, the Data Reporting Instruction Manual is located at:
<http://www.nerc.com/docs/pc/tadswg/Data%20Reporting%20Instr%20Manual%2020101202a%20clean.pdf>.

⁸⁵For additional details on the unpaired Poisson statistical method, the EIA memo is located at:
http://www.nerc.com/docs/pc/tadswg/07_agenda%20item%20EIA%20Memo.pdf.

To evaluate annual changes in the metrics, NERC wide metrics ALR6-11 – ALR6-14 for **Single Mode Outages of AC Circuits** only were analyzed using the Unpaired Poisson method.⁸⁶ ALR6-11 through ALR 6-14 for Single Mode Outages of Transformers were not analyzed due to a lack of sufficient outage data over the four year period and a high focus on AC circuits. This method makes the following assumptions:

1. Assume the outages for each circuit in year 1 comes from identical but independent Poisson distributions.
2. Assume the outages for each circuit in year 2 comes from identical but independent Poisson distributions.
3. Assume the number of outages in year 1 and the numbers of outages in year 2 are independent.

The Unpaired Poisson method is only applicable for assessing the statistical change from one year to another year, and will use the significance labels in Figure 63 to represent how confident we are that the mean change in number of outages per year per circuit is not zero. In other words, how confident we are that there is a statistically significant change from one year to another year.

Figure 63: Significance Labels

Key to Significance Labels	
NS	Not Significant
*	90% Confident

This method is not appropriate for assessing the overall trend from 2008 to 2011, and further study will be conducted to develop such a method. Also, this method is not appropriate to use for analyzing Common mode outages and Dependent mode outages. The framework for analyzing these metrics using the Unpaired Poisson method are only appropriate when the outages at any circuit are independent of the outages on any other circuit.

An in-depth study of Common mode outages and Dependent mode outages will be needed to understand the contributing factors of these outages because independence is not assumed. This study is under way, and in future reports analysis of ALR6-11 – ALR6-14 for Single Mode, Common Mode, Common Mode Initiating, Dependent Mode, and Dependent Mode Initiating for AC Circuits and Transformers will be conducted, but only analysis of Single Mode outages for AC Circuits is included in the Reliability Indicator Trends section of this report.

AC Circuit Outage Summary and Leading Causes

Table 14 shows the 2008, 2009, 2010, and 2011 NERC total AC circuit inventory and a summary of the associated outages. The number of circuits increased from year-to-year due to new construction or reconstruction to higher voltages. For every outage experienced on the

⁸⁶ The Unpaired Poisson method is located at:
http://www.nerc.com/docs/pc/tadswg/07_agenda%20item%20EIA%20Memo.pdf.

transmission system, cause codes are recorded according to the TADS process.⁸⁷ Causes of both momentary and sustained outages have been indicated. These causes are analyzed to identify trends, similarities, and to provide insight into what could be done to prevent future occurrences.

Figure 64 and Figure 65 display the top ten initiating cause codes for sustained and momentary automatic outages from 2008 to 2011. “Weather, excluding lightning” and “Unknown” are the top two causes of sustained outages with 31 percent of the total outages. The two largest causes of momentary outages within NERC are “Lightning” and “Unknown”.

From 2008 to 2011, nearly 20 percent of automatic sustained outages were initiated by either failed AC substation equipment or failed AC circuit equipment as shown in Figure 64. These equipment failures along with human error and failed protection system equipment are high causes for bulk power system transmission-related events resulting in loss of firm load, and should be considered significant focus points in reducing the number of expected challenges incurred by the bulk power system.

⁸⁷Please refer to section F in <http://www.nerc.com/docs/pc/tadswg/Appendix%207%2020101202a%20clean.pdf>.

Table 14: NERC - AC Circuit Sustained and Momentary Outage Performance Summary						
2008 Number of Outages						
AC Voltage Class	No of Circuits	Circuit Miles	Sustained	Momentary	Total Outages	Total Outage Hours
200-299kV	4,373	102,482	1,560	1,062	2,622	56,595
300-399kV	1,597	57,903	795	753	1,548	14,701
400-599kV	587	31,579	391	196	587	11,776
600-799kV	110	9,529	43	40	83	369
All Voltages	6,667	201,493	2,789	2,051	4,840	83,411
2009 Number of Outages						
AC Voltage Class	No of Circuits	Circuit Miles	Sustained	Momentary	Total Outages	Total Outage Hours
200-299kV	4,472	103,417	1,389	896	2,285	28,124
300-399kV	1,632	58,660	640	610	1,250	24,714
400-599kV	593	32,130	264	166	430	9,110
600-799kV	110	9,529	53	38	91	442
All Voltages	6,807	203,736	2,346	1,710	4,056	62,390
2010 Number of Outages						
AC Voltage Class	No of Circuits	Circuit Miles	Sustained	Momentary	Total Outages	Total Outage Hours
200-299kV	4,576	105,231	1,510	918	2,428	54,962
300-399kV	1,693	64,823	723	602	1,325	16,044
400-599kV	607	31,702	295	174	469	10,442
600-799kV	111	9,555	63	50	113	2,303
All Voltages	6,987	211,311	2,591	1,744	4,335	83,751
2011 Number of Outages						
AC Voltage Class	No of Circuits	Circuit Miles	Sustained	Momentary	Total Outages	Total Outage Hours
200-299kV	4,709	107,239	1,460	1,014	2,474	46,115
300-399kV	1,722	65,429	795	652	1,447	27,398
400-599kV	620	32,329	303	142	445	27,951
600-799kV	111	9,555	31	38	69	2,942
All Voltages	7,162	214,552	2,589	1,846	4,435	104,406

Figure 64: NERC 2008 – 2011 AC Circuit Top Ten Sustained Automatic Outage Occurrences by Initiating Cause Code⁸⁸

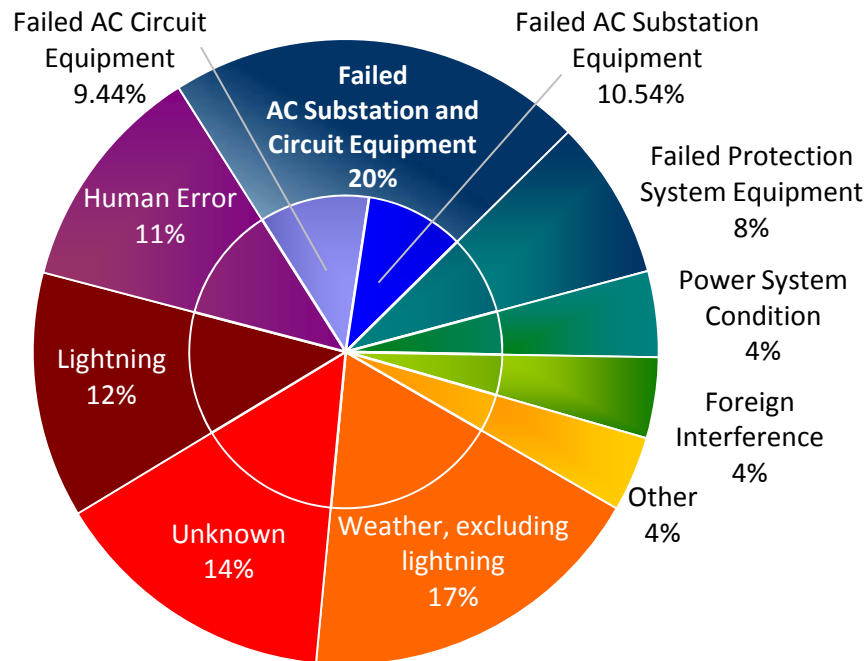
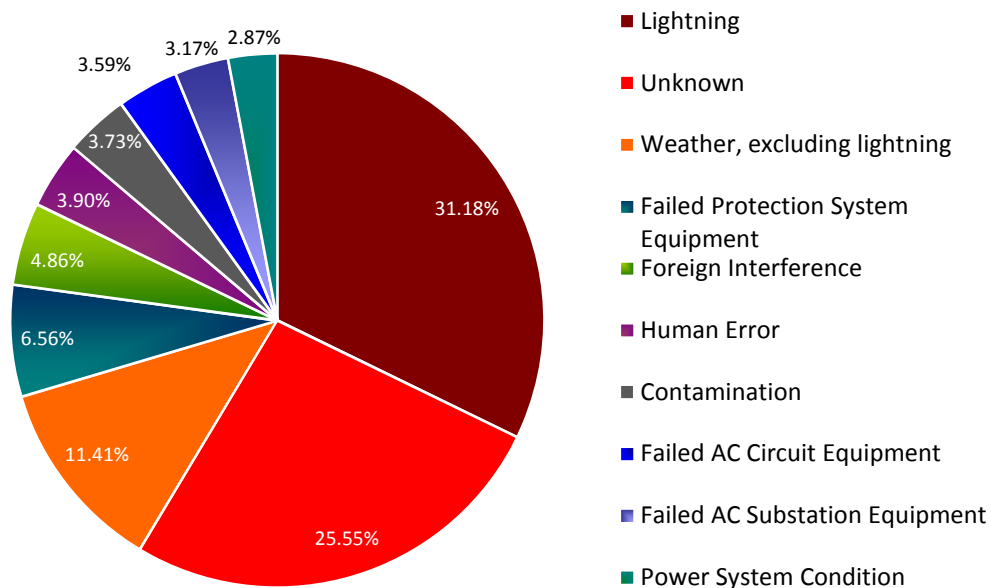


Figure 65: 2008 – 2011 AC Circuit Top Ten Momentary Automatic Outage Occurrences by Cause Code⁸⁹



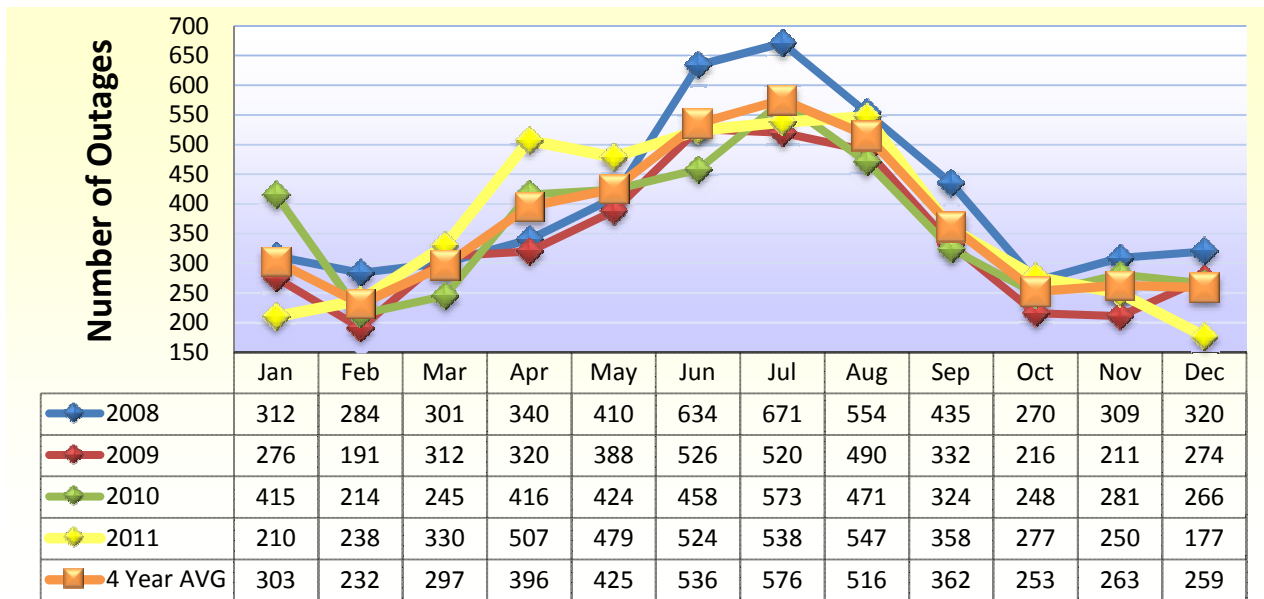
⁸⁸ Percent is out of total number of outages. The remaining 7.40 percent include: Fire, Contamination, Vegetation, etc. Foreign interference is non-transmission equipment, such as an aircraft, machinery, a bird, or flying debris not caused by wind.

⁸⁹ Percent is out of total number of outages. The remaining 3.18 percent include: Other, Fire, Vegetation, etc.

AC Circuit Monthly Outages

Figure 66 displays monthly AC circuit total automatic outages. The three months with the highest total of automatic outages were June, July, and August. From a seasonal perspective, winter, November to February, had a monthly, four-year average of 264 outages. Summer, June to September, had a monthly, four-year average of 498 outages.

Figure 66: Monthly AC Circuit Automatic Outage Count (2008-2011)



Outage Initiation

For every outage experienced on the transmission system, the outage initiation code is identified and recorded. A review of outage initiation code statistics can identify trends and similarities and provide insight into areas for improvement.

The “Outage Initiation Code” describes where an automatic outage was initiated on the power system. The five codes are as follows:

- Element-Initiated;
- Other Element-Initiated;
- AC Substation-Initiated;
- AC/DC Terminal-Initiated (for DC circuits); and
- Other Facility Initiated: any facility not included in any other outage initiation code.

Notably, the protection system is not part of an “AC Substation” or an “AC/DC Terminal”. If a protection system misoperates and initiates an outage, it will be classified as “Other-Facility Initiated”. Figure 67 and Figure 68 show where the sustained and momentary automatic AC Circuit outages were initiated for 2008 to 2011. For sustained outages, the outage was initiated on the AC Circuit element more than 61 percent of the time.

Figure 67: 2008 – 2011 Outage Initiation Location for AC Circuit Sustained Automatic Outages by Initiation Code

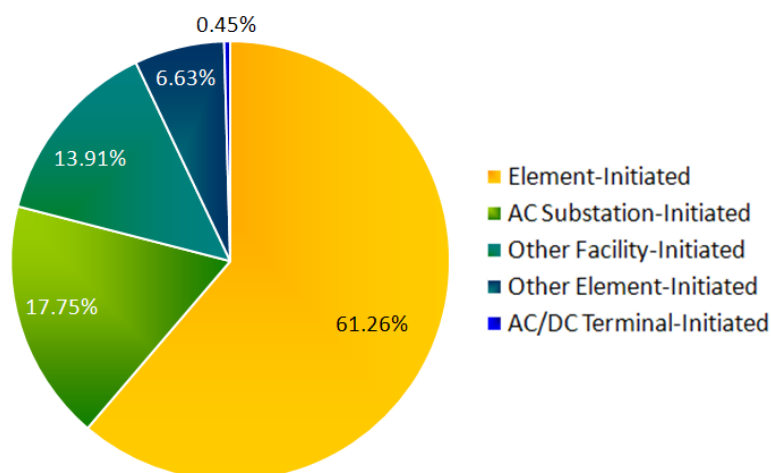
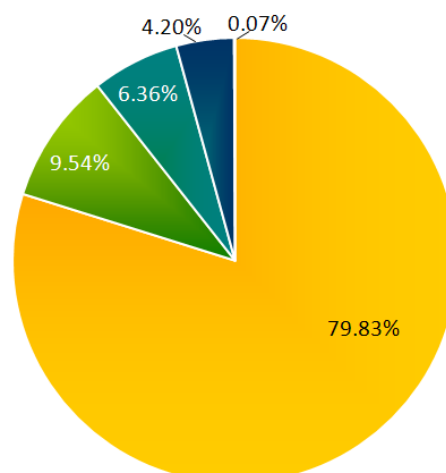


Figure 68: 2008 – 2011 Outage Initiation Location for AC Circuit Momentary Automatic Outages by Initiation Code

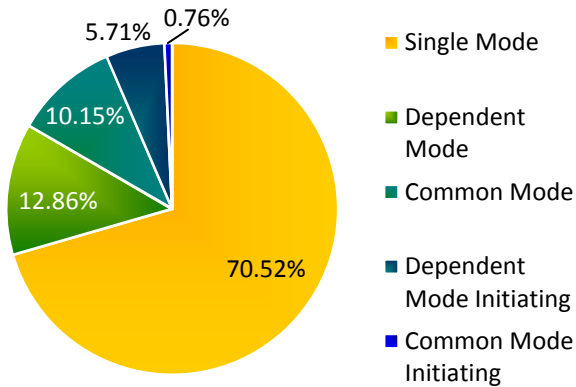
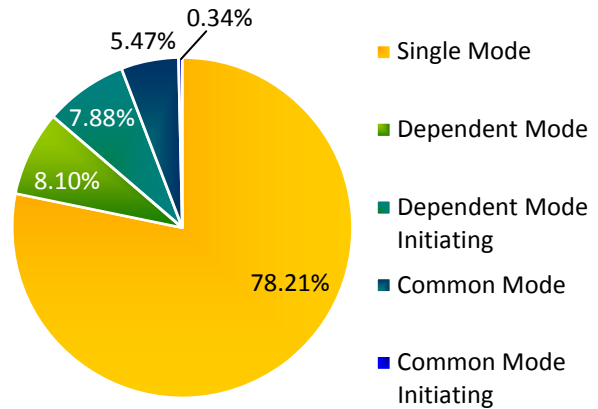


Transmission Outage Modes

Figure 69 and Figure 70 show the percentage of outage modes. The “outage mode code” relates one automatic outage to other automatic outages. A definition of each outage mode code is provided in Table 15.

Table 15: Outage Mode Codes	
Outage Mode Code	Automatic Outage Description
Single Mode	A single element outage which occurs independently of another automatic outage
Dependent Mode Initiating	A single element outage that initiates at least one subsequent element automatic outage
Dependent Mode	An automatic outage of an element which occurred as a result of an initiating outage, whether the initiating outage was an element outage or a non-element outage
Common Mode	One of at least two automatic outages with the same initiating cause code where the outages are not consequences of each other and occur nearly simultaneously
Common Mode Initiating	A common mode outage that initiates one or more subsequent automatic outages

Over 70 percent of sustained and momentary AC circuit outages are single mode. This reinforces the long held belief that the majority of all sustained and momentary automatic outages are single mode. However, a significant percent of automatic outages, 29.5 percent sustained and 21.8 percent momentary, are in the dependent or common mode family.

Figure 69: 2008 – 2011 AC Circuit Sustained Automatic Outage Mode**Figure 70: 2008 – 2011 AC Circuit Momentary Automatic Outage Mode**

For sustained AC circuit outages 70.5 percent are single mode single element outage events. A dependent mode single element outage may occur, as noted in the definition above, due to a non-Element (<200kV) outage. Out of the 29.5 percent dependent or common mode sustained outages, 8.1 percent are single element outage events. 78.6 percent (70.5 + 8.1) of the AC circuit sustained outages are single element outage events. The remaining 21.4 percent of the AC circuit sustained outages are two or more element outage events.

Based on typical TOP daily operations criteria (and associated TPL design criteria - Table 1 Category B), at a minimum the system is operated to withstand a fault on an element with normal clearing. Normal clearing by design may outage more than one element, such as a 500/230 kV transformer which is tapped on a 500 kV line. For such an example, a fault on the 500 kV line would result in one 500 kV line “Dependent Mode Initiating” outage and one 500/230 kV transformer “Dependent Mode” outage. Such Table 1 Category B events are covered by TOP daily operations criteria. An unknown portion of the above 21.4 percent multi-element outages are Category B events with normal clearing.

More importantly an unknown portion of the 21.4 percent multi-element outages are not Category B events and are potentially an operational reliability risk. Several types of lesser probability dependent or common mode outages are covered by TPL design criteria – Table 1 Category C. For example the system is designed to be capable of being operated in a manner to withstand any one of the following Category C events: a single bus section outage, two adjacent circuit outages on a multi-circuit transmission structure, delayed clearing due to a circuit breaker failure or failed high speed protection system. However, since these are lesser probability events, the TOP standards do not explicitly require the system to be operated within all Category C dependent or common mode failures.

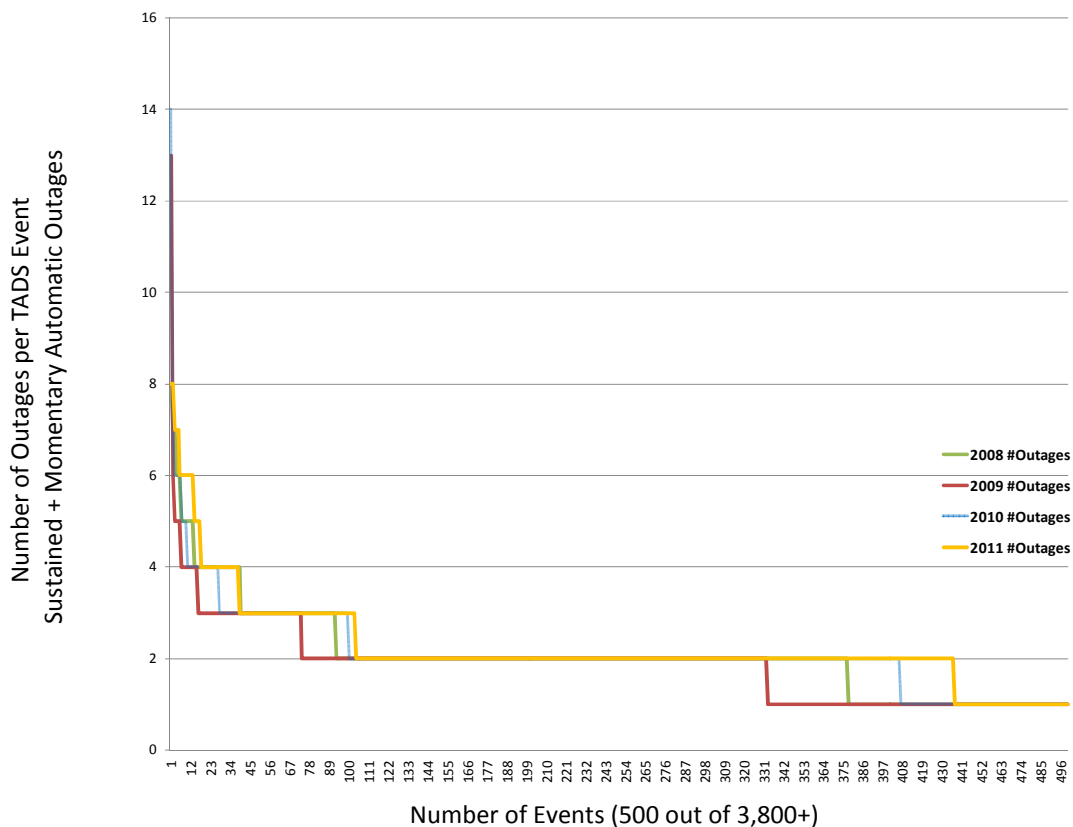
Transmission Outage Events

A single transmission event, as defined in TADS, may include both sustained and momentary element outages. Such an event which includes one or more momentary outages (for up to one minute) does change substation bus voltage magnitudes and voltage angles. Such events

may cause dynamic stability or steady state voltage magnitude or angle limits to be exceeded. If the voltage magnitudes are below acceptable limits or unstable, system voltages may continue to deteriorate and collapse. If the voltage angles are too far apart or unstable, line circuit breaker reclosing is automatically blocked, and the system may become unstable. Figure 71 illustrates the relationship between the numbers of total automatic outages (sustained + momentary) per TADS event.

In the figure, the total number of events in 2008 to 2011 ranged from 3,898 to 4,563 events per year. On a four-year average, 4,185 events occurred per year. All four years, 2008-2011 follow a similar trend. The largest number of automatic outages in an event for elements greater than 200kV is eight in 2011, 14 in 2010, 13 in 2009, and eight in 2008. Based on a four-year average there are approximately 92 events per year (two percent of 4,185) that contain between three and 14 automatic outages (see below). There are 297 events per year (seven percent) that contain two automatic outages. On the average 3,796 (91 percent) of TADS events were single element automatic outages.

**Figure 71: TO Reported Outages per TADS Event
(Including Sustained + Momentary outages for all > 200kV Elements)
(2008-2011)**



In last year's annual report, it was noted an investigation into the root causes of dependent and common mode events which include three or more automatic outages is a high priority. Some protection systems are designed to normally trip three or more circuits, but some of the above events go beyond what is designed. In addition, protection system misoperations are associated with a number of multiple outage events.

On the average there are 61 events per year (2.5 percent of 2,422) that contain between fourteen and three sustained automatic element outages.

Events with three or more automatic outages

As noted in the discussion of momentary and sustained outages, based on a four year average, approximately 92 events per year (two percent) contain between three and 14 automatic outages. Transmission Owners which reported 369 such events during 2008 to 2011 were sent a voluntary survey request to better understand such events. Survey responses for 133 (36 percent) of the 369 events were received and summarized in Table 16.

Table 16: Survey Summary - Three Outages or More per TADS Event		
Description	TADS Events	Percent
Total Common and Dependent mode events with 3 or more circuit outages	369	100 percent
Survey Responses (Number of Events)	133	36 percent (133 of 369)
Normal Clearing Events	49	37 percent (49 of 133)
Abnormal Clearing Events (TADS Event Types 60+61+62+90)	84	63 percent (84 of 133)
Events Caused by Misoperations (TADS Event Types 61+62)	63	47 percent (63 of 133)

As shown, 49 (37 percent) of the 133 event responses were Normal Clearing events. Eighty-four (63 percent) of the events contained one or more abnormal clearing outage (TADS Event Types 60 to 90). This represents a 100 percent total (37 percent + 63 percent) of the responses. Out of the 84 abnormal events, 63 events contained one or more outages caused by a misoperation. These 63 events represent 47 percent of the 133 event responses. In other words, for events which contained 3 or more automatic outages, 47 percent of these unusual events involved one or more misoperation.

Conclusions

For 2011, metric ALR6-15 indicates that the transmission element availability outage percentage exceeded 98 percent for AC circuits.

On a NERC-wide basis, the automatic transmission sustained outage number of events decreased from 2008 (2,611 events) to 2011 (2,411 events). However, there was not a commensurate decrease in the number of events which contain two or more automatic outages.

There are two potential improvements to reliability based on the data. First, continued analysis of the ALR metric data for non-weather or lightning related known causes involving Human Error, Failed Protection System Equipment, Failed AC Substation Equipment and Failed AC

Circuit Equipment should continue to be a focal point to reduce the number of sustained automatic single element outages. When system operation is challenged by such single element outages, the more likely it may result in an abnormal clearing event of multiple elements. Second, as announced at the March 2012 NERC Planning Committee meeting, a deeper investigation into the root causes of misoperations which contribute to dependent and common mode events is a high priority. A Protection System Misoperation Task Force (PSMTF) has been formed to analyze misoperations. Some of these misoperation events go beyond the basic TPL standard Table 1 planning criteria, or go beyond the Table 1 Category B⁹⁰ events commonly used in daily operation. More analysis would improve understanding of the assumptions used for TPL and TOP contingency criteria which form the basis for system planning adequacy studies and daily operation of the system.

⁹⁰ <http://www.nerc.com/files/TPL-002-0b.pdf>

Generating Availability Analysis

Introduction

The development of the Generating Availability Data System (GADS) began in 1982. GADS collects and stores voluntarily provided unit operating information on a quarterly basis. By pooling individual unit information, overall generating unit availability performance is calculated. The information supports equipment reliability, availability analyses and risk-informed decision making to industry. Finally, reports and information resulting from the data collected through GADS are now used for benchmarking and analyzing electric power plants.

Currently, the data collected through GADS contains 72 percent of North American generating units with generating capacity of 20 MW and larger.⁹¹ Through the end of 2011, generating unit data in GADS was collected strictly on a voluntary reporting basis. This report is based on conventional units which are outlined in Section 2 of the GADS Data Reporting Instructions.⁹² Renewable units (solar and wind) are not reported to GADS at this time and were not included in this report. Starting in January 2012, GADS became mandatory for conventional generating units 50 MW and larger. In 2013, GADS will become mandatory for conventional generating units 20 MW and larger. This will increase the number of units in GADS to about 94 percent of the installed capacity in North America.

Many newer combined-cycle plants and other unit types are not reporting data, and a full representation of each unit type is not always presented. Rather, a sample of all the units in North America that fit a given, more general category is provided for the 2008 to 2011 assessment period.

Generation Key Performance Indicators

Three key performance indicators⁹³ used to measure the availability of generating units are Equivalent Availability Factor (EAF), Net Capacity Factor (NCF), and Equivalent Forced Outage Rate – Demand (EFORD). EAF measures the fraction of net maximum generation that could be provided after all types of outages are taken into account. It also measures percent of maximum generation available over time. Generating companies want high EAF numbers. NCF measures the actual energy generated as a fraction of the maximum possible energy it could have generated at maximum operating capacity. The higher the NCF, the more the unit is used to meet load demands. EFORD is a good measure of reliability. EFORD measures the probability that a unit will not meet its demand periods for generating requirements because of forced outages or deratings.

In Table 17, the North American fleet average EAF, NCF, and EFORD compared to unit age for all generating units with a capacity of 20 MW and larger is summarized for the years 2008 to 2011. For 2008-2010, the same group of units was used so a true measure of comparable trending

⁹¹ GADS contains 1,500+ units under 20 MW that are not included in this report.

⁹² GADS Data Reporting Instructions is located at <http://www.nerc.com/page.php?cid=4|43|45>.

⁹³ Equations for EAF, NCF and EFORD are found in Appendix F of the GADS Data Reporting Instructions at: <http://www.nerc.com/page.php?cid=4|43|45>.

could be completed over those three reporting years. However for 2011, only 70 percent of the data was available at the time this report was prepared. Nonetheless, valid inferences can still be made using 2008 to 2010 versus 2011 data.

During the last four years, the EAF and NCF have dropped from 2008 to 2009 and have partly recovered in the 2010 and 2011 reporting periods, while EFORD has increased in 2010 and 2011. Overall, the fleet of units reported to GADS appears to be aging. On a four-year average, fossil-steam units are around 13 years older than the rest of the fleet.⁹⁴

Table 17: General Availability Review of GADS Fleet Units by Year*				
Metric/Year	2008	2009	2010	2011
Equivalent Availability Factor (EAF)	87.75	87.61	86.46	86.53
Net Capacity Factor (NCF)	49.65	46.46	48.18	48.96
Equivalent Forced Outage Rate - Demand (EFORD)	5.51	5.65	6.19	6.16
Number of Units $\geq$ 20 MW	4,366	4,366	4,366	2,510
Average Age of the Fleet in Years (all unit types)	31.89	32.65	33.49	31.43
Average Age of the Fleet in Years (fossil-steam units only)	42.25	43.11	43.96	44.36

**Includes only GADS reporting units with greater than 20 MW generation capability*

Generating Unit Retirements and New Units

GADS has been recording the number of units retiring from service for several years. It has also recorded the number of new units coming into service based on the date of commercial operation. Table 18 and Table 19, respectively, present the number of units retired and added to GADS. All analysis is based on generating companies reporting to GADS during the 2008 to 2011 timeframe⁹⁵ which does not include all of North America.

Table 18 shows the total number of MW and the total number of generating units removed from service for each Region in GADS. For example, Texas Reliability Entity (TRE) retired the largest number of fossil-steam units, 29, for a total of 7,813 MW. However, Table 18 shows, TRE also added four new fossil-steam units that will add 3,304 MW to their fleet. Table 18 and Table 19 present retired and new, commercial generating units for fossil-steam, simple-cycle gas turbines, diesel, multi-boiler/turbine fossil, combined cycle block and hydro electric plants.

In summary, GADS shows 14,647 MW of retired generation but 42,760 MW of new generation during the four-year period. This is nearly three times more new generation added than required to simply offset reported requirements. A large number of small fossil-steam units are

⁹⁴ Fossil-steam units are generating facilities with a single boiler and single steam turbine. These units are normally coal, oil, or natural gas-fired. Combined cycle plants are not part of the fossil-steam category but are a separate group of units.

⁹⁵ At the publication of this report, only 70 percent of the 2011 GADS was available for review.

retiring, but the fossil-steam unit additions almost match the capacity retired. A large number of simple cycle gas turbines and combined cycle blocks have been added to the generation mix to make up for fossil-steam units retired, and to serve projected load growth. As a result, there are fewer units using coal, and more fossil-steam units using natural gas as their primary fuel source. From 2008 to 2011, no hydroelectric capacity was retired, and no new multi-boiler fossil capacity was added.

Some of the new generating units (18,105 MW of the 42,760 MW) were not reported in detail to GADS by the time this report was prepared. Therefore, it is unclear which fuels those new units will burn. However, some new generating units have reported the fuel that they will burn. As a result, a sample of the types of fuels these new units will use was gathered. Table 20 and Table 21 represent units retiring (14,647 MW) and new units coming on-line (24,655 MW) where fuel type is known. The vast majority of old and new units are gas fired. The amount of new coal units MW is almost three times the MW as those retiring. The largest number of new coal and lignite MW were in Reliability First Corporation (RFC) with 2,269 MW. TRE was the second largest with 2,166 MW. The “Other” fuels include fuels types such as kerosene, diesel, biomass, and landfill off gases. They are not as commonly used like coal, oil, natural gas, and water.

Table 18: Retired Generating Units in GADS 2008 – 2011

Regional Entity	Fossil-Steam Capacity, MW	# of Fossil-Steam units	Simple cycle Gas Turbines Capacity, MW	# of simple Cycle GT units	Diesel Capacity, MW	# of Diesel units	Multi-boiler Fossil Capacity, MW	# of Multi-boiler Fossil units	Combined Cycle Capacity, MW	# of Combined Cycle units
FRCC	446	3	65	1	0	0	0	0	0	0
MRO	850	16	119	5	4	2	0	0	0	0
NPCC	1,115	5	0	0	0	0	0	0	0	0
RFC	1,736	16	156	6	0	0	319	3	0	0
SERC	1,006	17	168	7	0	0	0	0	0	0
SPP	0	0	0	0	0	0	43	2	0	0
TRE	7,813	29	32	1	0	0	0	0	335	1
WECC	384	7	56	4	0	0	0	0	0	0
Totals	13,350	93	596	24	4	2	362	5	335	1

Table 19: New Generating Units in Commercial Operation in GADS 2008 - 2011

Regional Entity	Fossil-Steam Capacity, MW	# of Fossil-Steam units	Simple cycle Gas Turbines Capacity, MW	# of simple Cycle GT units	Diesel Capacity, MW	# of Diesel units	Combined Cycle Capacity, MW	# of Combined Cycle units	Hydro Capacity, MW	# of Hydro units
FRCC	0	0	858	8	0	0	2,405	4	0	0
MRO	1,944	4	781	6	0	0	1,162	2	16	16

Table 19: New Generating Units in Commercial Operation in GADS 2008 - 2011

Regional Entity	Fossil-Steam Capacity, MW	# of Fossil-Steam units	Simple cycle Gas Turbines Capacity, MW	# of simple Cycle GT units	Diesel Capacity, MW	# of Diesel units	Combined Cycle Capacity, MW	# of Combined Cycle units	Hydro Capacity, MW	# of Hydro units
NPCC	0	0	654	14	0	0	1,643	4	85	5
RFC	1,379	3	911	13	57	18	1,145	1	2	2
SERC	3,476	6	1,552	11	0	0	4,512	9	0	0
SPP	1,165	2	1,634	11	0	0	1,276	2	0	0
TRE	3,304	4	784	12	0	0	3,127	6	0	0
WECC	1,475	4	2,311	32	170	10	4,426	8	506	2
Total	12,743	23	9,485	107	227	28	19,696	36	609	25

Table 20: NERC-wide Retirement Units by Fuel (2008 – 2011)

Fuel	MW	Percent
Coal & Lignite	2,106	14
Gas	11,588	79
Oil	854	6
Water	0	0
Other	99	1
Total	14,647	100

Table 21: NERC-wide New Commercial Units by Fuel (2008 – 2011)

Fuel	MW	Percent
Coal & Lignite	5,961	24
Gas	14,802	60
Oil	158	1
Water	609	2
Other	3,125	13
Total	24,655	100

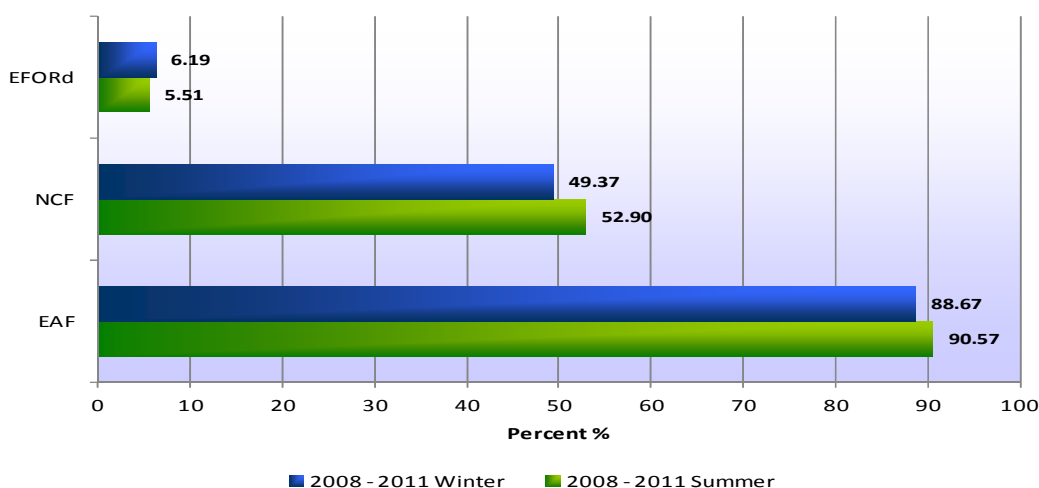
2008-2011 Review of Summer and Winter Availability

To address seasonality of unit availability from 2008 to 2011, unit information for the months of June to September (summer) and December through February (winter) were pooled to calculate forced outage statistics.⁹⁶ Figure 73 compares the average EAF, NCF and EFORD for the time periods of 2008 to 2010 and 2008 to 2011.

The average EAF during the winter improved between 2008 to 2010 and 2008 to 2011 by 0.5 percentage points, however, EAF during the summer worsened by a similar margin. The gap between summer and winter EAF is less in 2008 to 2011 than it was in 2008 to 2010. The difference can be attributed to the increase in forced outages as demonstrated by the increase in summer and winter EFORD in the two graphs. The surprising increase in EFORD was not related to full forced outage events but to an increase in the number of deratings caused by component failures. The losses due to full forced outage hours are about the same between the summer and winter periods. However, the increase in deratings between the two winter periods was only 5.6 percent and there was an increase of 3.4 percent between both summer periods.

In last year's report, we showed that during the spring season (March-May), 77 percent of the units took a planned outage (PO) for an average 231 hours or 9.6 days. During the fall season (October through November), only 42 percent of the units experienced a planned outage, and the average duration was shorter at 134 hours, 5.6 days. Some units took both spring and fall planned outages, although this is rare. Based on this assessment, generating units are well prepared for the summer peak demand. The resulting availability indicates that spring and fall maintenance effort were, on average, successful as measured by a higher EAF and a lower EFORD.

Figure 73: Seasonal EAF, NCF, and EFORD Rates Comparison



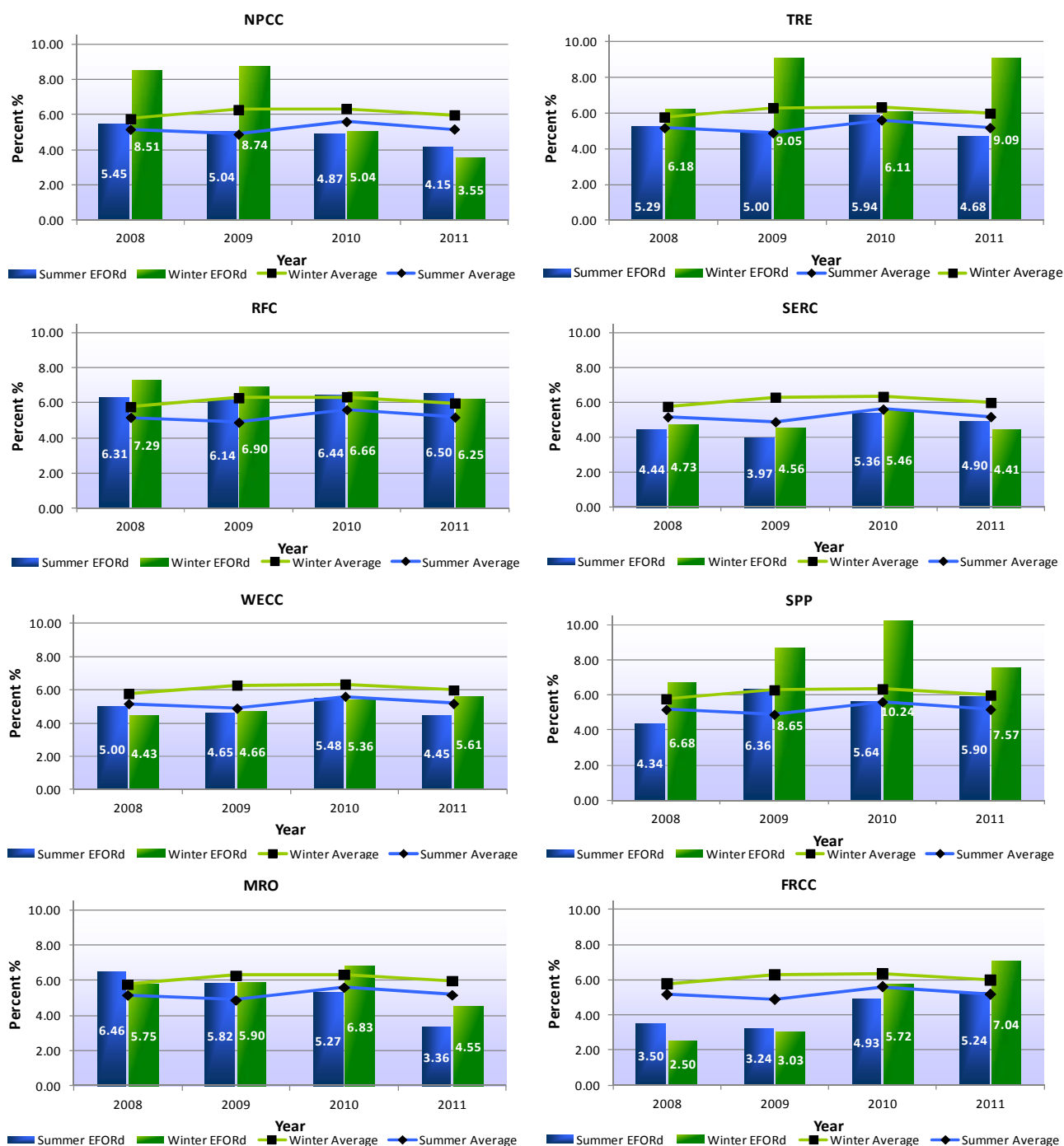
⁹⁶ A study of peak periods was conducted by the NERC Generating Availability Trend Evaluation (GATE) Working Group several years ago, see <http://www.nerc.com/files/Seasonal-Performance-Trends.pdf>.

The percent differences between 2008 to 2010 and 2008 to 2011 for EAF, NCF, and EFORD can be found in Table 22. Differences in EAF and NCF were found to be insignificant at around one percent, however, EFORD increased for both summer and winter periods by a margin of approximately 40 percent. There were much more immediate forced outages in 2011 due to weather-related events. Additional findings on these weather-related events are presented later in the report.

Table 22: Percent difference in Seasonal Averages between 2010 and 2011		
	Summer	Winter
EAF	-0.65 percent	0.56 percent
NCF	-0.99 percent	0.84 percent
EFORD	39.14 percent	40.36 percent

The summer and winter EFORD for each Region are presented in Figure 74. In each graph, the average EFORD for all reported units across all NERC Regions is also shown, with the lines on the graph representing the NERC average EFORD for each summer and winter period. In some cases, the regional averages (shown as bars in Figure 74) are below the national averages and other times they are above. The figure shows that in general across the Regions, summer EFORD is at or below the NERC average, while some Regions experienced higher winter EFORD values than average. The majority of winter issues were explained by natural events (freezing temperatures, icing, tornados, etc). For example, in the ERCOT Region, freezing temperatures and some freezing precipitation occurred across the Region during the month of December 2009. These weather events, some of which included significant icing on transmission equipment coupled with protection system misoperations, caused several unit trips. Then again in February 2011 a major cold wave swept across the ERCOT Region bringing with it extreme low temperatures, wind, ice, and snow, resulting in high winter peak electrical demand and cold-weather-related issues.

Figure 74: Summer vs. Winter EFORd Rates – 2008 - 2011



Review of Forced Outages Resulting in Automatic Grid Separation

Many times generating units will trip and automatically shut down without any operator action. In 2011, GADS started to track the automatic, forced outage events for all units. Although only 70 percent of the 2011 data was available at the time of this report, there were slightly more than 12,000 of these events captured by GADS.

Generating plants are not designed the same, nor do they operate the same. For example, hydro units do not have boilers. Another example is that gas turbines do not have coal mills. However, all units have generators, and from the electric generator to the transmission lines, all generating units have common equipment. Since this common equipment would, if any, have an effect on the bulk power system, it is important to determine if any forced, automatic outage problems associated with this common equipment could have affected the bulk power system.

Table 23 below lists the top causes of automatic grid separations ranked by the number of occurrences. Only the “common” equipment or causes that all generating units share are listed.

Table 23: Groups of Specific GADS Cause Codes with Descriptions	
Cause Codes Groups	Number of occurrences
(4500-4899) Generator / Exciter and Associated Controls	1,173
(9300) Transmission system	1,141
(3600 - 3799) Electrical equipment including substations	972
(9000-9036) External (weather)	555
(9200 - 9291) Fuel Quality	508
(9900-9960) Personnel, Maintenance or procedure errors	386

The top cause of automatic unit trips is the electric generator and exciter equipment. These cause codes include problems with the stator, bearings, hydrogen system, oil lubrication and other areas related to the unit. There were 29 events that caused units to be offline for more than 1,000 hours, and 10 events that caused units to be offline for more than 3,000 hours. These events were local to the facility and had no affect on the bulk power system.

The second most common cause of automatic unit trips is transmission related problems. The vast majority of these outages lasted for a short period of time, with only nine events lasting more than 200 hours, and one event lasting more than 3,000 hours. These are inconvenient outages, and most of them affect only the local area and have no affect on the bulk power supply because other generating plants pick up the load.

The other top problems (other than weather related outages) are also local problems within the plants, which do not affect the bulk power system or other generating units outside the plant location.

Multiple Unit Forced Outages and Causes

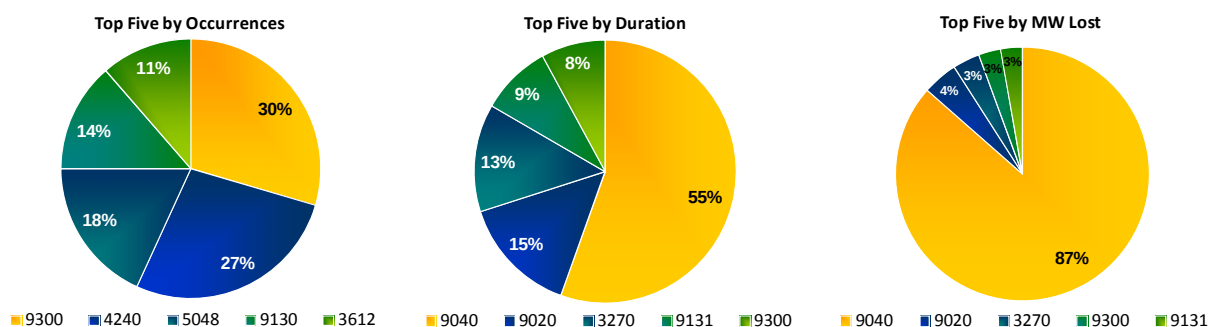
Multiple unit forced outages constitute a reliability risk to the bulk power system, and this has prompted the industry to monitor and track these types of trips. Table 24 provides data on the annual multiple-unit forced outage trips that occurred in the 2011 assessment year. Last year's report evaluated the number of trips from generators rated at 20 MW and above occurring from 2008 to 2010. With mandatory reporting beginning in 2012, the GADSWG decided to only include in the study units which are rated at 50 MW and above. Trips were analyzed in two distinct summary ranges for Net Dependable Capacity (NDC): $450 \leq 749$ MW and $750+$ MW. For example, a trip of "two units" is classified as any combination of unit capacity with the total amount of lost capacity equaling $450 \leq 749$ MW or $750+$ MW.

Total Net Dependable Capacity is a summation of the total generation that tripped automatically at once. The total of multi-unit trips was determined by evaluating unit proximity (Region and state) and event times within five minutes. Figure 75 summarizes the analyses completed on the available 2011 data.

Table 24: Frequency of Multiple Unit Forced Outages						
Units per Trip	Total NDC (MW)	Units Tripped	Trips	Outage Duration Total	Average Outage Hrs/Trip	Average Outage Hrs/Unit
Two	$450 \leq 749$	62	31	1,198.75	38.67	19.33
	≥ 750	30	15	280.48	18.70	9.35
Three	$450 \leq 749$	120	40	1,488.79	37.22	12.41
	≥ 750	12	4	2,129.57	532.39	177.46
Four	$450 \leq 749$	128	32	627.64	19.61	4.90
	≥ 750	24	6	136.27	22.71	5.68
Five*	$450 \leq 749$	15	2	99.54	49.77	6.64
	≥ 750	64	8	935.51	116.94	14.62

*Represents five or more units that tripped at the same time during one event

The following three tables represent the top five causes by the number of occurrences, total duration or outage time, and total MW lost respectively during the trips. Only a total NDC of 450 or greater was included in the analyses. In Table 25, causal code 9300 was determined to be the most frequent cause of multi-unit trips cited in 2011. Transmission related problems (code 9300) equated to a total of 56 units automatically forced offline. In Table 26 and Table 27, causal code 9040 is cited as the top event type. Upon further investigation, it was found that this was the result of tornados which swept across Alabama in late April, resulting in a massive loss of generation. These losses represent over 80 percent of the top five causes of MW lost due to multi-unit forced outages in 2011.

Figure 75: Top Five Causes for Multiple Unit Trips - 2011**Table 25: Top Five Causes of Multiple Unit Forced Outages by Number of Occurrences**

Cause Code	Cause Code Description	Number of Events
9300	Transmission system problems other than catastrophes	13
4240	Steam Turbine Bearings	12
5048	Gas fuel system	8
9130	Lack of fuel (coal mines, gas lines, etc) where the operator is not in control of contracts, supply lines, or delivery of fuels	6
3612	Switchyard system protection devices - external	5

Table 26: Top Five Causes of Multiple Unit Forced Outages by Total Duration (Hrs)

Cause Code	Cause Code Description	Duration
9040	Other catastrophe (Tornados)	2,036
9020	Lightning	535
3270	Intake system problems other than traveling screens	488
9131	Lack of fuel (interruptible supply of fuel part of fuel contract)	321
9300	Transmission system problems other than catastrophes	290

Table 27: Top Five Causes of Multiple Unit Forced Outages by Total MW Lost

Cause Code	Cause Code Description	MW Lost
9040	Other catastrophe (Tornados)	2,311,796
9020	Lightning	119,721
3270	Intake system problems other than traveling screens	92,572
9300	Transmission system problems other than catastrophes	75,278
9131	Lack of fuel (interruptible supply of fuel part of fuel contract	73,883

Influence of Renewables on Reliability

In some Regions, renewable capacities and generation have increased significantly in recent years. There is evidence that wind generation does not coincide with peak demand hours but rather during the late evening or early morning hours. This has resulted in conventional steam generating units being dispatched during these off-peak hours to loads that are lower than those for which the plants were designed. More data and analysis is needed to measure whether this low load off-design operation will impact unit availability.

Suggestions for Improving the Quality of Data

The Generating Availability Data System Working Group (GADSWG) used GADS data to analyze the data for this report. GADS has provided a good foundation, however, there are areas where it should be improved in order to allow more thorough analyses of power plants and their impact on the bulk power system. The following suggestions, if implemented could address key shortcomings in the current dataset related to unit design data and event descriptions.

Design Data in GADS

When mandatory GADS reporting was implemented in 2012, the mandatory design data was limited to nine items based on concerns expressed by a few industry stakeholders. In order for NERC members to benchmark their plants against their peers, more design data will be required. In many cases, plant reliability is affected by the reliability of manufacturer supplied equipment. Complete design data is needed in order to evaluate problems with a particular type of equipment. As manufacturers provide equipment modifications to eliminate design issues and improve reliability, these modifications need to be tracked in GADS design data so that the industry can conduct studies to determine if reliability has improved. Pollution control equipment can also affect reliability; this equipment should be tracked in GADS design data especially given the number of new scrubbers and SCRs added in recent years. Next, there is a concern that newer plants may have less redundant equipment and are less reliable. In order to evaluate the reliability of plants without redundant equipment vs. others, it will be necessary to have more design data. Previously, the GADSTF Design Subgroup reduced the amount of design data needed. Submission of the GADSTF design data is highly recommended and should be considered as a mandatory item in the future. The software to submit the data is available from NERC.

Event Descriptions in GADS

The event description field for a GADS event is currently an optional field and in many cases is often left blank. The event description can be compared to cause codes in order to verify whether or not the correct cause code(s) were selected. Several GADSWG members reported matching event descriptions to cause codes as part of their data review process. Under mandatory GADS reporting, each reporting company is expected to review their events for correctness. If no description is provided, there is no way for the reviewer to verify that the cause code is correct. When GADS data is analyzed for reliability trends (as in the annual report), the results can be misleading if incorrect cause codes are reported. Companies should review events and require reporting units to provide complete and accurate event descriptions.

Conclusion

During 2008 to 2011, the overall performance of generating units changed insignificantly, and analysis suggests that overall, the generating fleet within the NERC footprint remains reliable. Furthermore, availability is adequate to meet load and respond to unplanned events. The average Equivalent Availability Factor (EAF), which measures the overall availability of generating units, decreased in 2010 but slightly recovered in 2011. At the same time, the average Net Capacity Factor (NCF), an indicator of energy production, decreased in 2009, and rebounded in 2010 and 2011. The average number of forced outages in 2010 is greater than in 2008, while the average planned outage times have slightly increased. As a result, the EFORD also increased which illustrates that more units have experienced forced events during peak-demand times in 2010 than in the previous two years. However, in 2011, the time for planned outage increased slightly, resulting in a slightly lower EFORD. More or longer planned outage time is needed to repair the generating fleet. Whether age is the cause of the increased need for planned outage time remains unknown, and further investigation into the cause for longer planned outage time is warranted, if the trend continues.

A large number of generating units were retired from service over the last four years. However, a larger number of units started commercial operation over the same time period. The majority of new units (60 percent) use natural gas as their fuel. Based on MW capacities, there are about three times as many new coal units coming online from 2008 to 2011 than those put into retirement.

Summer months (June through September) out produced the winter months (December through February) again. When we compare the 2008 to 2010 and 2008 to 2011 data, there is a mix of increases and decreases between the summer and winter periods. In 2008 to 2011, the differences between the EAF and NCF summer-winter periods are much smaller than the 2008 to 2010. EFORD in 2008 to 2011 is due mostly to increased equipment, storms and related transmission problems.

From 2008 to 2011, there were a large number of multiple-unit outages resulting from the same event types. Investigations show that the top reasons for multiple outages are caused by transmission or weather-related events.

Finally, based on the information assessed, generating units continue to be reliable with no affect on the bulk power system from an overall, annualized perspective.

Demand Response Availability Analysis

Introduction

This chapter focuses on Demand Response enrollment and event information from the 2011 summer collection period; which was Phase II's first reporting period. This includes actual Demand Response performance information from April 1 – September 30, 2011 across 133 entities administrating Demand Response programs within North America.

NERC is reviewing the North American Demand Response enrollment and event information to provide the appropriate reliability performance trends to monitor. No conclusions as to the absolute value of any of these metrics can be drawn at this time due to this being the first year of data collection.

Further, the metrics should not be compared between Regions or subregions as their bulk power system characteristics and market structures differ significantly in terms of resource-mix, system and market design, load characteristics, and simple physical, geographic, regulatory, and climatic conditions.

The metrics in this report have been vetted by the industry via the Demand Response Availability Data System Working Group (DADSWG) and are part of a preliminary set of metrics. The DADSWG intends to continue to develop metrics and reports from DADS to ensure proper trending and reliability analysis is performed.

The DADSWG expects with publication of this data, issues may be identified which require review and modification of the reported data. The list of metrics will change over time. In some cases, the database for a given metric does not yet contain enough historical information to reveal useful information. The selections here and in the future will be based on the ranking process, which recognizes a metric's potential for indicating impending reliability issues and performance.

This activity is only in its early stage. Identifying benchmarks for performance is a separate and future activity which may aid the industry in quantifying Demand Response reliability performance.

Background

Demand Response is one of many resources used to satisfy the increasing demand for electricity in North America. First, Demand Response provides capacity for resource adequacy and planning purposes. Secondly, capacity and ancillary services provided by Demand Response helps ensure resource adequacy while providing operators with additional flexibility in maintaining operating reliability. Although Demand Response is not a new resource, the increased usage and varying applications of Demand Response, compared to the past, demonstrate that NERC and stakeholders should evaluate its performance to gauge effects on reliability. More complete information about the performance of Demand Response will also help the industry develop confidence in relying on Demand Response as a resource.

NERC established a Demand Response Data Task Force (DRDTF) in early 2008 based on recommendation from the Demand-Side Management Task Force (DSMTF) because the

industry needed a more systematic approach for collecting and quantifying Demand Response performance. The DRDTF specified statistics to quantify demand response performance and the data collection requirements necessary to develop the Demand Response Availability Data System (DADS). In December 2011, the DADSWG was formed with Operating and Planning Committee approval. The DADSWG will continue the efforts of the DRDTF by implementing a uniform approach to reporting and measuring Demand Response availability, performance and other related reliability data.

DADS will be implemented in four phases. The current phase of DADS, Phase II, is mandatory and focuses on reliability or event related Demand Response programs which are both dispatchable and controllable. Phase I was voluntary, and Phases III and IV incorporate the reporting of various types of non-dispatchable Demand Response. Phases III and IV will be implemented once sufficient Phase II data is collected and validated and requirements for non-dispatchable Demand Response are determined. The approximate implementation of Phase III is the summer 2013 reporting period.

DADS collects Demand Response enrollment, event, and participation information to measure actual performance including its contribution to improved reliability. Ultimately, this analysis can provide industry with a basis for projecting contributions of dispatchable and non-dispatchable (e.g., price-driven) Demand Response that supports forecast adequacy and operational reliability. DADS provides a consistent and timely basis for counting and validating the contributions at the different NERC functioning levels.

Responsible Entities are required to submit DADS data. These entities are defined as a NERC registered entity that either dispatches a demand response resource and/or administers a demand response program, product or service. Responsible Entities for DADS data submittals are limited to the NERC registered Entity types listed in Table 28.

Table 28: NERC Responsible Entities for DADS Reporting	
Function Name	Responsible Entity
Balancing	Balancing Authority
Distribution	Distribution Provider
Load-Serving	Load-Serving Entity
Purchasing-Selling	Purchasing-Selling Entity

DADS requires data for all demand response programs currently in effect. However, Responsible Entities are only required to register and submit data on demand response programs if:

1. The program has been commercially in service for more than 12 months; and
2. The program has enrolled 10 MW or more of combined demand response resources.

Summer 2011 Reporting Period Summary

The 2011 Summer Reporting Period had 100 percent participation from 133 entities that were required to provide input. Table 29 depicts an overall snapshot of the enrollment and event information that was collected from those entities. Entities that only had economic demand response programs were not required to report, and NERC anticipates the number of reporting entities may grow to over 200 once Phase III and IV are implemented.

In 2011, North America had the second warmest summer on record with an average temperature of 74.5°F⁹⁷. This record temperature factored into the months of June, July, and August having the largest number of events called and number of enrolled resources and capacity. August had the largest enrollment out of the six months with a total of 7,360,605 resources and 56,601 MW. There were 664 events during April through September 2011 with July (247 deployments, 16,283 MW with a 70 percent Realization Rate⁹⁸) and August (153 deployments, 10,896 MW with a 77 percent Realization Rate) being the most active, as expected. The summary table below shows the basic information from the data collected.

Table 29: Demand Response Enrollment and Event Information for 2011 Summer Reporting Period (April – September 2011)	
Total number of entities reported	133
Average enrolled resources each month	6,914,798
Total maximum enrolled resources (in August)	7,360,605
Average enrolled capacity (MW) each month	53,005
Total maximum enrolled capacity (MW) (in August)	56,601
Total number of deployment events ⁹⁹ (April to Sept.)	664
Total deployment (MW) from April to Sept.	49,721
Total realized demand reduction rate	65 percent (32,305 MW)
Average sustained response period	2 hours 51 minutes

Demand Response Enrollment

Program enrollment data includes aggregate information about the number of resources (end use customers, ranging from individual residential loads up to large industrial facilities) and registered demand response capacity (MW) on a monthly basis. Figure 76 and Figure 77 depict the total number of registered resources and total capacity available each month. These figures illustrate the unique resources and MW that could be called upon for use in reliability

⁹⁷ <http://www.ncdc.noaa.gov/sotc/national/2011/8>

⁹⁸ Realization Rate is defined as Actual MW achieved for event / MW requested for event.

⁹⁹ Note that in present DADS reporting, when a Demand Response deployment is called, resources in different local zones are counted as different events.

situations on a regional and NERC level. Figure 76 and Figure 77 eliminate the possibility of unintentional double-counting Demand Response resources.¹⁰⁰

Total Registered Demand Response Resources by Regional Entity

Figure 76: 2011 Summer Total Registered Demand Response Resources by Regional Entity (Includes NERC-Wide)



¹⁰⁰ There are two situations in which double-counting of Demand Response resources could occur:

1. When aggregation occurs up to a Balancing Authority, multiple enrollments for a given product category (Capacity, Reserves, Regulation or Energy) could occur; and/or
2. When resources are jointly enrolled in multiple product categories within a single entity.

On a NERC level, April and May had the lowest registration of resources out of the six month reporting period. April has 12 percent fewer registered resources, and May has 10 percent fewer registered resources than the NERC average. July and August had the largest registration of resources out of the six month reporting period. Compared to the NERC average, July had five percent more registered resources, and August had six percent more registered resources. This is typically due to some demand response programs that are only active during the summer months. For example, demand resources for certain PJM programs can only be activated starting in June for the summer period.

Total Registered Demand Response Capacity

On a NERC level, April and May had the lowest registered capacity out of the six month reporting period. April has 12 percent fewer registered MW, and May had 10 percent fewer registered MW than the NERC average. July and August had the largest registered capacity out of the six month reporting period. July had five percent more registered MW, and August had six percent more registered MW than the NERC average. The average capacity of all reported resources is 8 kW of Registered Capacity.

The RFC Region has the largest demand response capacity with an average 24,386 MW registered each month, which is almost half of NERC's 53,005 MW average.

Figure 77: 2011 Summer Total Registered Demand Response Capacity by Regional Entity (Includes NERC-Wide)¹⁰¹

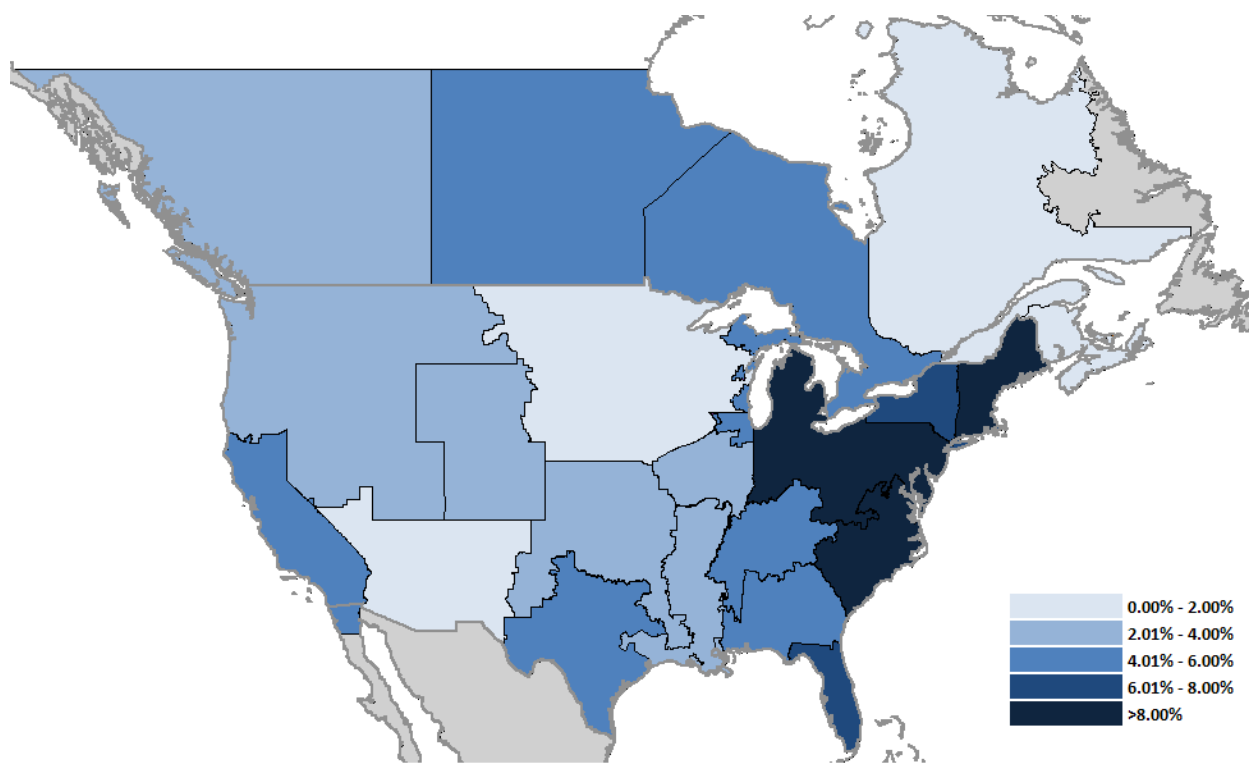


Registered Demand Response as a Percentage of Total Internal Demand

Figure 76 and Figure 77 above reemphasize the assumption that Demand Response is typically enrolled more during the summer peaking months of June through August. Figure 78, below, illustrates the percentage of registered Demand Response capacity that potentially could be used to reduce load served and/or relieve transmission constraints during those peak months by comparing each subregion's peak demand to registered demand response. In areas of SERC, RFC, and NPCC the potential of Demand Response to meet its demand requirements is as high as or higher than eight percent.

¹⁰¹ Figure displays total DR MWs actually registered in Regional Entity footprint and NERC wide. NERC's LTRA reports show only the portion of DR expected to be available during peak demand. These numbers are not comparable.

Figure 78: 2011 Summer Registered Demand Responses as a Percentage of Total Internal Demand*



**Approximate NERC subregional boundaries are used*

**Calculations in the creation of the map represent the 2011 peak of registered subregion Demand Response as a percent of 2011 summer peak total internal demand.*

Demand Response Program Categories

DADS collects three reporting types for controllable and dispatchable demand response. They are:

1. **Demand Response Reliability Event:** Participation where resources are obligated over a defined period of time to provide Demand Response upon deployment by the appropriate Balancing Authority, Load Serving Entity, Distribution Provider, etc. Reliability Event Data refers to emergency or contingency events, not economic Demand Response deployments.
2. **Market Participation:** Programs where Demand Response resources are scheduled to supplement generation based on market conditions or market offers. Market Participation may cover any type of dispatchable Demand Resources that are scheduled or dispatched primarily on an economic basis.
3. **Ancillary Services:** Demand Response Services, as defined in FERC Order 888-A¹⁰², as those services that are necessary to support the transmission of capacity and energy from resources to loads while maintaining reliable operation of the Transmission Service

¹⁰² <http://www.ferc.gov/legal/maj-ord-reg/land-docs/order888.asp>

Provider's transmission system in accordance with good utility practice. Ancillary Services provided by Demand Response typically fall into two primary categories: reserves and regulation.

All Demand Response reporting types will be categorized as one of the following products:

1. **Energy:** Demand resources that are compensated based solely on demand reduction performance of specific amount of electricity during a demand response event, typically the general energy market.
2. **Capacity:** Demand side resource that displaces or augments generation for planning and/or operating resource adequacy with an obligation to deliver the capacity as energy during a fixed contract period.
3. **Reserve:** Demand resources obligated to be available to provide demand reduction upon deployment by the system operator, based on operating reserve capacity requirements that are established to meet applicable reliability standards.
4. **Regulation:** Demand resource increase or decrease load in response to real-time signals from the system operator that are subject to dispatch continuously during a commitment period in response to changes in grid frequency, and also are subject to continuous dispatch based on instructions from the system operator. Provision of Regulation Service does not correlate to Demand Response Event timelines, deadlines and durations.

Figure 79 illustrates the relationship of a variety of Demand Response to Demand-Side Management services, how load reductions are implemented, the ability to dispatch a given resource, and the type of product or service that ultimately provides the MW. While four products are identified with dispatchable Demand Response Programs, there are multiple services for any product in DADS. The eight service types collected in DADS during Phase II reporting are Direct Control Load Management, Interruptible Load, and Critical Peak Pricing (CPP) with control, Load as a Capacity Resource, Spinning Reserves, Non-Spinning Reserves, Emergency, and Regulation. These services can be found in Figure 79 on the left side of the flow chart under Dispatchable and Reliability. The Non-Dispatchable and Economic service types will be collected in Phase III and IV.

Figure 79: Demand Side Management Categories

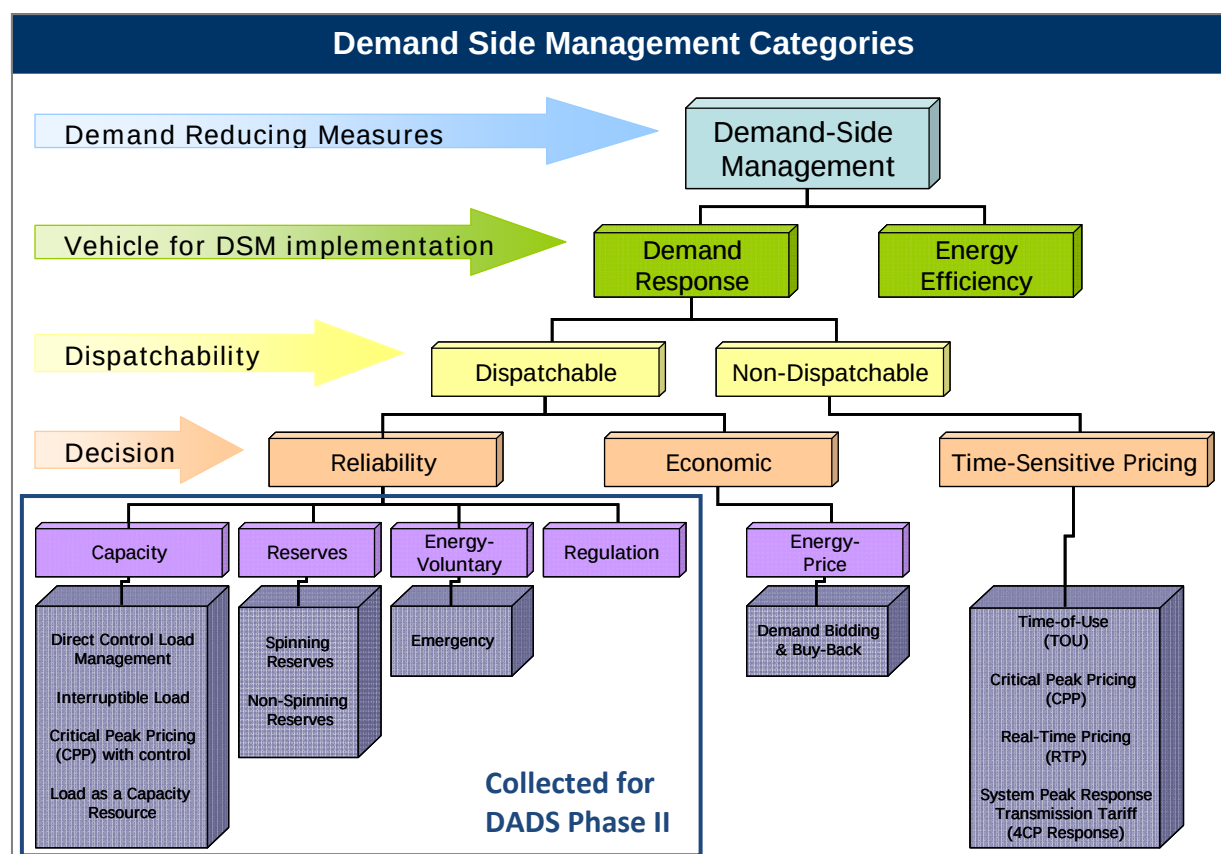
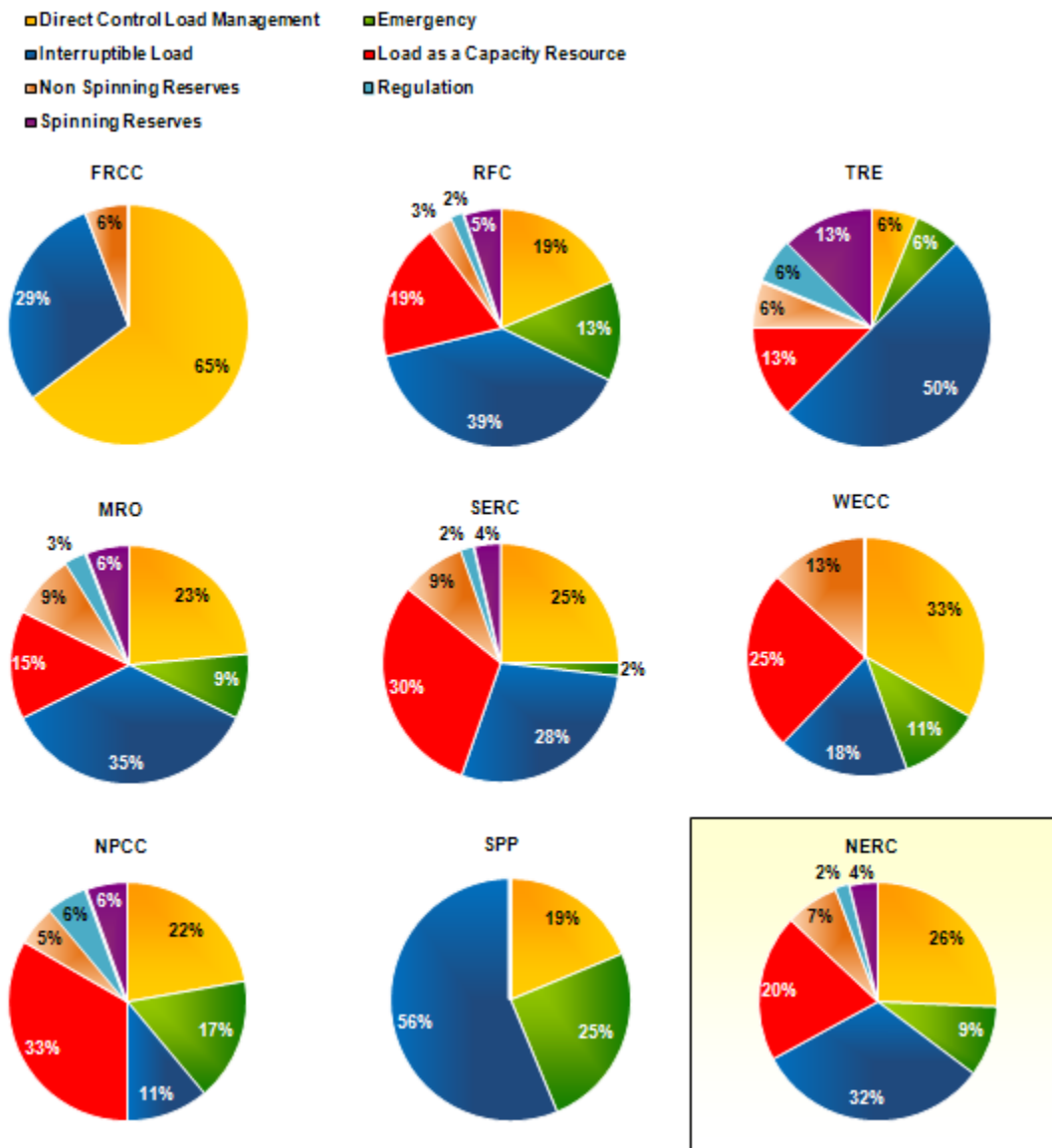


Figure 80 illustrates the percentage of different reliability service types that entities participated in for the 2011 summer reporting period. On a NERC level, there was a total count of 261 service type programs. The largest count of service types were Interruptible Load programs at 32 percent and Direct Control Load programs at 26 percent of total collected service types. The lowest count of service types were Spinning Reserve programs at 4 percent and Regulation programs at two percent of total collected service types. Note that programs vary in size and some load enrolled in more than one program type; this data does not reflect actual participation.

This was an expected result. As previously reported in NERC's reliability assessments, Demand Response providing ancillary services is still relatively new in most Regions. Generally, Direct Load Control Management (DCLM) is a service type commonly supported by residential and commercial loads, while Interruptible Load (IL) is commonly supported by large industrial load. Length of Ramp Periods are key differences between these two service types—DCLM will typically be a shorter Ramp Period, while IL is longer and may be sustained for several hours.

**Figure 80: 2011 Summer Service Type Enrollment Count by Regional Entity
(Includes NERC-Wide)**



Reliability Event Details

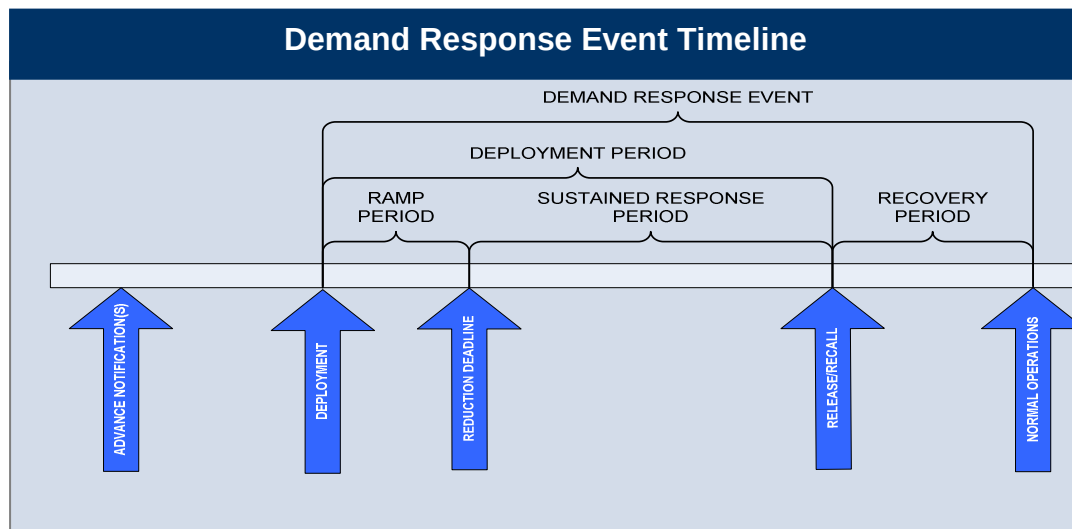
Reliability event data is reported for Demand Response services in which resources are obligated to provide Demand Response upon deployment by the appropriate system operator. Reliability event data refers to emergency or contingency events, not economic Demand Response deployments. The event information includes the following attributes:

- Event Type and Reason
- Product/Service Type (Capacity or Reserves)
- Zone
- Advance Notification, Deployment, Reduction Deadline, Release/Recall, and Normal Operations Date/Time
- Committed Load Reduction (MW)
- Number of Committed Resources

Note that in present DADS reporting, when a Demand Response deployment is called, resources in different local zones are counted as different events.

Figure 81 provides the framework for the Responsible Entity to report Demand Response event timeline data on a consistent basis. The figure represents the terms for timing events and time durations applicable to the characteristics of a Demand Response Event. Certain criteria are not captured by entities during a Demand Response event including Advanced Notification Time and Normal Operation Time, but for every event the Deployment, Reduction Deadline, and Release/Recall date and time were collected.

Figure 81: Demand Response Event Timeline¹⁰³



¹⁰³ Please see <http://www.naesb.org/dsm-ee.asp> for more information on NAESB M&V Standards.

The NERC six-month average Sustained Response period was 2 hours 51 minutes per event. July had the longest average Sustained Response period at 3 hours 32 minutes, and April had the lowest average Sustained Response period at 1 hour 32 minutes.

For all 261 programs captured for the 2011 summer reporting period, there were a total of 664 events¹⁰⁴. The statistics vary by Region and program characteristics and size, but on average each program was called upon 2.54 times during the 2011 summer reporting period. Figure 82 shows the number of reliability-driven demand response events that happened during the 2011 summer reporting period by Region. Out of 664 NERC wide reliability events, RFC has the most with 32.7 percent of the total, and MRO had the least with 1.5 percent of the total.

Figure 82: 2011 Summer Total Number of Demand Response Events by Regional Entity¹⁰⁵
(Includes NERC-Wide)

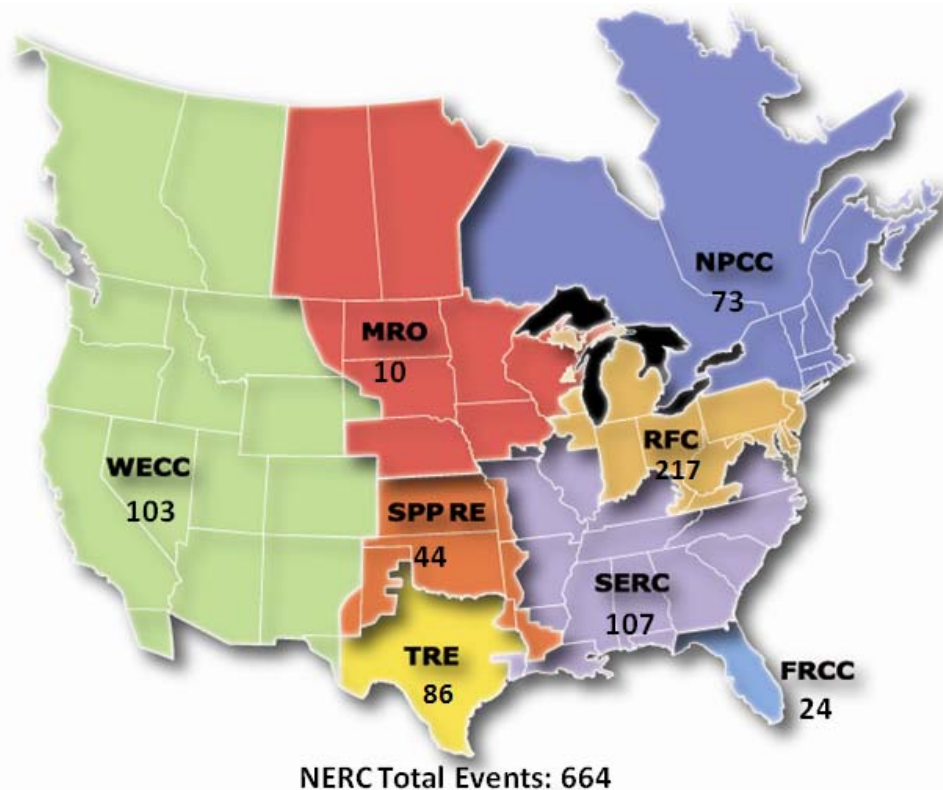


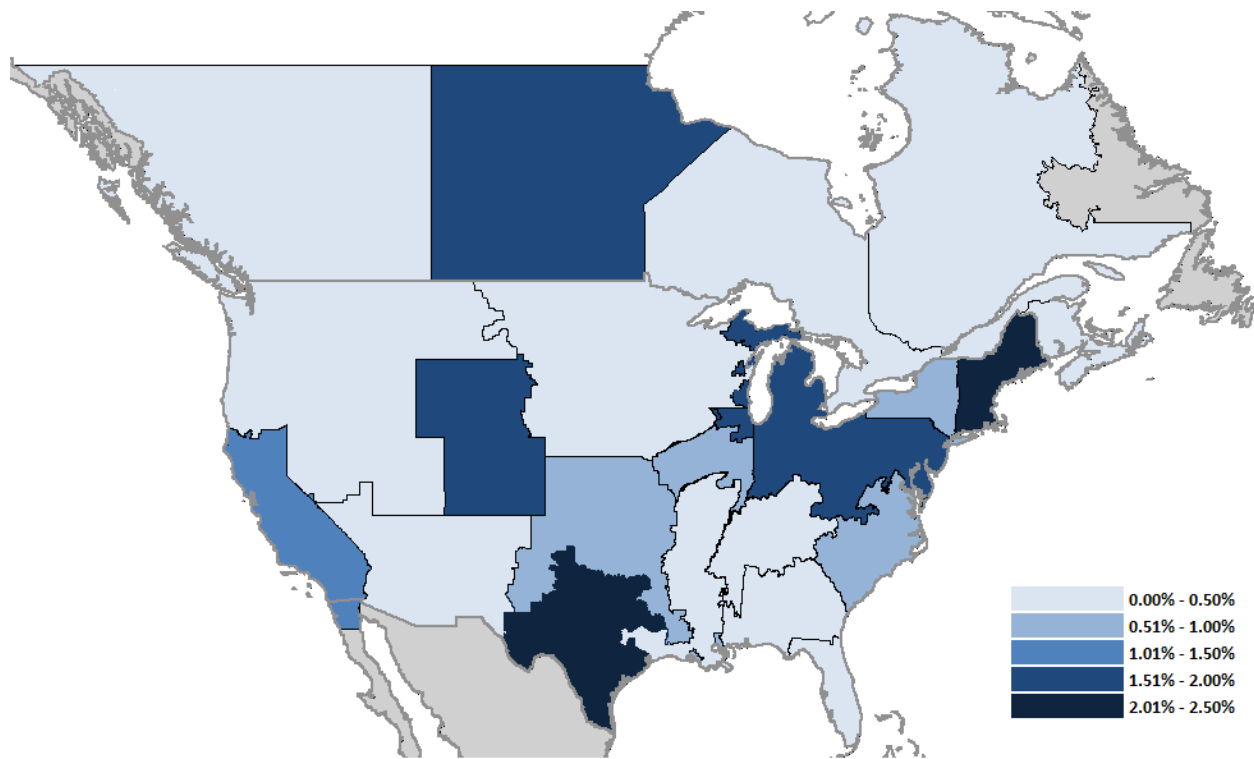
Figure 83 displays the percentage of each Region's total internal demand being met with Demand Response for the peak conditions observed during the summer. Achieved MW reduction is critical in assessing the significance of Demand Response reliability. Regions with a higher percentage may be more susceptible to issues should decreased customer participation in Demand Response occur in the future. Participation and performance of these programs will

¹⁰⁴ Note that in present DADS reporting, when a Demand Response deployment is called, resources in different local zones are counted as different events.

¹⁰⁵ Note that in present DADS reporting, when a Demand Response deployment is called, resources in different local zones are counted as different events.

be monitored over time to determine if these Demand Response programs can be counted on to relieve transmission constraints.

Figure 83: 2011 Summer Reduction Realization as a Percentage of Total Internal Demand from Demand Response*



*Approximate NERC subregional boundaries are used. Calculations in the creation of the map represent the 2011 peak of realized subregion Demand Response as a percent of 2011 summer peak total internal demand.

Figure 84 illustrates the number of monthly deployed demand response programs by Regional Entity. The summer months of June, July, and August had the most events while April and May had the least. DADS summer reporting is April 1 – September 30, 2011, but several entities programs are only active when demand is high during the months of June through August. This explains the decrease in resource registration, capacity registration, and low number of events in the months April and May. Six of eight Regional Entities had the least events in April, and five out of the eight Regional Entities had the most events in July. Overall July and August had the most Demand Response events with 247 and 153.

Figure 84: 2011 Summer Monthly Number of Demand Response Events¹⁰⁶ by Regional Entity (Includes NERC-Wide)

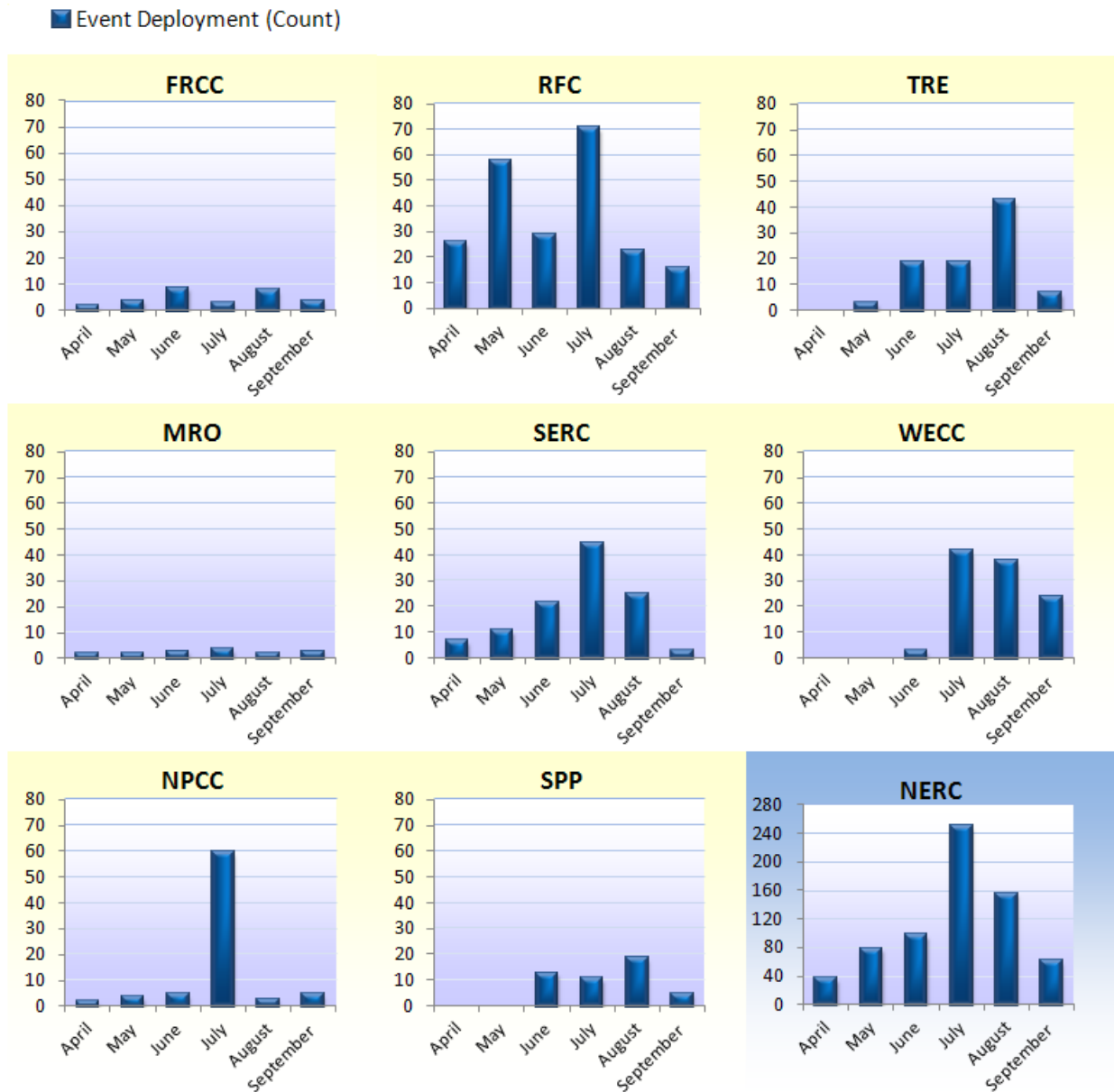
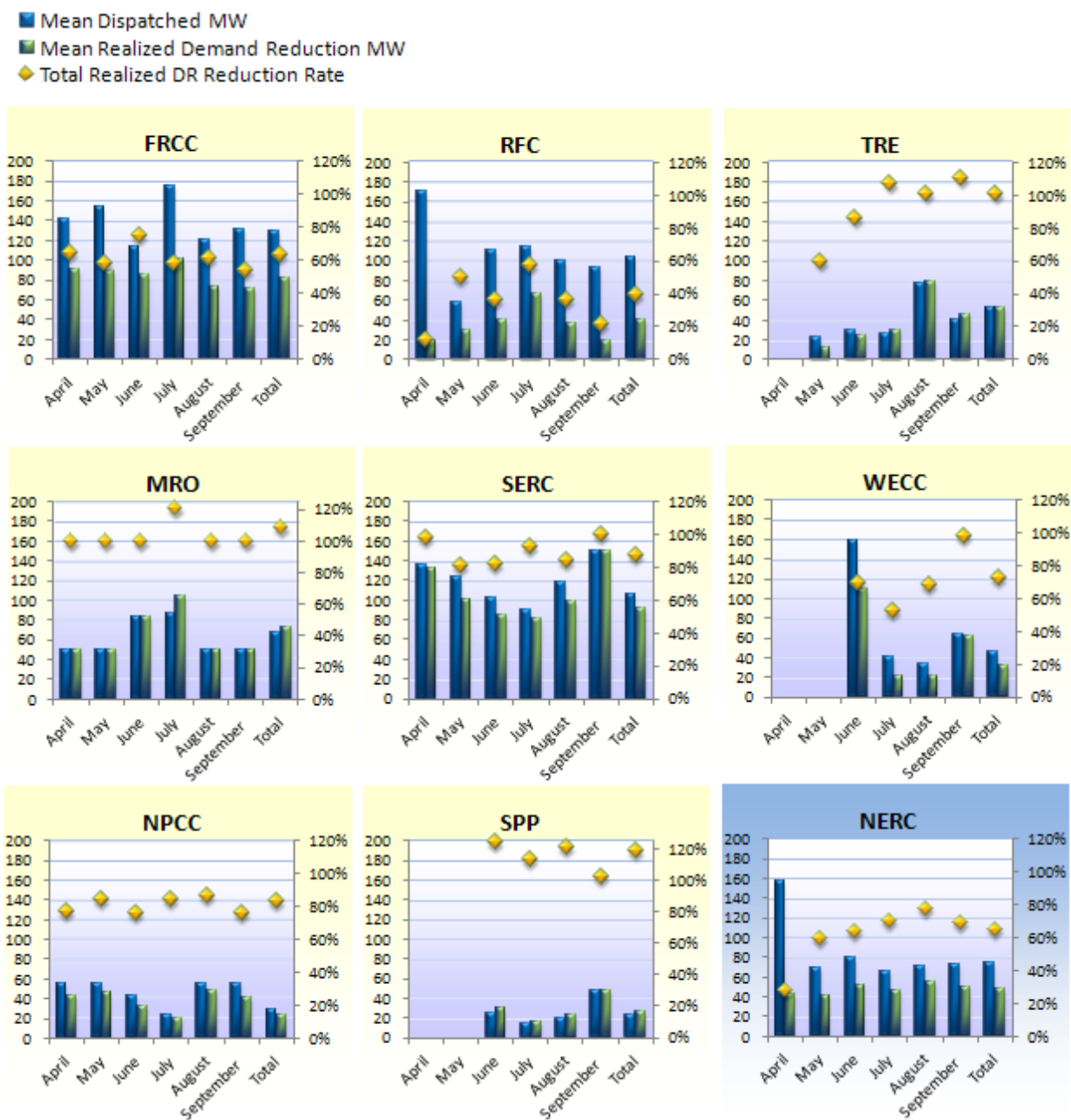


Figure 85 depicts the Demand Response event performance by participants within a Regional Entity footprint. The mean dispatched MW per event per month, mean realized demand reduction per event per month, and total realization rate per month are shown. On a NERC total, each event dispatched an average 75 MW and realized an average 49 MW, or a realization rate of 65 percent. NERC's April realization rate is 27.61 percent. NERC will monitor April's performance in future reporting periods to determine if this is a continuing trend or just an anomaly such as data enter error due to first mandatory reporting period in a new system.

¹⁰⁶ Note that in present DADS reporting, when a Demand Response deployment is called, resources in different local zones are counted as different events.

**Figure 85: 2011 Summer Demand Response Event Performance by Regional Entity
(Includes NERC-Wide)***



* Mean Dispatched MW and Mean Realized Demand Reduction MW displayed on left Y-axis.
Total Realized DR Reduction Rate displayed on right Y-axis.

Ancillary Services

Ancillary Services provide round-the-clock reliability in the form of regulation services, and can also be used for contingencies in the form of spinning and non-spinning reserves. Ancillary Service Product data is reported at a monthly level, providing a monthly summation of all activity related to ancillary services provided by demand response. The average number of hours per month for which Demand Response resources were offered or procured, the average number of hours per month for which Demand Response resources were actually deployed for use, and average hourly committed Demand Response Capacity by Demand Response resources per month are all displayed in Figure 86 and Figure 87. Spinning and non-spinning reserves are displayed on different figures to graphically represent the participation and capacity of each type. No reserve participation was recorded for the 2011 summer reporting period. Even though not all Regions participate, these figures display how ancillary service demand response plays a vital role in the reliability of the bulk power system in various Regions of North America. For example, spinning reserves for ERCOT within the TRE footprint had an average hourly committed Demand Response capacity of 1,100 MW. NERC spinning reserve average participation per month was 396 hours out of 443 hours with an average hourly committed Demand Response capacity of 392 MW. No Ancillary Service data was submitted for FRCC, MRO, NPCC, SERC, and SPP Regions.

Figure 86: 2011 Summer Spinning Reserves Ancillary Service Availability and Participation by Regional Entity (Includes NERC-Wide)

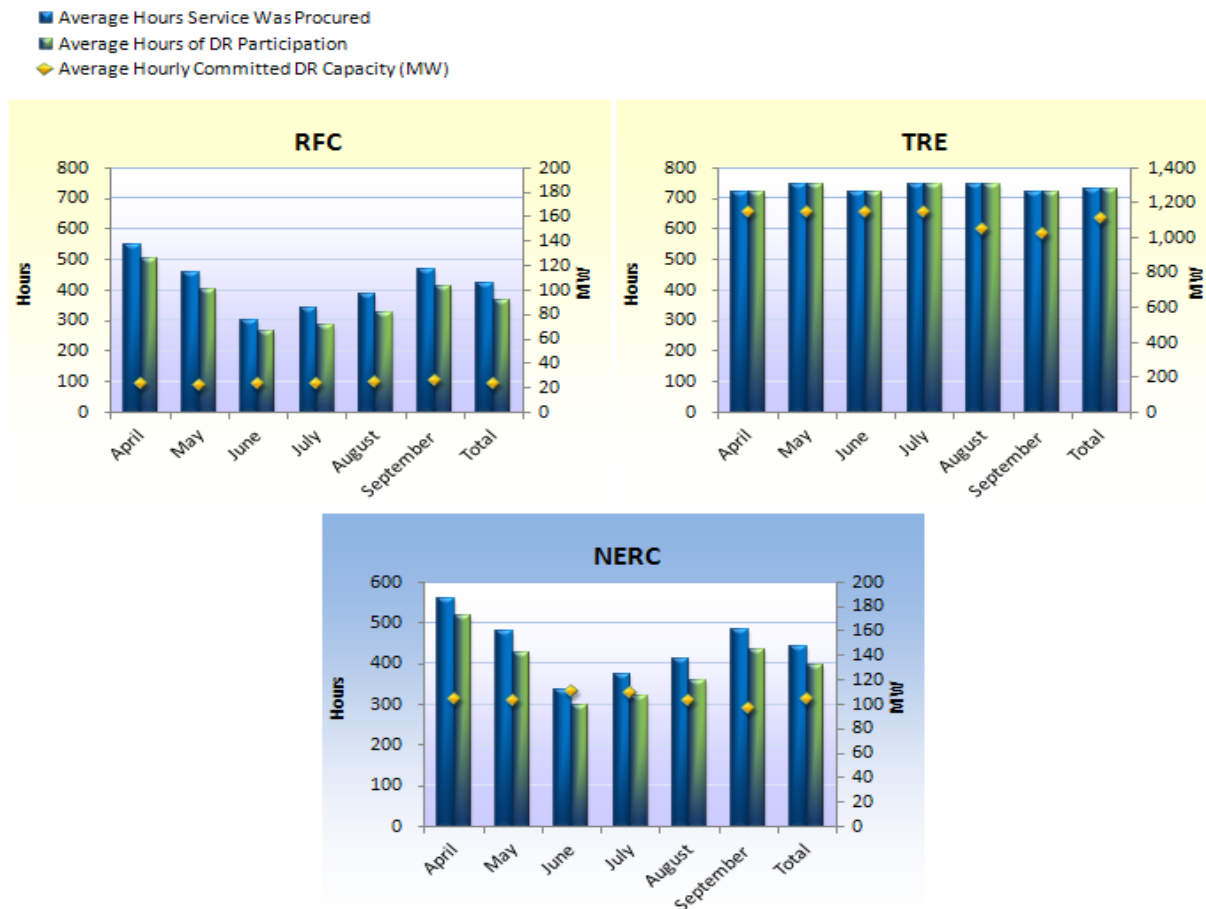
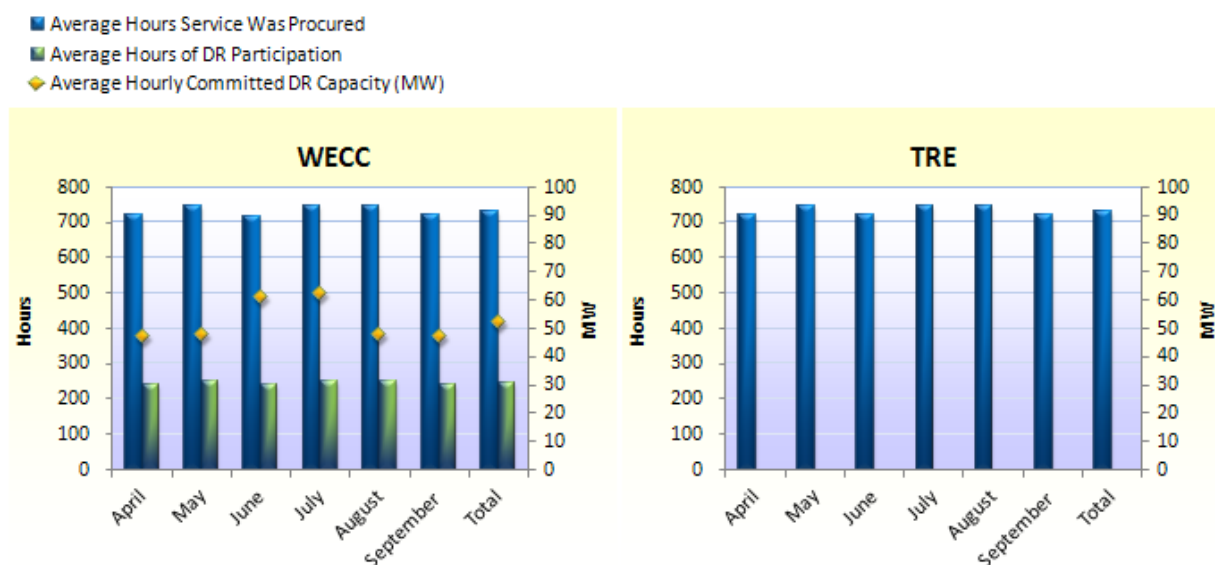


Figure 87: 2011 Summer Non-Spinning Reserves Ancillary Service Availability and Participation by Regional Entity



Conclusions

Demand Response is an increasingly important component in the overall portfolio of resources available to reliably meet the increasing demands for electricity in North America. The DADS system was designed to enable NERC to receive, manage, assess and disseminate data on Demand Response Programs, products and services administered by retail and wholesale entities throughout North America. The 2011 summer reporting period is the first mandatory reporting period, and issues may be identified which require review and modification of the reported data. The metrics collected now may change over time. Going forward, DADS will be a repository of historical Demand Response information for use in a wide range of applications for both planning and operating of the bulk power system. Performance metrics and data will help improve Demand Response projections by providing load forecasters, resource planners, and analysts with a comprehensive database for North America.

2011 Post Summer Assessment

Operational Highlights

Although each NERC Region is inherently different, many share similar operating challenges from season to season. Sharing these experiences and subsequent lessons learned with the industry can be helpful in developing solutions to mitigate or otherwise prevent future reliability issues. 2011 was a very hot summer and served recording breaking load in several parts of the system.

With the second warmest North American summer on record,¹⁰⁷ Reliability Coordinators (RCs) in all areas sustained adequate operating reserves during peak conditions, resulting in no uncontrolled firm demand interruptions during the 2011 summer season that impacted the reliability of the bulk electric system.

Despite a record-setting number of high temperature days and high average temperature across all of Texas, there was no loss of firm load due to resource unavailability or due to transmission element outages during the 2011 summer period in ERCOT. The day-ahead peak demand forecast of 109,851 MW in ERCOT was lower than the actual peak demand of 110,006 MW by 155 MW, reflecting a 0.14 percent difference. Across the MISO footprint, the month of July 2011 continued with persistent high temperatures, high relative humidity, and variable precipitation. The average load-weighted Heat Index, which is the combined effect of temperature and humidity, exceeded 100 degrees for seventy-seven hours during the peak month, leading to the declarations of several Hot Weather Alerts. Hourly Real-Time Load exceeded 100 GW for thirteen hours in July 2011.

There was increased penetration of wind in MISO and Saskatchewan. A third-party consultant service was used at Saskatchewan for next hour to next day wind forecasts. These forecasts are essential to ensure that conventional units are available to offset the variability of wind production. In the western parts of SERC-N, there was fuel shortage because the 2011 summer flooding impacted rail coal deliveries. The existing fuel supplies ensured reliable operation during these transportation interruptions in some utilities. Other utilities experienced no fuel delivery interruptions during the period. There were April 2011 tornadoes that affected large portions of the systems in the SERC-N, SERC-E, and SERC-SE reporting areas and caused delays to several transmission projects with summer in-service dates. There was loss of load due to heavy damage to the distribution system in ISO-NE when Hurricane Irene hit New England in August 2011. The bulk system was unaffected.

¹⁰⁷ <http://www.ncdc.noaa.gov/sotc/national/2011/8>

MISO: Challenges in Wind Integration

In 2011, one of the most important challenges to operating the bulk power system in summer peak load season is related to the integration of wind. Both wind capacity and wind output have grown consistently in many parts of the system, such as MISO, for the last three summers, as shown in Figure 88 and Table 30. This trend will continue due to state renewable portfolio standards and potential federal mandates. The intermittent nature of wind has made no guarantee that the generation be available during peak conditions. In MISO, wind output during the 2011 summer peak month ranged from 13 MW to 4,909 MW.

In order to better manage these operational challenges, on June 1st, 2011; MISO successfully launched the Dispatchable Intermittent Resources (DIRs) program, treating renewable resources like any other generation. Over 1,000 MW of wind capacity registered as DIRs, maximizing utilization and minimizing the need for manual real-time curtailments.

Figure 88: MISO Average Wind Generation and Registered Wind Capacity

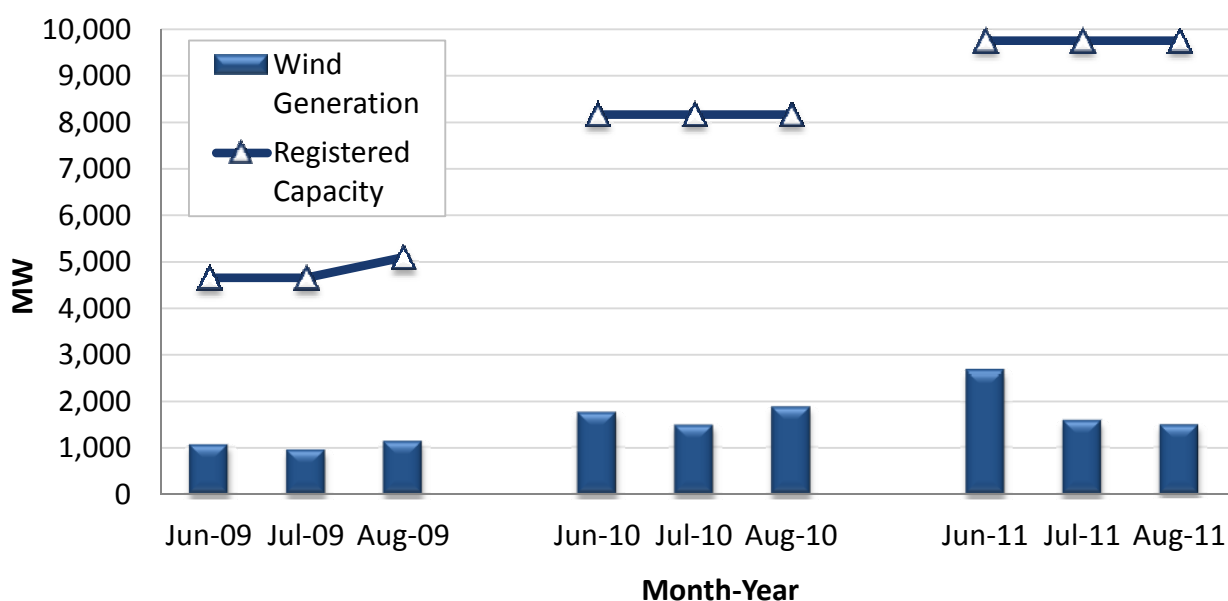
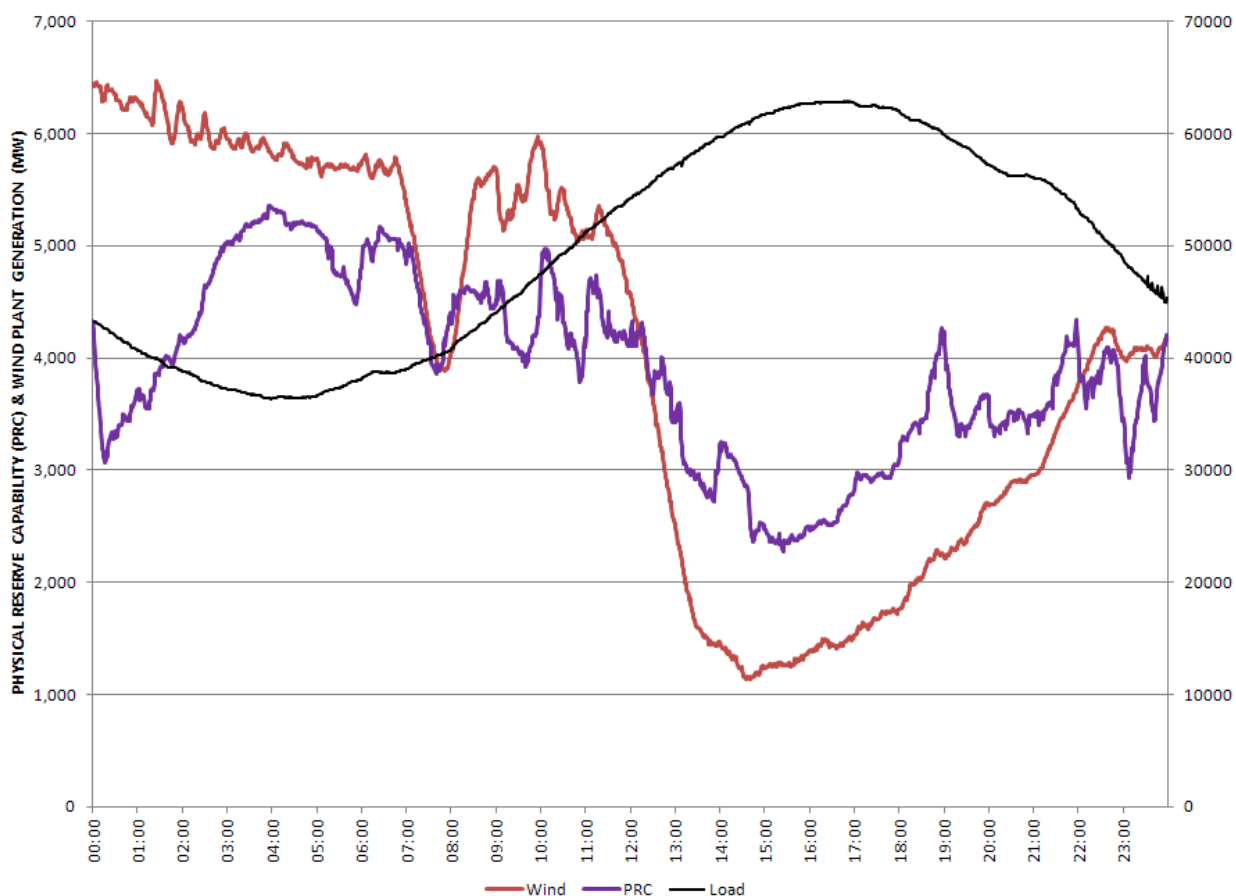


Table 30: MISO Wind Generation and Capacity in Summer Months		
Summer Months	Actual Monthly Average of Wind Generation MW	Registered Capacity MW
June 2009	1,051	4,658
July 2009	937	4,658
August 2009	1,125	5,096
June 2010	1,743	8,169
July 2010	1,466	8,169
August 2010	1,859	8,169
June 2011	2,665	9,578
July 2011	1,569	9,578
August 2011	1,478	9,578

ERCOT: Wind Generation Decline and Emergency Energy Alerts (EEAs)

On June 27, 2011, an EEA Level 1 was issued at 15:25 as a result of Physical Responsive Capability (PRC)¹⁰⁸ going below 2,300 MW, caused by three separate large unit trips totaling a loss of 1,765 MW of generation over a two hour period. This is shown in Figure 89. In addition to the three unit trips, wind generation began declining by approximately 4,200 MW over a four-hour period which led to further depletion of reserves. Load also increased during the hours 13:00-15:00 by approximately 4,020 MW. The EEA Level 1 was cancelled at 16:50.

¹⁰⁸ Definition of the ERCOT's Physical Responsive Capability can be found at: www.ercot.com/glossary/p.

Figure 89: ERCOT Peak Load Operations on June 27, 2011

Demand Response Contributed to Improved Reliability

PJM: Energy Demand Response and Emergency Energy Alerts (EEAs)

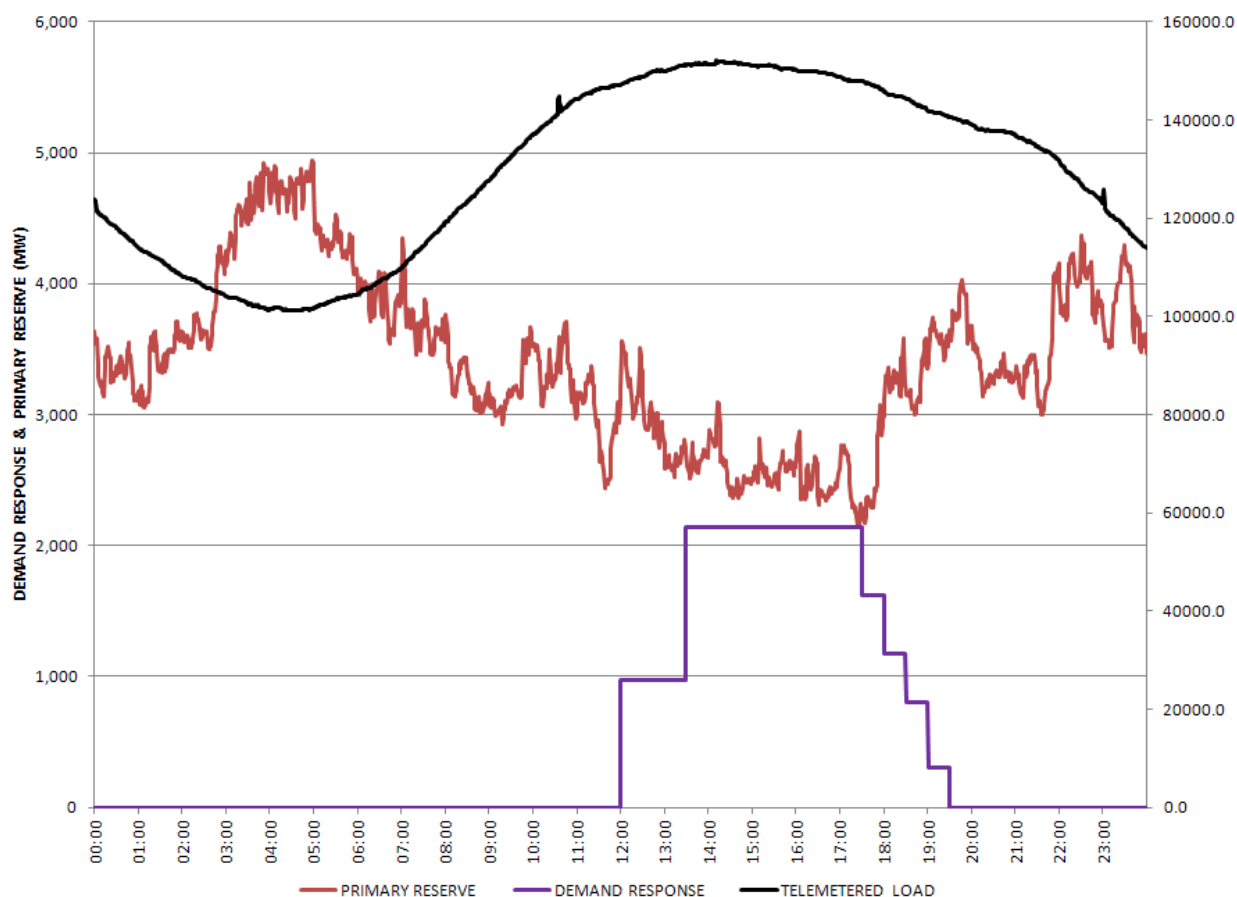
Effective 21:30 EDT on July 21, 2011, PJM issued a Maximum Generation Alert EEA Level 1 declaration for the PJM Mid-Atlantic region for Friday, July 22, 2011. High loads were mitigated by commitment of additional generation and use of Emergency Demand Response. The changes in load, wind, reserves are shown in Table 31. The call for Emergency Demand Response resulted in the declaration of Emergency Energy Alert 2 on July 22, 2011 at 12:00 EST. Emergency Demand Response of 2,412 MW was realized on July 22, 2011. Demand Response deployment is shown in Figure 90. The Demand Response Service Type¹⁰⁹ was Load as a Capacity Resource and Interruptible Load.

¹⁰⁹ http://www.nationaldrdirectory.com/programtypes_ndrd.html

Table 31: PJM Load Increase and Primary Reserves Decline				
Date	Time	Load MW	Wind MW	Reserves MW
July 22, 2011	05 00 hrs	101,706	709	4,752
July 22, 2011	15 00 hrs	151,015	268	2,588

Demand Response is an important component in the overall portfolio of resources required to reliably meet the increasing demand for electricity. The PJM example in Figure 90 of a day with high load, such as July 22, 2011, shows that during an energy emergency alert period, emergency Demand Response was employed. The main benefit of Emergency Demand Response in operations is to help ensure resource adequacy while providing operators with additional flexibility in maintaining operating reliability.

Figure 90: PJM Demand Response, Primary Reserves and Load on July 22, 2011

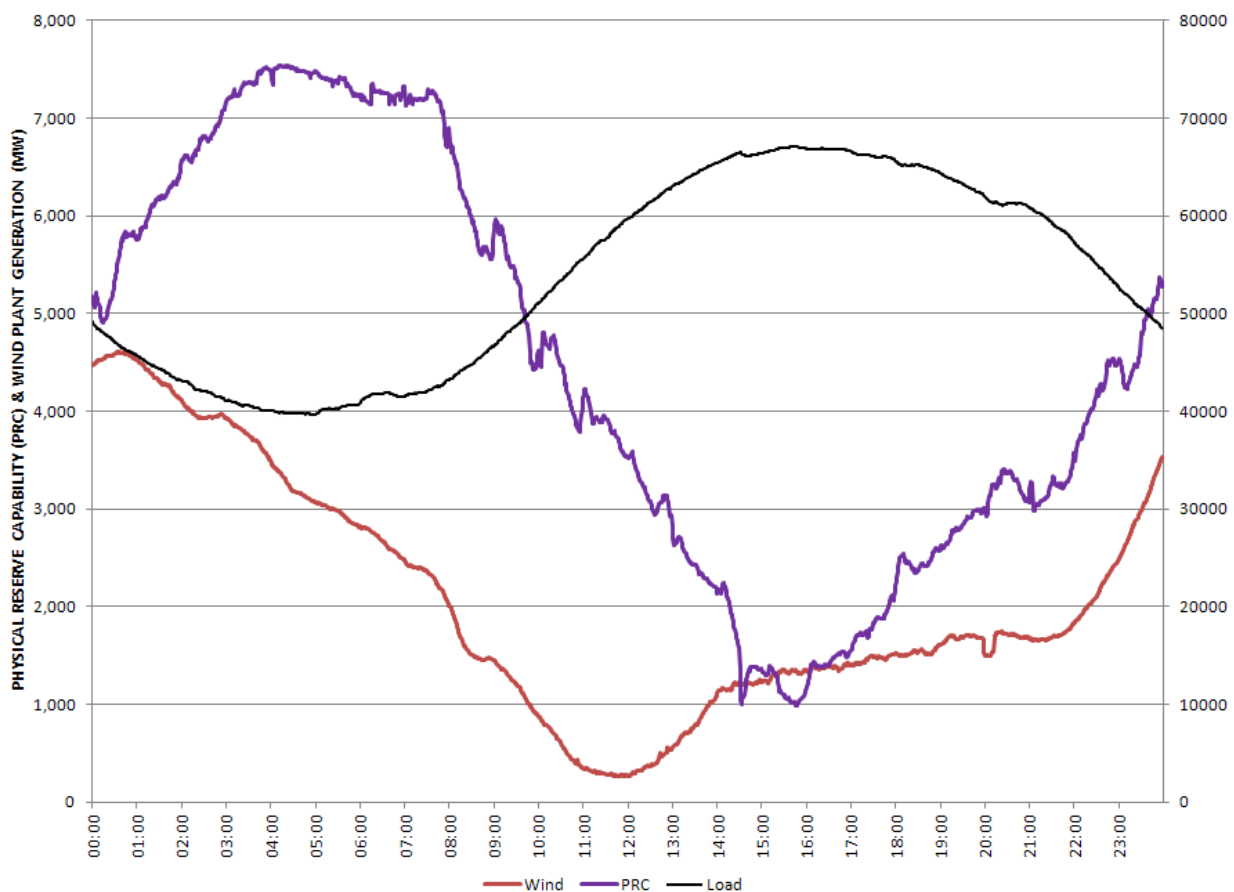


ERCOT: Energy Demand Response and Emergency Energy Alerts (EEAs)

On August 4, 2011, ERCOT issued an EEA Level 1 at 13:45 as Physical Responsive Capability dropped below 2,300 MW as a result of increasing load, decreasing wind generation and over 1,000 MW of forced outages. At 14:32, ERCOT declared EEA Level 2A, as Physical Responsive Capability dropped below 1,750 MW reaching a low of 983 MW. Load Resources (LR) providing Responsive Reserve Service (RRS) were deployed. This is shown in Figure 91. As the situation continued to decline, at 15:44 ERCOT declared EEA Level 2B; and, per operating procedures, ERCOT deployed Emergency Interruptible Loads (EILS) which are large industrial customers under contract to be interrupted under emergency situations. At 16:05, a second EILS deployment for Business Hours 3 from 4:00 PM to 8:00 PM.

At 17:53, as the situation began to improve, ERCOT moved to EEA Level 2A from EEA Level 2B, and then to EEA Level 1 at 18:09, recalling EILS at that time. The EEA Level 1 was cancelled at 18:52. No Firm load was interrupted during this EEA event.

Figure 91: ERCOT Peak Load Operations on Aug 04, 2011



ISO-NE: Maintaining Operating Reserve with Demand Response

On July 22, 2011, 643 MW of active demand response was dispatched as part of ISO-NE's implementation of OP 4.¹¹⁰ The performance of the active demand response was approximately 100 percent of the capacity supply obligation for those resources. This allowed ISO-NE to effectively maintain ten-minute reserves on the system with the reduction of 662 MW of system demand. The event on July 22 was effectively managed by the use of the use of the OP 4 procedure for the capacity deficiency. In particular, the use of the demand resources dispatched during the event allowed ISO-NE to maintain ten-minute operating reserves.

Effective preplanning and training of system operators resulted in a reliable outcome using ISO-NE's capacity and energy procedures to manage the higher than expected loads and generation losses that occurred on July 22. Overall, existing procedures and processes allowed ISO-NE to manage the operation of the New England system in a reliable manner during summer 2011.

The Demand Response Deployment started at 12 noon on July 22, 2011 and ended at 6 pm on July 22, 2011. All Demand Response service types were "Load as a Capacity Resource". 166 resources with a total capacity of 1871 MW participated in the demand response deployment and the realized demand reduction was 636 MW.¹¹¹

Transmission Constraints

SERC: Emergency Energy Alerts and Transmission Loading Relief

The EEA-3s requested in June were due to Level 5 Transmission Loading Relief conditions as a result of heavy imports into a localized area. The entity did not have adequate internal generation and served load entirely from external schedules. Therefore, capacity and Energy Emergency procedures were implemented. The Reliability Coordinator was able to allow enough power to flow into the area to avoid a firm load-shedding event.

SPP: Weather Related EEAs and TLRs

The most significant operational challenges for SPP came from two weather-related issues. The first challenge was the Missouri River flooding that occurred during the spring and early summer months caused several operational challenges including: responding to degraded transmission line footings within the elevated river's flow, the extension of a nuclear plant outage due to high river levels, and the termination of rail service that provided coal supplies to those resources along the river. The affected resources had a 60-day supply of coal during the beginning of this event, and operators were able to manage their supplies until rail service returned. There were no operational or capacity impacts due to fuel supply shortages during this period.

The second weather-related event occurred during the severe hot temperatures that occurred across the Region in late July and early August. Due to high air-conditioner load caused by the heat, an Oklahoma entity issued various EEA levels (1 through 3) during the summer. Additional operational challenges included parallel path impacts on SPP flow gates in the northeast corner

¹¹⁰ http://www.iso-ne.com/rules_proceeds/operating/isone/op4/index.html

¹¹¹ Realized demand response data is reported as an hourly value to DADS. ISO-NE uses a five minute interval calculation and its reported realized demand reduction is 644 MW.

of Kansas and the southeast corner of Nebraska due to from high transfers caused by wind generation located in the MISO Region. This resulted in large amounts of curtailment of both MISO and SPP market flows to resolve the issue. The SPP RC continued to manage this operational challenge via communication with MISO. The SPP RC experienced seven situations in which a TLR level 5 was required during this period.

Protection and Control Misoperations

WECC: Protection System Misoperations; Generation and Load Loss Events

WECC experienced three significant outage events during the summer of 2011. On June 6, the El Paso Texas area experienced a service interruption to about 162,000 customers and the loss of 106 MW of generation. Local transmission system protective relaying issues were involved in the event. On June 30, a transformer fire in Mesa, Arizona led to the loss of service to about 160,000 customers and the loss of one megawatt of generation. On July 13, transmission system protective relaying issues resulted in a loss of 599 MW and the interruption of service to approximately 93,000 customers in the Pueblo area of Colorado.

ERCOT

The ERCOT Region maintained reliable operations during the 2011 summer period. August had record-breaking demand levels as drought conditions and high temperatures continued. The summer season peak of 68,416 MW occurred on August 3, 2011 and was 2,640 MW above the 2010 summer season peak. Available capacity was 69,314 MW at the time of the summer peak

The actual peak demand for the 2011 summer period was 68,416 MW occurring on August 3, 2011. This peak was 5.31 percent higher than the seasonal summer peak forecast of 64,964 MW predicted for the 2011 summer period. The actual peak was 0.17 percent higher than the day-ahead peak demand forecast for August 3, 2011.

Despite a record-setting number of high temperature days and high average temperature across all of Texas, there was no loss of firm load due to Resource unavailability or due to transmission element outages during the 2011 summer period. In addition, there were no fuel situations impacting the availability of resources.

Emergency Operations were initiated seven times during the summer period. Energy Emergency Alerts (EEAs) were declared on June 27, August 2, 3, 4, 5, 23, and 24. The August 23, 2010 summer peak demand record of 65,776 MW was unofficially exceeded on August 1, 2011 by 1,091 MW; August 2 by 2,153 MW and for the third time on August 3 by 2,518 MW.

The required Contingency Reserve for the ERCOT Region as defined by NERC standard BAL-002 must be at least 1,375 MW, which ERCOT satisfied mostly throughout the 2011 summer period. On August 4 and August 24, Physical Responsive Capability reached lows of 983 MW and 1,191 MW, respectively as reserves were being deployed.

ERCOT strives to meet a requirement of at least 2,300 MW of Responsive Reserve for all hours under normal conditions and EEA procedures are built around this requirement. The projected Operating Reserve for the ERCOT Region for the peak period was 2,301 MW and the actual ERCOT Region Operating Reserve for the peak period was 1955 MW. The Operating Reserve Margin shown below does not include Load Resources.

The greatest challenges experienced during this period were forced outages and derates. ERCOT ISO's EEA procedures allowed it to adequately address the issues encountered during the extreme conditions experienced. To address high temperatures, ERCOT added an Extreme Heat Procedure used to issue notifications when forecasted temperatures certain thresholds in designated weather zones within the ERCOT footprint.

MISO

Despite the extreme weather conditions this summer, MISO was able to maintain reliability. This summer, MISO experienced an all-time reliability footprint peak demand of 110,006 MW on July 20th, HE 17. This surpassed the previous all-time peak demand of 109,532 MW on July 31st, 2006 in HE 15. The previous all-time unadjusted peak demand was 129,647 MW. The day-ahead peak demand forecast of 109,851 MW was lower than the actual peak demand of 110,006 MW by 155 MW, reflecting a 0.14 percent difference. The summer of 2011 has been one of the warmest in recent years. Across the MISO footprint, the month of July 2011 continued with persistent high temperatures, high relative humidity, and variable precipitation. The average load-weighted Heat Index, which is the combined effect of temperature and humidity, exceeded 100 degrees for seventy-seven hours during the peak month, leading to the declarations of several Hot Weather Alerts. Hourly Real-Time Load exceeded 100 GW for thirteen hours in July 2011.

There was no loss of firm load due to the non-performance of bulk power system resources. There was also no loss of firm load due to bulk transmission outages, and there were no fuel situations impacting the use of resources. MISO declared Conservative Operations, Hot Weather Alerts, and Maximum Generation Emergency actions for the footprint in July. On the peak load day of July 20th, 2011, MISO effectively managed load without the need to implement maximum generation procedures. However, on July 21st, 2011, with a substantial reduction in wind generation and a revised load forecast resulting in a projected energy surplus of only 427 MW, a Maximum Generation Emergency Alert was declared at 06:34 EST. At 11:13 EST, an energy shortfall of 106 MW was projected and MISO declared a Maximum Generation Emergency Event Step 1a. However no Energy Emergency Alerts were deployed to maintain reliability of the MISO footprint.

MISO experienced Maximum Generation Emergency Event Step 1a on July 21st, 2011. MISO notified load balancing authorities and/or market participants to commit additional Generation Resources; however, rain, cloud cover, and local voluntary Load Management activities caused load to flatten prior to 13:00 EST and therefore MISO downgraded the Maximum Generation Emergency Event Step 1a to a Maximum Generation Emergency Warning at 14:54 EST. The Maximum Generation Emergency Warning was terminated at 17:10 EST.

ISO-NE

Hurricane Irene hit New England on August 28, 2011, causing loss of load over time primarily related to heavy damage to the distribution system. At the height of the storm, over 2 million customers were without power. The storm caused the loss of over forty 115 kV transmission lines and two 230 kV transmission lines. Operations of the bulk electric system remained within limits before, during, and after the storm and no capacity deficiencies occurred before, during, or after the storm. The primary cause of the loss of load was the damage to distribution circuits caused by tree damage due to winds. The primary causes of the 115 kV and above outages

were primarily flooding and vegetation contacts from trees falling over from outside the utility Rights of Way. No load was lost due to firm load shedding by the system operators. The restoration of load did not present any operational issues to ISO-NE in maintaining the reliability of the bulk system.

NYISO

During summer of 2011, the NYISO did not experience any loss in firm load due to the non-performance of a bulk power system resource or due to bulk transmission outages. In addition, no resources were impacted by fuel restrictions, no Emergency Procedures were implemented and no Energy Emergency Alerts (EEA's) were declared. No other special operating measures were required. All operational procedures were in place prior to the assessment period, and did not result in needing to adjust or revise the plan to mitigate a reliability related situation. There were no specific challenges in operating the bulk power system besides the typical operating challenges. The NYISO used existing operating procedures to deal with system conditions. Because operation was unexceptional, no lessons learned were determined. The operating experiences this season will be reviewed and discussed for planning next summer's assessment.

SASKPOWER

The Saskatchewan Power Corporation RC experienced no operational difficulties with meeting the 2011 summer peak demand. Saskatchewan's summer actual peak demand was 3,079 MW. The peak demand occurred on July 18, 2011 at hour ending 15:00 during an extended period of unseasonably high temperatures. Internal Saskatchewan generation was adequate to meet summer peak demand. No Demand Response was deployed. The seasonal peak demand forecasted was 3,034 MW. The actual peak demand was 1.48 percent more than the seasonal peak demand forecasted. The day-ahead peak demand forecast was 2,820 MW for the hour ending 17:00, the peak demand of 3,079 MW occurred at hour ending 15:00. The forecasted peak demand was 9.18 percent under the actual peak.

With the increased penetration of wind in Saskatchewan and its variability in production, it is important for system operators to ensure conventional units are available to offset this variability and its potential impacts. Forecasting the amount of wind production to be utilized during the day is a demanding task. Operators must continually look ahead at what the wind production is forecasted to be at every hour to ensure the system is operated economically and securely. To accomplish these goals a third party consultant service is used for next-hour to next-day wind forecasts. Along with internal unit commitment tools, this allows the system operators to manage wind resources and its expected production.

SERC

The following narrative is a response for the entities within SERC who are in the SERC-N, SERC-E, SERC-W, and SERC-SE reporting areas. These reporting areas exclude entities that are within MISO and PJM. One entity reported 235 automatic interruptions to bulk transmission lines. Ninety-seven of these interruptions were sustained outages due to equipment failures caused by lightning. Most of those outages resulted in no loss of load. During the 2011 summer, flooding on the Tennessee and Missouri Rivers impacted rail coal deliveries within western portions of SERC-N. As a result, some entities simply relied on existing fuel supplies to ensure reliable operation during these transportation interruptions. Other utilities within the Region experienced no fuel delivery interruptions that compromised reliability during the period.

SPP

The SPP Reliability Coordinator (RC) EEA activity remained within the normal range aside from the public appeals issued by three SPP members due to their EEA activity during the extreme summer heat event. Even though public appeals were issued, no voltage reductions were required, and no interruptions of firm transactions or load were experienced.

In the south region of the SPP reliability footprint there were four EEA's declared by entities that had firm schedule curtailments due to TLR activity. There were no load shed or public appeals associated with these declarations as the RC excluded the firm schedules from curtailment.

WECC

By far the most significant event occurred on September 8 when a portion of the Western Interconnection power grid experienced a loss of service to over approximately 2.8 million customers in southern California, parts of Arizona, and northern Baja, Mexico. WECC entities are participating in the Event Analysis activities associated with the service interruption and are assisting NERC and governmental authorities with their inquiries. The Arizona-Southern California outage and other notable events are discussed in the operation issues section of this post-season assessment.

Regions within the Western Interconnection experienced brief periods of high summer temperatures but the hot-spells were not particularly intense and were not widespread geographically. The normally summer-peaking WECC actual non-coincident peak demand of 147,068 MW was 7.6 percent less than the all-time summer non-coincident peak demand of 159,182 MW, which occurred on July 24, 2006 and was 11.7 percent greater than the all-time winter non-coincident peak demand of 131,708 MW, which occurred in December 2008.

Abbreviations Used in This Report

Acronym	Definition
ALP	Acadiana Load Pocket
ALR	Adequate Level of Reliability
APC	Availability Percentage
BA	Balancing Authority
BES	Bulk Electric System
BPS	Bulk Power System
CDI	Condition Driven Index
CIPC	Critical Infrastructure Protection Committee
CLECO	Cleco Power LLC
DADS	Demand Response Availability Data System
DADSWG	Demand Response Availability Data System Working Group
DCLM	Direct Load Control Management
DCS	Disturbance Control Standard
DIR	Dispatchable Intermittent Resources
DOE	Department Of Energy
DSM	Demand Side Management
EA	Event Analysis
EAF	Equivalent Availability Factor
EAR	Event Analysis Report
EAS	Event Analysis Subcommittee
EAWG	Event Analysis Working Group
EDI	Event Driven Index
EEA	Energy Emergency Alert
EFORD	Equivalent Forced Outage Rate, Demand

Acronym	Definition
EI	Eastern Interconnection
EIA	United States Energy Information Administration
EMS	Energy Management System
ERCOT	Electric Reliability Council of Texas
ERO	Electric Reliability Organization
ERO-RAPA	ERO-Reliability Assessment and Performance Analysis
FERC	Federal Energy Regulatory Commission
FOH	Forced Outage Hours
FRCC	Florida Reliability Coordinating Council
FWG	Frequency Working Group
GADS	Generation Availability Data System
GADSWG	Generation Availability Data System Working Group
GOP	Generation Operator
IESO	Independent Electricity System Operator
IL	Interruptible Load
IROL	Interconnection Reliability Operating Limit
ISO	Independent System Operator
ISO-NE	ISO New England
LR	Load Resource
MRO	Midwest Reliability Organization
MSSC	Most Severe Single Contingency
NCF	Net Capacity Factor
NDC	Net Dependable Capacity
NERC	North American Electric Reliability Corporation
NPCC	Northeast Power Coordinating Council
NYISO	New York Independent Service Operator

Acronym	Definition
OC	Operating Committee
OP	Operating Procedures
ORS	Operating Reliability Subcommittee
PAS	Performance Analysis Subcommittee
PC	Planning Committee
PO	Planned Outage
PSMTF	Protection System Misoperation Task Force
QI	Québec Interconnection
RAPA	Reliability Assessment Performance Analysis
RAS	Remedial Action Schemes
RC	Reliability Coordinator
RCIS	Reliability Coordination Information System
RCWG	Reliability Coordinator Working Group
RE	Regional Entities
RFC	ReliabilityFirst Corporation
RMWG	Reliability Metrics Working Group
RRM	Reliability Risk Management
RRS	Responsive Reserve Service
RSG	Reserve Sharing Group
SCADA	Supervisory Control and Data Acquisition
SDI	Standard/statute Driven Index
SERC	SERC Reliability Corporation
SNL	Sandia National Laboratories
SOL	System Operating Limit
SPS	Special Protection Schemes
SPCS	System Protection and Control Subcommittee

Acronym	Definition
SPP	Southwest Power Pool
SRI	Severity Risk Index
TADS	Transmission Availability Data System
TADSWG	Transmission Availability Data System Working Group
TO	Transmission Owner
TPL	Transmission Planning
TRE	Texas Reliability Entity
UFLS	Under Frequency Load Shedding
WECC	Western Electricity Coordinating Council
WI	Western Interconnection

Contributions

Acknowledgements

NERC would like to express its appreciation to the many people who provided technical support and identified statistical areas for improvement. Special gratitude goes to the staff at the U.S. Energy Information Administration (EIA) who shared their knowledge and offered assistance in TADS's year-to-year trend analysis. In particular, Stan Kaplan, Glenn McGrath, Orhan Yildiz, Chachi Fan, and Jonathan DeVilbiss offered invaluable technical insights and built significance test models.

NERC is also indebted to Dr. David Robinson of the Sandia National Laboratories (SNL) for his evaluation of reliability indices and recommendations to establish a cause-effect model. Thanks to Joe Eto of the Lawrence Berkeley National Laboratory for his support and helpful suggestions in forming the recommendations.

NERC Industry Groups

Table 32 lists the NERC industry group contributors.

Table 32: NERC Group Acknowledgements	
Group	Officers
Planning Committee Reviewers	Jay Farrington, PowerSouth Energy Cooperative Brian Keel, Salt River Project Pedro Modia, Florida Power & Light Co. Branden Sudduth, WECC
Performance Analysis Subcommittee	Chair: Bill Adams, Georgia Power Vice Chair: Melinda Montgomery, Entergy
Demand Response Availability Data System Working Group	Chair: Sharon Bauer, Progress Energy
Events Analysis Working Group	Chair: Jacquie Smith, RFC Vice Chair: Steven Ashbaker, WECC
Generation Availability Data System Working Group	Chair: Gary Brinkworth, TVA Vice Chair: Leeth DePriest, Southern Company
Transmission Availability Data System Working Group	Chair: Jake Langthorn, Oklahoma Gas and Electric Co. Vice Chair: Jeff Schaller, Hydro One Networks, Inc.
Resources Subcommittee	Chair: Don Badley, Northwest Power Pool Corp. Vice Chair: Gerald Beckerle, Ameren Services
Operating Reliability Subcommittee	Chair: Colleen Frosch, ERCOT Vice Chair: Joel Wise, TVA
Frequency Working Group	Chair: Sydney Niemeyer, NRG Energy

Regional Entity Staff

Table 33 provides a list of the Regional Entity staff that provided data and content review.

Table 33: Contributing Regional Entity Staff	
Name	Regional Entity
Vince Ordax	FRCC
John Seidel	MRO
Phil Fedora	NPCC
Jeffery Mitchell	RFC
Joe Spencer	SERC
Alan Wahlstrom and Deborah Currie	SPP
Curtis Crews	TRE
Layne Brown	WECC

NERC Staff

Table 34 provides a list of the NERC staff who contributed to this report.

Table 34: NERC Staff		
Name	Title	E-mail Address
Mark Lauby	Vice President and Director of Reliability Assessment and Performance Analysis	mark.lauby@nerc.net
Jessica Bian	Director of Performance Analysis	jessica.bian@nerc.net
John Moura	Manager of Reliability Assessments	john.moura@nerc.net
Andrew Slone	Engineer, Reliability Performance Analysis	andrew.slone@nerc.net
Jim Robinson	TADS Project Manager	jim.robinson@nerc.net
Matthew Varghese	Senior Performance Analysis Engineer	matthew.varghese@nerc.net
Clyde Melton	Engineer, Reliability Performance Analysis	clyde.melton@nerc.net
Mike Curley	Manager of GADS Services	mike.curley@nerc.net
James Powell	Engineer, Reliability Performance Analysis	james.powell@nerc.net
Elliott Nethercutt	Technical Analyst	elliott.nethercutt@nerc.com
Earl Shockley	Director of Reliability Risk Management	earl.shockley@nerc.net
Jule Tate	Manager of Event Analysis	jule.tate@nerc.net
James Merlo	Manager of Human Performance	james.merlo@nerc.net
Ben McMillan	Risk Analysis Engineer	ben.mcmillan@nerc.net
Ed Ruck	Senior Data and Alert Specialist	ed.ruck@nerc.net
Michelle Marx	Administrative Assistant	michelle.marx@nerc.net

From: [Kimberly Mielcarek](#)
To: [Kimberly Mielcarek](#)
Subject: NERC Announcement - State of Reliability Report Offers Historical Reference on Bulk Power System Trends
Date: Tuesday, May 15, 2012 10:38:21 AM

Announcement

State of Reliability Report Offers Historical Reference on Bulk Power System Trends

Click link for [announcement](#), [2012 State of Reliability](#) report

ATLANTA – The North American Electric Reliability Corporation (NERC) released the *2012 State of Reliability* report that reviews and assesses the state of reliability based on trends identified through data combined with root cause analysis of events. This report is follow-on to the 2011 foundational report and represents NERC's integrated view of ongoing bulk power system reliability trends.

This report assesses 18 metrics that address the characteristics of an adequate level of reliability, industry-wide automatic transmission and generating outage rates from 2008 to 2011. Analysis from the frequency response, 2011 demand response availability, event analysis trends, and post summer operations also are highlighted.

For more information or assistance, please contact [Kimberly Mielcarek](#).

**3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com**

You are currently subscribed to nerc-info as: lpedowicz@npcc.org
To unsubscribe send a blank email to leave-1292007-325654.1ca6f85fb1574a8515cc07df72d3bfe0@listserv.nerc.com

Announcement

State of Reliability Report Offers Historical Reference on Bulk Power System Trends

May 15, 2012

ATLANTA – The North American Electric Reliability Corporation (NERC) released the *2012 State of Reliability* report that reviews and assesses the state of reliability based on trends identified through data combined with root cause analysis of events. This report is follow-on to the 2011 foundational report and represents NERC's integrated view of ongoing bulk power system reliability trends.

"This report is a realization of ongoing efforts to synthesize data from multiple databases and combine them with analyses of events seen each year to allow NERC to produce an annual, independent assessment on reliability performance," said Gerry Cauley, president and chief executive officer of NERC. "The report is a major step forward in characterizing and identifying risks in order to develop coordinated, multifunctional solutions."

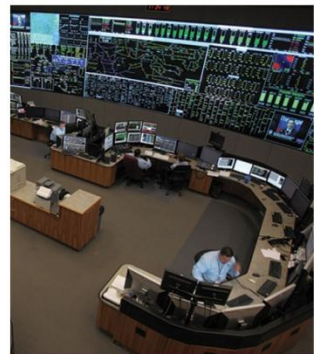
Key findings identified in the report include:

- Reliability of the bulk power system remains adequate, with little change in trends between 2008 to 2011.
- Frequency response is stable with no deterioration.
- Protection system misoperations are a significant reliability issue.
- Equipment failure warrants further analysis.
- Resource mix changes necessitate new metrics.
- More data and research is needed.

"This information provides a historical reference for the industry on bulk power system reliability," said Jessica Bian, director of Performance Analysis at NERC. "The report's findings and recommendations serve as technical input to NERC's efforts to control reliability risks, standards development and compliance process improvement."

CONTACT:
Kimberly.Mielcarek@nerc.net

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com



This report assesses 18 metrics that address the characteristics of an adequate level of reliability, industry-wide automatic transmission and generating outage rates from 2008 to 2011. Analysis from the frequency response, 2011 demand response availability, event analysis trends, and post summer operations also are highlighted.

Click [here](#) to download the 2012 *State of Reliability* report.

###

The North American Electric Reliability Corporation's mission is to ensure the reliability of the North American bulk power system. NERC is the electric reliability organization (ERO) certified by the Federal Energy Regulatory Commission in the United States to establish and enforce reliability standards for the bulk-power system. NERC has equivalent relationships with provincial and federal authorities in Canada. NERC develops and enforces reliability standards; assesses adequacy annually via a 10-year forecast, and summer and winter forecasts; monitors the bulk power system; and educates, trains and certifies industry personnel. Learn more at www.nerc.com

Agenda

Board of Trustees Conference Call

May 24, 2012 | 2:00-3:30 p.m. Eastern

Dial-In: 888-391-0101

No Code Needed

Introductions and Chair's Remarks

NERC Antitrust Compliance Guidelines

Agenda

1. **NERC Summer Reliability Assessment —Approve**
2. **ReliabilityFirst Corporation Regional Standards Development Procedure and Amended and Restated Bylaws* —Approve**
3. **Project 2009-26 — Interpretation of CIP-004-1 for WECC* —Adopt**
4. **Member Representatives Committee Members to the Board of Trustees Nominating Committee* —Accept**

*Background materials included.

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

ReliabilityFirst Corporation Regional Standards Development Procedure and Amended and Restated Bylaws

Action

Approve the following standards documents and direct staff to file with applicable regulatory authorities:

- Version 4 of ReliabilityFirst Corporation Regional Standards Development Procedure
- Amended and Restated Bylaws of ReliabilityFirst Corporation

Background

The NERC Board of Trustees approved Version 3 of the ReliabilityFirst Corporation Reliability Standards Development Procedure at the May 10, 2011 meeting. The principal issue raised in the comments on Version 3 was the addition of the language regarding the effective date of Regional Reliability Standards. This language made Regional Reliability Standards “mandatory and enforceable” for ReliabilityFirst Corporation (RFC) members upon approval by the RFC Board of Directors. Commenters objected to inclusion of this language, stating that standards cannot be made mandatory and enforceable under section 215 of the Federal Power Act until they have been approved by NERC and the Federal Energy Regulatory Commission. The NERC Board of Trustees action for approval included an understanding that the RFC President would discuss possible changes to the Amended and Restated Bylaws of ReliabilityFirst Corporation (Bylaws) to address industry concern regarding enforcement of Regional Reliability Standards prior to FERC approval.

Discussion

Subsequent to the May 10, 2011 NERC Board of Trustees action, RFC’s membership approved a revised definition of “Regional Reliability Standard” contained within the amended Bylaws and Certificate of Incorporation. The RFC Standards Committee then made a conforming change to the Version 4 of ReliabilityFirst Reliability Standards Development Procedure. This change was made to ensure that the ReliabilityFirst Reliability Standards Development Procedure defines the term “Regional Reliability Standard” in a manner consistent with the member-approved definition. During the December 1, 2011 RFC Board of Directors meeting, the RFC Board concurred with the change in Version 4 of the ReliabilityFirst Corporation Reliability Standards Development Procedure.

The proposed amended definition of “Regional Reliability Standard” specifically states that a Regional Reliability Standard is not binding upon any member or Registered Entity, nor is it effective or enforceable, until the Regional Reliability Standard has been adopted by NERC and approved by the Commission.

RFC made additional minor modifications to enhance the clarity and efficiency of the Bylaws pertaining to RFC member action and changes related to succession of RFC directors concurrently with the change described above. Specifically, these changes include:

1. Modifying RFC's ballot procedures that eliminate the ability of members to take action by written ballot without a meeting. Member action must now take place at an annual or special meeting that meets the quorum requirement (Section 6.8).
2. Moving, but not altering, language from Section 7.4(e) (Industry Sector responsibility) to 7.4(g) (Nominating and Governance Committee responsibility) directing the Nominating and Governance Committee to consider factors such as geographic and functional representation of the Board when nominating at-large directors.
3. Allowing resigning directors to designate an effective-date of their resignations, which provides greater flexibility to the members and board to fill the resulting vacancies. (Sections 7.7(a) and 7.7(b)).

Directives

None.

A link to the project history and files is included here for reference:

<https://rsvp.rfirst.org/SDP501RFC03/default.aspx>

If trustees have questions or need additional information, they may contact Herb Schrayshuen, Vice President of Standards and Training at herb.schrayshuen@nerc.net.



**SUPPLEMENTAL MEMORANDUM
AMENDMENTS TO RELIABILITYFIRST CORPORATION
RELIABILITY STANDARDS DEVELOPMENT PROCEDURE**

The following lists the proposed revisions to the ReliabilityFirst Corporation Reliability Standards Development Procedure for consideration.

The changes to the Reliability Standards Development Procedure effectuate the amended definition of a “Regional Reliability Standard,” contained within the amended Bylaws and Certificate of Incorporation that the Members recently approved. Specifically, since a “Regional Reliability Standard” is now effective and enforceable upon Commission approval, the changes to the Reliability Standards Development Procedure propose to incorporate the amended effective and enforceable date language.

Proposed Changes to Relating to Regional Reliability Standards:

Section Amended:	Proposed Amendment:
Introduction, Third Paragraph	ReliabilityFirst standards shall be subject to approval by NERC, as the electric reliability organization, and by the Federal Energy Regulatory Commission (FERC) before becoming mandatory and enforceable under Section 215 of the FPA. <u>No Standard shall be effective within the ReliabilityFirst area unless filed by NERC with FERC and approved by FERC. The approval date of each ReliabilityFirst standard is upon ReliabilityFirst Board approval.</u> The effective date will depend on the implementation plan that is provided with each new or revised standard. <u>The ReliabilityFirst standard is mandatory and enforceable (without monetary penalties for non-compliance) upon the effective date after ReliabilityFirst Board approval for applicable entities that are members of ReliabilityFirst.</u> ³ The ReliabilityFirst standard is mandatory and enforceable <u>(with monetary penalties for non-compliance)</u> to all applicable <u>Registered Entities</u> within the ReliabilityFirst footprint upon approval by <u>the</u> FERC. <u>No Standard shall be effective within the ReliabilityFirst area unless filed by NERC with FERC and approved by FERC. The effective date for non-members upon the FERC approval will be determined by the implementation plan that is provided with each new or revised standard.</u>
Definition of a Reliability Standard, First Paragraph	As contained in the ReliabilityFirst By-laws, ReliabilityFirst “Regional Reliability Standard” shall mean a type of Reliability Standard that is applicable only within a particular Regional Entity or group of Regional Entities. A Regional

	Reliability Standard may augment, add detail to, or implement another Reliability Standard or cover matters not addressed by other Reliability Standards. <u>A Regional Reliability Standard is not binding upon any Member or Registered Entity, nor is it effective or enforceable, until the Regional Reliability Standard has been s, upon-adopted</u> by NERC and approved by the Commission <u>as a Reliability Standard enforced</u> within the applicable Regional Entity or Regional Entities pursuant to delegated authorities.
Regional Reliability Standard Format Requirement Template Example, Effective Date and Status Section	The effective date of the Standard <u>is the date of the FERC approval and the applicable implementation timeline. or, prior to approval of the Standard, the proposed effective date.</u>
Regional Reliability Standard Development Process, Step 8 - Implementation of a Regional Reliability Standard	<u>Upon approval of a draft Standard action by the FERC, t</u>The SPM will notify the membership <u>and applicable entities within the ReliabilityFirst footprint upon ReliabilityFirst Board approval of the standard of the effective date</u> through the normal and customary membership communication procedures and processes then in effect. The SPM will also notify the ReliabilityFirst Compliance Staff for integration into the ReliabilityFirst Compliance Program. <u>The approval date of each ReliabilityFirst standard is upon Board approval. The effective date will depend on the implementation plan that is provided with each new or revised standard. The ReliabilityFirst standard is mandatory and enforceable (without monetary penalties for non-compliance) upon the effective date after ReliabilityFirst Board approval for applicable entities that are members of ReliabilityFirst.</u>³ <u>ReliabilityFirst standards shall be subject to approval by NERC, as the electric reliability organization, and by the Federal Energy Regulatory Commission (FERC) before becoming mandatory and enforceable under Section 215 of the FPA. Upon approval of a ReliabilityFirst standard action by FERC, it is mandatory and enforceable (with monetary</u>

³ By applying for and becoming a Regular or Associate Member of the Corporation, each Member agrees to comply with all Reliability Standards, all NERC standards and requirements, and the other obligations of Members of the Corporation set forth in the ReliabilityFirst Bylaws or duly adopted by the Board in order to achieve the purposes of the Corporation.



	~~penalties for non-compliance) to all applicable entities within the ReliabilityFirst footprint. The effective date for non-members upon the FERC approval will be determined by the implementation plan that is provided with each new or revised standard.~~
Appendix C, Flowchart for Standards Process, Step 8	Filed <u>with and approved by</u> ~~for~~ NERC/FERC. <u>approval Once approved, and</u> ~~implement~~ standard throughout RFC

Reliability*First* Corporation
Reliability Standards Development
Procedure
Version 4

Reliability*First* Corporation Reliability Standards Development Procedure

Table of Contents

Introduction	1
Background.....	2
Regional Reliability Standard Definition, Characteristics, and Elements	3
Roles in the Regional Reliability Standards Development Process.....	7
Regional Reliability Standards Development Process	8
Appendix A: Maintenance of Regional Reliability Standards Development Process.....	17
Appendix B: Standard Authorization Request.....	21
Appendix C: Flowchart for Standards Process	28
Appendix D: Ballot Pool Categories and Registration.....	30

ReliabilityFirst Corporation Reliability Standards Development Procedure

Introduction

This procedure establishes the process for adoption of a Regional Reliability Standard (hereinafter referred to as “Standard”) of the ReliabilityFirst Corporation (ReliabilityFirst) and the development of consensus for adoption, approval, revision, reaffirmation, and deletion of such Standards. ReliabilityFirst Standards provide for the reliable regional and sub-regional planning and operation of the Bulk Power System¹ (BPS), consistent with Good Utility Practice¹ within the ReliabilityFirst geographical footprint.

This procedure was developed under the direction of the ReliabilityFirst Board of Directors (Board), who may request changes to this ReliabilityFirst Reliability Standards Development Procedure (hereinafter referred to as “this Procedure”) as deemed appropriate. A procedure for revising this Procedure is contained in Appendix A. This Procedure is consistent with the North American Electric Reliability Corporation (NERC) Reliability Standards Development Procedure.

ReliabilityFirst standards shall be subject to approval by NERC, as the electric reliability organization, and by the Federal Energy Regulatory Commission (FERC) before becoming mandatory and enforceable under Section 215 of the FPA. No Standard shall be effective within the ReliabilityFirst area unless filed by NERC with FERC and approved by FERC. The effective date will depend on the implementation plan that is provided with each new or revised standard. The ReliabilityFirst standard is mandatory and enforceable to all applicable entities within the ReliabilityFirst footprint upon approval by the FERC.

ReliabilityFirst Standards shall provide for as much uniformity as possible with NERC reliability standards across the interconnected BPS. A ReliabilityFirst Standard shall be more stringent than a NERC reliability standard, including a regional difference that addresses matters that the NERC reliability standard does not, or shall be a regional difference necessitated by a physical difference in the BPS. A ReliabilityFirst Standard that satisfies the statutory and regulatory criteria for approval of proposed NERC reliability standards, and that is more stringent than a NERC reliability standard, would generally be acceptable.

ReliabilityFirst Standards, when approved by FERC, shall be made part of the body of NERC reliability standards and shall be enforced upon all applicable BPS owners, operators, and users within the ReliabilityFirst area, regardless of membership in the region.

¹ As defined in the ReliabilityFirst By-laws

Background

Regions may develop, through their own processes, separate “Regional Standards” (ReliabilityFirst Standards) that go beyond, add detail to or aid implementation of NERC reliability standards, or otherwise address issues that are not addressed in NERC reliability standards.

As a condition of ReliabilityFirst membership, all ReliabilityFirst Members² agree to adhere to the NERC reliability standards. As such, the ReliabilityFirst and its Members will adhere to the NERC reliability standards in addition to the ReliabilityFirst Standards. NERC reliability standards and the ReliabilityFirst Standards are both to be included within the ReliabilityFirst Compliance Program.

ReliabilityFirst Standards are intended to apply only to that part of the Eastern Interconnection within the ReliabilityFirst geographical footprint. The development of these ReliabilityFirst Standards is developed according to the following principles via the process contained within this Procedure:

- Developed in a fair and open process that provided an opportunity for all interested parties to participate;
- Does not have an adverse impact on commerce that is not necessary for reliability;
- Provides a level of BPS reliability that is adequate to protect public health, safety, welfare, and national security and would not have a significant adverse impact on reliability; and
- Based on a justifiable difference between Regions or between sub-Regions within the Regional geographic area.

² As defined in the ReliabilityFirst By-laws

Regional Reliability Standard Definition, Characteristics, and Elements

Definition of a Reliability Standard

As contained in the ReliabilityFirst By-laws, ReliabilityFirst “Regional Reliability Standard” shall mean a type of Reliability Standard that is applicable only within a particular Regional Entity or group of Regional Entities. A Regional Reliability Standard may augment, add detail to, or implement another Reliability Standard or cover matters not addressed by other Reliability Standards. A Regional Reliability Standard is not binding upon any Member or Registered Entity, nor is it effective or enforceable, until the Regional Reliability Standard has been adopted by NERC and approved by the Commission as a Reliability Standard within the applicable Regional Entity or Regional Entities pursuant to delegated authorities.

Inherent in this definition, a ReliabilityFirst Standard will define certain obligations or requirements of entities that own, operate, plan, and use the BPS within the ReliabilityFirst geographical footprint. These obligations or requirements as contained in the ReliabilityFirst Standards are to be measurable and consistent with Good Utility Practice. Standards are not to include processes or procedures that implement a Standard. In addition, obligations, requirements or procedures imposed upon ReliabilityFirst by NERC reliability standards are not to be ReliabilityFirst Standards, unless those obligations, requirements or procedures require the establishment of a “policy or standard” as defined by the ReliabilityFirst By-laws.

Characteristics of a Regional Reliability Standard

A Standard is policy, including adequacy criteria to provide for the reliable regional and sub-regional planning and operation of the BPS, consistent with Good Utility Practice

A Standard shall generally have the following characteristics:

- **Measurable** - A Standard shall establish technical or performance requirements that can be practically measured.
- **Relative to NERC Reliability Standards** - A Standard generally must go beyond, add detail to, or implement NERC Reliability Standards, or cover matters not addressed in NERC Reliability Standards.

Format Requirements of a Regional Reliability Standard

A Standard shall consist of the requirements shown in the Regional Reliability Standard Template. These requirements apply to the development and revision of Standards. These requirements are necessary to achieve Standards that are measurable, enforceable, and consistent. Supporting documents to aid in the implementation of a Standard may be referenced by the Standard but are not part of the Standard itself. The most current

version of the approved NERC Reliability Standard template and its associated elements posted on the NERC website will be used at the time of the development of a ReliabilityFirst Regional Reliability Standard if different from the elements listed below.

Regional Reliability Standard Format Requirement Template Example

Identification Number	A unique identification number assigned in accordance with an administrative classification system to facilitate tracking and reference ReliabilityFirst documentation.
Title	A brief, descriptive phrase identifying the topic of the Standard.
Applicability	Clear identification of the functional classes of entities responsible for complying with the Standard, noting any specific additions or exceptions. If not applicable to the entire ReliabilityFirst area, then a clear identification of the portion of the BPS to which the Standard applies. Any limitation on the applicability of the Standard based on electric facility requirements should be described.
Effective Date and Status	The effective date of the Standard is the date of the FERC approval and the applicable implementation timeline.
Purpose	The purpose of the Standard. The purpose shall explicitly state what outcome will be achieved or is expected by this Standard.
Requirement(s)	Explicitly stated technical, performance, and preparedness requirements. Each requirement identifies what entity is responsible and what action is to be performed or what outcome is to be achieved. Compliance is mandatory for each statement in the requirements section.

Risk Factor(s)	The potential reliability significance of each requirement, designated as a High, Medium, or Lower Risk Factor in accordance with the criteria listed below: A High Risk Factor requirement (a) is one that, if violated, could directly cause or contribute to BPS instability, separation, or a cascading sequence of failures, or could place the BPS at an unacceptable risk of instability, separation, or cascading failures; or (b) is a requirement in a planning timeframe that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to BPS instability, separation, or a cascading sequence of failures, or could place the BPS at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to abnormal condition. A Medium Risk Factor requirement (a) is a requirement that, if violated, could directly affect the electrical state or the capability of the BPS, or the ability to effectively monitor and control the BPS, but is unlikely to lead to BPS instability, separation, or cascading failures; or (b) is a requirement in a planning timeframe that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly affect the electrical state or capability of the BPS, or the ability to effectively monitor, control, or restore the BPS, but is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to BPS instability, separation, or cascading failures, nor to hinder restoration to a normal condition. A Lower Risk Factor requirement is administrative in nature and (a) is a requirement that, if violated, would not be expected to affect the electrical state or capability of the BPS, or the ability to effectively monitor and control the BPS; or (b) is a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to affect the electrical state or capability of the BPS, or the ability to effectively monitor, control, or restore the BPS.
Measure(s)	Each requirement shall be addressed by one or more measurements that will be used to assess performance and outcomes for the purpose of determining compliance with the requirements stated above. Each measurement identifies to whom the measurement applies. Each measurement shall be tangible, and as objective as is practical. Achieving the full compliance level of each measurement is a necessary and sufficient indicator that the requirement was met.

Compliance Administration Elements

Compliance Monitoring Process	Defines for each measure: • The specific data or information that is required to measure performance or outcomes. • The entity that is responsible to provide the data or information for measuring performance or outcomes. • The process that will be used to evaluate information for the purpose of assessing performance or outcomes. • The entity that is responsible for evaluating information to assess performance or outcomes. • The time period in which performance or outcomes is measured, evaluated, and then reset. • Data retention requirements and assignment of responsibility for data archiving. • Violation severity levels.

Supporting Information Elements

Interpretations	Any ReliabilityFirst interpretations of the Standards that were developed, and approved in accordance with the “Interpretation of Standards” section of this Procedure, to expound on the application of the Standard for unusual or unique situations or provide clarifications.
Implementation Plan	Each ReliabilityFirst Standard shall have an associated implementation plan describing the effective date of the Standard or effective dates if there is a phased implementation. The implementation plan may also describe the implementation of the Standard in the compliance program and other considerations in the initial use of the Standard, such as necessary tools, training, etc. The implementation plan must be posted for at least one public comment period and be approved as part of the ballot of the standard.
Supporting References	This section references related documents that support reasons for, or provide additional information related to the Standard. Examples include, but are not limited to: • Glossary of Terms • Developmental history of the Standard and prior versions • Subcommittee(s) responsible for Standard • Notes pertaining to implementation or compliance • Standard references • Procedures/Practices • Training and/or Technical Reference

Roles in the Regional Reliability Standards Development Process

Process Roles

Originator - Any entity (person, organization, company, government agency, individual, etc.) that is directly and materially affected by the reliability of the ReliabilityFirst BPS, is allowed to request a Standard be developed or an existing Standard is modified, or deleted, by creating a Standards Authorization Request (SAR). See Appendix B.

Board – The ReliabilityFirst Board shall act on any proposed Standard that has gone through the process contained in this Procedure. Once the ReliabilityFirst Board approves a Standard, compliance with the Standard will be enforced consistent with the By-laws and the terms of the Standard.

Standards Committee (SC) - The ReliabilityFirst SC will consider which requests for new or revised Standards shall be assigned for development (or existing Standards

considered for deletion). The SC manages the Standards development process. The SC will advise the ReliabilityFirst Board on Standards presented for adoption by the ReliabilityFirst Board.

Standards Process Manager (SPM) – A person or persons on the ReliabilityFirst staff assigned the task of ensuring that the development, revision or deletion of Standards is in accordance with this Procedure. The SPM works to ensure the integrity of the process and consistency of quality and completeness of the Standards. The SPM facilitates the administration of all actions contained in all steps in the process.

Standards Process Staff – Employees of the ReliabilityFirst that work with or for the SPM.

Standard Drafting Team (SDT) – A team of technical experts, and typically including a member of the ReliabilityFirst Standards staff and the Originator, assigned the task of developing a proposed Standard based upon an approved SAR using the Standard development process contained in this Procedure.

Ballot Body (BB) – The Ballot Body comprises all entities that qualify for one or more of the categories and are registered with ReliabilityFirst as potential ballot participants in the voting on standards. The categories of registration within the Ballot Body and the registration process are described in Appendix D.

Ballot Pool – The Ballot Pool is comprised of those members of the Ballot Body that register to vote for each particular standard. A separate Ballot Pool is established for each standard up for vote. Only individuals who have joined the Ballot Pool for that particular standard are eligible to vote on a standard.

Reliability Committee (RC) – The ReliabilityFirst RC serves as a technical advisory body to address the reliability related activities required by the Reliability Standards via review and discussion of the regional activities as requested by the SC.

Regional Reliability Standard Development Process (Flow chart of Process shown in Appendix C)

Assumptions and Prerequisites

The ReliabilityFirst Regional Reliability Standards Development Process has the following characteristics:

- **Fair due process** - The ReliabilityFirst standards development process shall provide for reasonable notice and opportunity for public comment. At a minimum, the procedure shall include public notice of the intent to develop a standard, a public comment period on the

proposed standard, due consideration of those public comments, and a ballot of interested stakeholders.

- **Openness** - Participation is open to all Organizations who are directly and materially affected by the ReliabilityFirst region BPS reliability. There shall be no undue financial barriers to participation. Participation shall not be conditioned upon membership in the ReliabilityFirst, and shall not be unreasonably restricted on the basis of technical qualifications or other such requirements. Meetings of SDTs are open to the ReliabilityFirst membership and to others.
- **Balanced** - The ReliabilityFirst standards development process strives to have an appropriate balance of interests and shall not be dominated by any two interest categories and no single interest category shall be able to defeat a matter.
- **Inclusive** - Any entity (person, organization, company, government agency, individual, etc.) with a direct and material interest in the BPS in the ReliabilityFirst area shall have a right to participate by: a) expressing a position and its basis, b) having that position considered, and c) having the right to appeal.
- **Transparent** - All actions material to the development of ReliabilityFirst Standards shall be transparent. All standards development meetings shall be open and publicly noticed on ReliabilityFirst's Web site.
- Does not unnecessarily delay development of the proposed Standard.

Note: The term "days" refers to calendar days.

Each standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of the reliability of the regional BPS. Each standard shall also be consistent with all of the reliability principles, thereby ensuring that no standard undermines reliability through an unintended consequence.

While ReliabilityFirst Standards are intended to promote reliability, they must at the same time accommodate competitive electricity markets. Reliability is a necessity for electricity markets, and robust electricity markets can support reliability. Recognizing that BPS reliability and electricity markets are inseparable and mutually interdependent, all ReliabilityFirst Standards shall be consistent with NERC's market interface principles. Consideration of the market interface principles is intended to ensure that standards are written such that they achieve their reliability objective without causing undue restrictions or adverse impacts on competitive electricity markets.

ReliabilityFirst will coordinate with NERC such that the acknowledgement of receipt of a standard request identified in step 1, notice of comment posting period identified in step 4, and notice for vote identified in step 5 below are concurrently posted on both the ReliabilityFirst and NERC websites.

Step 1 - Development of a Standards Authorization Request (SAR) to Develop, Revise or Delete a Regional Reliability Standard

Any individual representing an organization (Originator) which is directly or materially impacted by the operation of the BPS within the geographical footprint of the ReliabilityFirst may request, via a submittal of a Standard Authorization Request (SAR) form, the development, modification, or deletion of a ReliabilityFirst Standard. Any such request shall be submitted to the ReliabilityFirst SPM, or his/her designee, or by another process as otherwise posted on the ReliabilityFirst website. The SAR form may be downloaded from the ReliabilityFirst website.

The SAR contains a description of the proposed Standard subject matter containing sufficiently descriptive detail to clearly define the purpose, scope, impacted parties, and other relevant information of the proposed Standard. The SPM will verify that the submitted SAR form has been adequately completed. The SPM may offer the Originator suggestions regarding changes and/or improvements to improve clarity and assist the ReliabilityFirst community to understand the Originator's intent and objectives. The Originator is free to accept or reject these suggestions. Within 15 days the SPM will electronically acknowledge receipt of the SAR.

The SPM will forward the adequately complete SAR to the ReliabilityFirst SC, at which time, the SC will, post the SAR for comments within 15 days, SARs will be posted and publicly noticed.

Comments on the SARs will be accepted for a 30-day period from the notice of posting. Comments will be accepted online using an internet-based application. The SPM will provide a copy of the comments to the Originator and the SC.

Based on the comments, the SC shall make available a consideration of comments report and determine the disposition of the SAR (within 60 calendar days following the SAR commenting period). The disposition decision and decision process shall use the normal "business rules and procedures" of the SC then in effect. The SC may take one of the following actions³ in accordance with the ReliabilityFirst Standards Committee Governance document:

- Accept the SAR as a candidate for: development of a new Standard, revision of an existing Standard or deletion of an existing Standard. The SC may, in its sole discretion, expand or narrow the scope of the SAR under consideration. The SC

³Actions by the Standards Committee may be appealed per the Appeals process in Appendix A

shall prioritize the development of SARs as may be required based on the number of SARs under development at any time.

- Reject the SAR. If the SC rejects a SAR, a written explanation for rejection will be delivered to the Originator within 30 days of the decision.
- Remand the SAR back to the Originator for redirection to the NERC process. In cases where there is a Reliability need identified in the SAR but it does not meet the criteria for Regional standards (more stringent reliability requirements than the NERC reliability standard or cover matters not covered by an existing NERC reliability standard), the Standards Committee will assist the Originator in submitting the SAR to NERC.
- Remand the SAR back to the Originator for additional work. The SPM will make reasonable efforts to assist the Originator in addressing the deficiencies identified by the SC. The Originator may then resubmit the modified SAR using the process above. The Originator may choose to withdraw the SAR from further consideration prior to re-submittal to the SC

Any SAR that is accepted by the SC for development of a Standard (or modification or deletion of an existing Standard) shall be posted for public viewing on the ReliabilityFirst website within 30 days of acceptance by the SC. The status of posted SARs will be publicly posted.

Any documentation of the deliberations of the SC concerning SARs shall be made available according to the “ReliabilityFirst Standards Committee Governance” document then in effect.

The SC shall submit a written report to the ReliabilityFirst Board on a periodic basis (at least at every regularly scheduled ReliabilityFirst Board meeting) showing the status of all SARs that have been brought to the SC for consideration.

Step 2 – *Formation of the Standard Drafting Team and Declaration of Milestone Date*

Upon acceptance by the SC of a SAR for development of a new Standard (or modification or deletion of an existing Standard), the SC shall direct the SPM to develop a qualified balance slate for the SDT using the specific directions and preferences of the SC. The SPM will send out self-nomination forms to solicit SDT nominees. The SDT will consist of a group of people (members of ReliabilityFirst and, as appropriate, non-members) who collectively have the necessary technical expertise and work process skills. The SPM will recommend a slate of ad-hoc individuals or a preexisting task force, work group or similar for the SDT based upon the SC’s desired SDT capabilities.

The SC may also direct the SPM to designate an existing ReliabilityFirst committee (or subset thereof) as the SDT augmented by other persons as may be appropriate for the

subject matter. The SC will insure that SDT membership includes all necessary administrative support. This support typically includes a ReliabilityFirst staff member and the Originator if he/she chooses to participate. The SC appoints the interim chair (should not be a staff person) of the SDT. The SDT will elect the permanent Chair and Vice-chair at its first meeting.

The SPM submits the proposed list of names of the SDT to the SC. The SC will either accept the recommendations of the SPM or modify the SDT slate, as it deems appropriate within 60 days of accepting a SAR for development.

Upon approval of the SDT slate, the SC will declare a preliminary date on which the SDT is expected to have ready a completed draft Standard and associated supporting documentation available for consideration by the ReliabilityFirst membership.

Step 3 – Work and Work Product of the Standard Drafting Team

The SDT will then develop a work plan for completing the Standard development work, including the establishment of milestones for completing critical elements of the work in sufficient detail to ensure that the SDT will meet the deadline established by the SC or the SDT shall propose an alternative date. This plan is then delivered to the SC for its concurrence.

The SDT is to meet, either in person or via electronic means as necessary, establish sub-work teams (made up of members of the SDT) as necessary, and performs other activities to address the parameters of the SAR and the milestone date(s) established by the SC.

The work product of the SDT will consist of the following:

- A draft Standard consistent with the SAR on which it was based.
- An assessment of the impact of the SAR on neighboring regions, and appropriate input from the neighboring regions if the SAR is determined to impact any neighboring region.
- An implementation plan, including the nature, extent and duration of field-testing, if any.
- Identification of any existing Standard that will be deleted, in part or whole, or otherwise impacted by the implementation of the draft Standard.
- Technical reports, white papers and/or work papers that provide technical support for the draft Standard under consideration.
- Document the perceived reliability impact should the Standard be approved.

Upon completion of these tasks, the SDT submits these documents to the SC, which will verify that the proposed Standard is consistent with the SAR on which it was developed

The SDT regularly (at least once each month) informs the SC of its progress in meeting a timely completion of the draft Standard. The SDT may request of the SC scope changes of the SAR at any point in the Standard development process.

The SC may, at any time, exercise its authority over the Standards development process by directing the SDT to move to Step 4 and post for comment the current work product. If there are competing drafts, the SC may, at its sole discretion, post the version(s) of the draft Standard for comment on the *ReliabilityFirst* website. The SC may take this step at any time after a SDT has been commissioned to develop the Standard.

Step 4 – *Comment Posting Period*

At the direction from the SC, the SPM then facilitates the posting of the draft Standard on the *ReliabilityFirst* website, along with a draft implementation plan and supporting documents, for a 30-day comment period. The SPM shall also inform *ReliabilityFirst* Members and other potentially interested entities inside or outside of *ReliabilityFirst* of the posting using typical membership communication procedures then currently in effect or by other means as deemed appropriate. As early as the start of the first posting for comment, entities may join the Ballot Pool established for the eventual voting on the proposed standard. The Ballot Pool category description and associated requirements are in Appendix D.

Within 30 days of the conclusion of 30-day comment posting period the SDT shall convene and consider changes to the draft Standard, the implementation plan and/or supporting technical documents based upon comments received. Based upon these comments, the SDT may elect to return to step 3 to revise the draft Standard, implementation plan and/or supporting technical documentation.

The SDT shall prepare a “modification report” summarizing the comments received and the changes made as a result of these comments. The modification report also summarizes comments that were rejected by the SDT and the reason(s) that these comments were rejected, in part or whole. Responses to all comments will be posted on the *ReliabilityFirst* website no later than the next posting of the proposed Standard.

Step 5 – *Posting for Voting by ReliabilityFirst Registered Ballot Body*

Upon recommendation of the SDT, and if the SC concurs that all of the requirements for development of the Standard have been met, the SPM will post the revised draft Standard, implementation plan, supporting technical documentation and the “modification report”. Once the notice for a vote has been issued, no substantive modifications may be made to the proposed standard unless the revisions are posted and a new notice of the vote is issued.

Entities may register in the BB at any time during the Standards process. The BB category description and associated rules are in Appendix D.

By 11:59 PM Central Prevailing Time (CPT) of the seventh day of the 15 day pre-ballot posting period, registered BB members intending to vote on the proposed standard must have joined the Ballot Pool established for the eventual voting on the proposed standard being posted. The SPM will schedule a Vote by the Ballot Pool which is to be scheduled to commence no sooner than 15 days and no later than 30 days following this posting. The Vote by the Ballot Pool is an advisory to the ReliabilityFirst Board.

The Ballot Pool shall be allowed to vote over a period of 15 days. Votes will be submitted electronically, but may be submitted through other means as approved by the SC.

All BB members are eligible to participate in voting on proposed new Standards, Standard revisions or Standard deletions. There is a requirement to join a Ballot Pool to participate in voting for each standard.

The voting results will be composed of only the votes from BB entities that have joined the Ballot Pool for the standard being voted on and responding within the voting period. Votes may be accompanied by comments explaining the vote, but are not required. All comments shall be responded to and posted to the ReliabilityFirst website prior to going to the SC or Board.

Step 6A – Voting Receives Two-Thirds or Greater Majority of Affirmative Category Votes

A two-thirds or greater majority⁴ of votes within a category determines the vote for that category. The Initial ballot has passed if there is a two-thirds or greater affirmative majority of category votes (only those categories with votes cast will be considered) during the 15-day voting period and a quorum⁵ is met.

If there is at least one (1) Negative vote with comment during the initial ballot, then the standard will be posted for a 10-day Recirculation ballot. If there are no Negative votes with comments, the SC will forward the Standard to the ReliabilityFirst Board for action (Step 7). In the recirculation ballot, members of the Ballot Pool shall again be presented the proposed standard (that has not been significantly changed from the previous ballot) along with the reasons for negative votes, the responses, and any resolution of the differences. An insignificant revision is a revision that does not change the scope, applicability, or intent of any requirement and includes but is not limited to things such as correcting the numbering of a requirement, correcting the spelling of a word, adding an obviously missing word, or rephrasing a requirement for improved clarity. Where there is a question as to whether a proposed modification is “substantive” the Standards Committee shall make the final determination. All members of the Ballot Pool shall be permitted to reconsider and change their vote from the prior ballot. Members of the Ballot Pool who did not respond to the prior ballot shall be permitted to vote in the

⁴ For the purposes of determining majority within a category, an abstention is not considered a vote.

⁵ A quorum is achieved when three-fourths (75%) or greater of the ballot pool casts a vote.

recirculation ballot. In the recirculation ballot, Ballot Pool members may indicate a revision to their original vote otherwise their vote shall remain the same as in their prior ballot.

Upon successful completion of the initial and recirculation voting periods, the SC will forward the Standard to the ReliabilityFirst Board for action (Step 7).

Step 6B – Voting Does Not Receive Two-Thirds or Greater Majority of Affirmative Category Votes or a Quorum⁵ is Not Met

If a draft Standard does not receive a two-thirds or greater affirmative majority of votes determined for each category (only those categories with votes cast will be considered) or does not reach quorum during the 15-day Initial voting period, the SC may:

- Direct the SDT to respond to ballot comments and post the standard for a 10-day Recirculation ballot (as discussed in Step 6A) to determine if the response to comments alleviates reasons for the Negative initial ballots.
- Direct the existing SDT to reconsider or modify certain aspects of the draft Standard and/or implementation plan. The resulting draft Standard and/or implementation plan will be posted for a second initial voting period. The SC may require a second comment period prior to the second voting period. The second posting of the draft Standard, implementation plan, and supporting documentation shall be within 60 days of the SC action.
 - If there is a two-thirds or greater affirmative majority of categories with votes cast and a quorum is met during the second initial ballot and second recirculation ballot, the SC will forward it to the ReliabilityFirst Board for action (Step 7).
 - If a draft Standard does not receive a two-thirds or greater majority of affirmative category votes cast during the second initial ballot or a quorum is not met, the SC will refer the draft Standard and implementation plan to the ReliabilityFirst Board. The SC may also submit an assessment, opinion and recommendations to the ReliabilityFirst Board (Step 7).
- Revise the SAR on which the draft Standard was based and remand the development work back to the original SDT or a newly appointed SDT. The resulting draft Standard and/or implementation plan will be posted for a second voting period. The SC may require a second comment period prior to a second voting period. The second posting of the draft Standard, implementation plan, and supporting documentation shall be within 60 days of the SC action.
 - If there is a two-thirds or greater affirmative majority of categories with votes cast and a quorum is met during the second initial ballot and second

recirculation ballot, the SC will forward it to the ReliabilityFirst Board for action (Step 7).

- If a draft Standard does not receive a two-thirds or greater majority of affirmative category votes cast during the second voting period or a quorum is not met, the SC will refer the draft Standard and implementation plan to the ReliabilityFirst Board. The SC may also submit an assessment, opinion and recommendations to the ReliabilityFirst Board (Step 7).
- Recommend termination of all work on the development of the Standard action under consideration and so notify the ReliabilityFirst Board.

Step 7 – Action by the ReliabilityFirst Board

A draft Standard submitted to the ReliabilityFirst Board for action must be publicly posted at least 30 days prior to action by the Board. At a regular or special meeting, the ReliabilityFirst Board shall consider adoption of the draft Standard. The Board will consider the results of the voting and dissenting opinions. The Board will consider any advice offered by the SC.

Draft Standards that received a two-thirds or greater of categories with votes cast shall be delivered to the ReliabilityFirst Board for their action. The ReliabilityFirst Board shall be provided with an “informational package” which includes:

- The draft Standard and any modification or deletion of other related existing Standard(s)
- Implementation Plan (including recommending field testing and effective dates)
- Technical Documentation supporting the draft Standard
- A summary of the vote and summary of the comments and responses that accompanied the votes.

The ReliabilityFirst Board is expected to either:

- Approve the draft Standard action with only minor or no modification. Under no circumstances may the Board substantively modify the proposed regional reliability standard.
- Remand to the SC with comments and instructions, or
- Disapprove the draft Standard action without recourse.

Draft Standards that did not receive a two-thirds or greater of categories with votes cast in the second voting period shall be delivered to the ReliabilityFirst Board for their action. The ReliabilityFirst Board shall be provided with an “informational package”.

The ReliabilityFirst Board is expected to either:

- Approve the draft Standard action with only minor or no modification. Under no circumstances may the Board substantively modify the proposed regional reliability standard.
- Remand to the SC with comments and instructions, or
- Disapprove the draft Standard action without recourse.

Once a regional ReliabilityFirst Standard is approved by the Board, the standard will be submitted to NERC for approval and filing with FERC.

Step 8 - Implementation of a Regional Reliability Standard

Upon approval of a draft Standard action by the FERC, the SPM will notify the membership and applicable entities within the ReliabilityFirst footprint of the effective date through the normal and customary membership communication procedures and processes then in effect. The SPM will also notify the ReliabilityFirst Compliance Staff for integration into the ReliabilityFirst Compliance Program.

Appendix A

Maintenance of Regional Reliability Standards Development Process

Significant changes to this Procedure shall begin with the preparation of a SAR and be handled using the same procedure as a request to add, modify, or delete a Standard.

The ReliabilityFirst SC has the authority to make ‘minor’ changes to this Procedure as deemed appropriate by the SC and subject to the SC voting practices and procedures according to the “ReliabilityFirst Standards Committee Governance” document. The SC shall promptly notify the ReliabilityFirst Board of such ‘minor’ changes to this Procedure for their review and concurrence at the next ReliabilityFirst Board meeting.

Maintenance of Regional Reliability Standards

The SC shall ensure that each Standard shall be reviewed at least once every five years from the effective date of the Standard or the latest revision to the Standard, whichever is the later. The review process shall be conducted by soliciting comments from the stakeholders. If no changes are warranted, the SC shall recommend to the ReliabilityFirst Board that the Standard be reaffirmed. If the review indicates a need to revise or delete a Standard, a SAR shall be prepared and submitted in accordance with the standards development process contained in this Procedure.

Urgent Action

Under certain conditions, the SC may designate a proposed Standard or revision to a Standard as requiring urgent action. Urgent action may be appropriate when a delay in implementing a proposed Standard or revision could materially impact reliability of the BPS. The SC must use its judgment carefully to ensure an urgent action is truly necessary and not simply an expedient way to change or implement a Standard.

A requester prepares a SAR and a draft of the proposed Standard and submits both to the SPM. The SAR must include a justification for urgent action. The SPM submits the request to the SC for its consideration. If the SC designates the requested Standard or revision as an urgent action item, then the SPM shall immediately post the draft for pre-ballot review. This posting requires a minimum 30-day posting period before the ballot and applies the same voting procedure as detailed in Step 5. Processing will continue as outlined in the subsequent steps. In the event additional drafting is required, a SDT will be assembled as outlined in the Procedure.

Any Standard approved as an urgent action shall have a termination date specified that shall not exceed one year from the approval date. Should there be a need to make the Standard permanent, then the Standard would be required to go through the full Standard

development process. All urgent action Standards require ReliabilityFirst Board, NERC and FERC approval, as outlined for Standards in the regular process.

Urgent actions that expire may be renewed using the urgent action process again, in the event a permanent Standard is not adopted. In determining whether to authorize an urgent action Standard for a renewal ballot, the SC shall consider the impact of the Standard on the reliability of the BPS and whether expeditious progress is being made toward a permanent replacement Standard. The SC shall not authorize a renewal ballot if there is insufficient progress toward adopting a permanent replacement Standard or if the SC lacks confidence that a reasonable completion date is achievable. The intent is to ensure that an urgent action Standard does not in effect take on a degree of permanence due to the lack of an expeditious effort to develop a permanent replacement Standard. With these principles, there is no predetermined limit on the number of times an urgent action may be renewed. However, each urgent action Standard renewal shall be effective only upon approval by the ReliabilityFirst Board, NERC and FERC.

Any person or entity, including the SDT working on a permanent replacement Standard, may at any time submit a SAR proposing that an urgent action Standard become a permanent Standard by following the full Standards process.

Interpretations of Standards

All persons who are directly and materially affected by the reliability of ReliabilityFirst BPS shall be permitted to request an interpretation of the standard. The person requesting an interpretation will send a request to the SPM explaining the specific circumstances surrounding the request and what clarifications are required as applied to those circumstances. The request should indicate the material impact to the requesting party or others caused by the lack of clarity or a possibly incorrect interpretation of the standard.

The SPM, along with guidance from the SC, will assemble a team with the relevant expertise to address the request. The Interpretation Drafting Team (IDT) typically consists of members from the original SDT. The SPM submits the proposed list of names of the IDT to the SC. The SC will either accept the recommendations of the SPM or modify the IDT slate.

As soon as practical (not more than 45 days), the team will prepare an initial draft interpretation of the standard addressing the issues raised. Once the IDT has completed the initial draft interpretation, the team will post the draft for a 30-day informal⁶ stakeholder comment period. The IDT will review the stakeholder feedback and may make changes before preparing a final draft of the interpretation. The IDT will then

⁶ An informal comment period does not require the IDT to respond to every stakeholder comment and is only used to make potential changes for the final draft of the interpretation.

forward the draft interpretation to the SPM. The SPM will forward the interpretation to the Reliability Committee (RC). Barring receipt of an opinion from the RC within 21 calendar days, that the interpretation is not technically appropriate for the Standard, respectively, the SPM will forward the interpretation to the SC. The SC will determine if the interpretation is consistent with the Standard and does not add additional requirements to the standard. The SC will forward the interpretation to the ReliabilityFirst Board for informational purposes as being appended to the approved Standard.

Note: In the event that the RC determines that the interpretation makes the standard technically inappropriate the RC shall provide an explanation of its reasoning to the SPM and IDT for inclusion in a subsequent revision. In either case, the IDT and SPM will continue to re-circulate the interpretation as stated above.

The interpretation will stand until such time as the standard is revised through the normal process, at which time the standard will be modified to incorporate the clarifications provided by the interpretation.

Appeals

Persons who have directly and materially affected interests and who have been or will be adversely affected by any substantive or procedural action or inaction related to the development, approval, revision, reaffirmation, or withdrawal of a Standard shall have the right to appeal. This appeals process applies only to the Standards process as defined in this Procedure.

The burden of proof to show adverse effect shall be on the appellant. Appeals shall be made within 30 days of the date of the action purported to cause the adverse effect, except appeals for inaction, which may be made at any time. In all cases, the request for appeal must be made prior to the next step in the process.

The final decisions of any appeal shall be documented in writing and made public.

The appeals process has two levels, with the goal of expeditiously resolving the issue to the satisfaction of the participants:

Level 1 Appeal

Level 1 is the required first step in the appeals process. The appellant submits a complaint in writing to the SPM that describes the substantive or procedural action or inaction associated with a Standard or the standards process. The appellant describes in the complaint the actual or potential adverse impact to the appellant. Assisted by any necessary staff and committee resources, the SPM shall prepare a written response addressed to the appellant as soon as practical but not more than 45-days after receipt of the complaint. If the appellant accepts the response as a satisfactory resolution of the

issue, both the complaint and response will be made a part of the public record associated with the standard.

Level 2 Appeal

If after the Level 1 Appeal the appellant remains unsatisfied with the resolution, as indicated by the appellant in writing to the SPM, the SPM shall convene a Level 2 Appeals Panel. This panel shall consist of five members total appointed by the ReliabilityFirst Board.

In all cases, Level 2 Appeals Panel members shall have no direct affiliation with the participants in the appeal.

The SPM shall post the complaint and other relevant materials and provide at least 30-days notice of the meeting of the Level 2 Appeals Panel. In addition to the appellant, any person that is directly and materially affected by the substantive or procedural action or inaction referenced in the complaint shall be heard by the panel. The panel shall not consider any expansion of the scope of the appeal that was not presented in the Level 1 Appeal. The panel may in its decision find for the appellant and remand the issue to the SC with a statement of the issues and facts in regard to which fair and equitable action was not taken. The panel may find against the appellant with a specific statement of the facts that demonstrate fair and equitable treatment of the appellant and the appellant's objections. The panel may not, however, revise, approve, disapprove, or adopt a reliability standard. The actions of the Level 2 Appeals Panel shall be publicly posted.

In addition to the foregoing, a procedural objection that has not been resolved may be submitted to the ReliabilityFirst Board for consideration at the time the Board decides whether to adopt a particular reliability standard. The objection must be in writing, signed by an officer of the objecting entity, and contain a concise statement of the relief requested and a clear demonstration of the facts that justify that relief. The objection must be filed no later than 30-days after the announcement of the vote on the Standard in question.

Appendix B

Standard Authorization Request

The SC shall be responsible for implementing and maintaining this form as needed to support the information requirements of the standards development process in this Procedure. Changes to this form are considered minor, and therefore subject to only the approval of the SC.

ReliabilityFirst Standard Authorization Request Form

**ReliabilityFirst
will complete**

Title of Proposed Standard
Request Date

ID
Authorized for Posting
Authorized for Development

SAR Originator Information

Name	SAR Type (Check box for one of these selections.)	
Company	☐	New Standard
Telephone	☐	Revision to Existing Standard
Fax	☐	Withdrawal of Existing Standard
E-mail	☐	Urgent Action

Purpose (Provide one or two sentences.)

Industry Need (Provide one or two sentences.)

Brief Description (A few sentences or a paragraph.)

Reliability Functions

The Standard will Apply to the Following Functions (Check box for each one that applies.)

	Reliability Authority	Ensures the reliability of the bulk transmission system within its Reliability Authority area. This is the highest reliability authority.
	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within its metered boundary and supports system frequency in real time
	Generator Owner	Owns and maintains generating units
	Interchange Authority	Authorizes valid and balanced Interchange Schedules
	Planning Authority	Plans the BPS
	Resource Planner	Develops a long-term (generally one year and beyond) plan for the resource adequacy of specific loads (customer demand and energy requirements) within a Planning Authority Area
	Transmission Planner	Develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within its portion of the Planning Authority Area
	Transmission Service Provider	Provides transmission services to qualified market participants under applicable transmission service agreements
	Transmission Owner	Owns transmission facilities
	Transmission Operator	Operates and maintains the transmission facilities, and executes switching orders
	Distribution Provider	Provides and operates the “wires” between the transmission system and the customer

	Generator Operator	Operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services
	Purchasing-Selling Entity	The function of purchasing or selling energy, capacity and all necessary Interconnected Operations Services as required
	Load-Serving Entity	Secures energy and transmission (and related generation services) to serve the end user
	Market Operator	Integrates energy, capacity, balancing, and transmission resources to achieve an economic, reliability-constrained dispatch of resources. The dispatch may be either cost-based or bid-based
	Regional Reliability Organizations	An entity that ensures that a defined area of the BPS is reliable, adequate and secure. A member of the North American Electric Reliability Council. The Regional Reliability Organization can serve as the Compliance Monitor

NOTE: The SDT may find it necessary to modify the initial reliability function responsibility assignment as a result of the standards development and comments received.

Reliability Principles

<i>Applicable Reliability Principles (Check box for all that apply.)</i>	
	1. Interconnected BPS shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
	2. The frequency and voltage of interconnected BPS shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
	3. Information necessary for the planning and operation of interconnected BPS shall be made available to those entities responsible for planning and operating the systems reliably.
	4. Plans for emergency operation and system restoration of interconnected BPS shall be developed, coordinated, maintained, and implemented.
	5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected BPS.
	6. Personnel responsible for planning and operating interconnected BPS shall be trained, qualified, and have the responsibility and authority to implement actions.
	7. The security of the interconnected BPS shall be assessed, monitored, and maintained on a wide-area basis.

Market Interface Principles

<i>Does the proposed Standard comply with all of the following Market Interface Principles?</i>	
Recognizing that reliability is an essential requirement of a robust North American economy:	
yes or no	1. A reliability standard shall not give any market participant an unfair competitive advantage.
yes or no	2. A reliability standard shall neither mandate nor prohibit any specific market structure.
yes or no	3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.
yes or no	4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.

Detailed Description (Provide enough detail so that an independent entity familiar with the industry could draft a Standard based on this description.)

Related Standards (NERC and Regional)

Standard No.	Explanation

Related SARs

SAR ID	Explanation

Implementation Plan

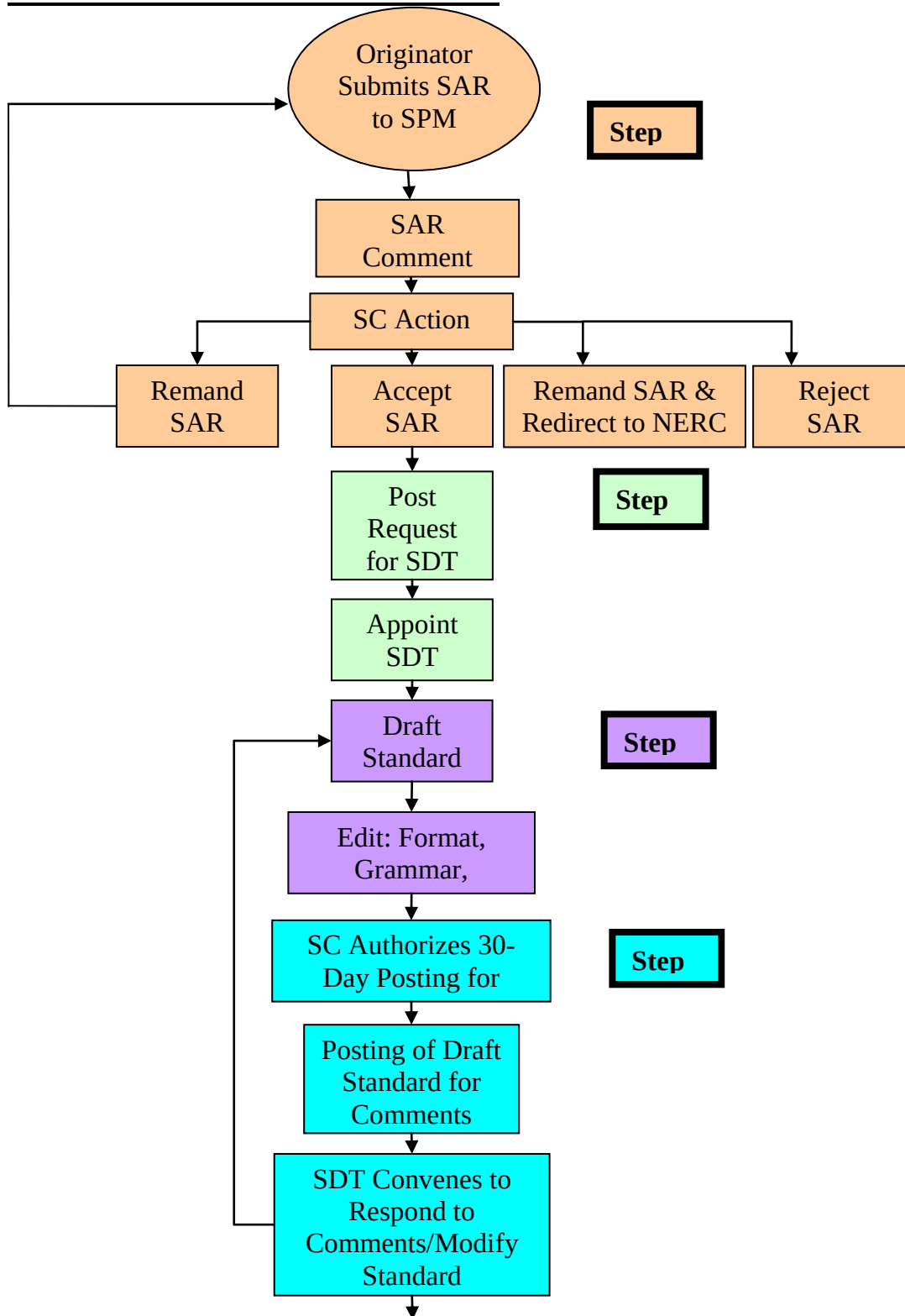
Description <i>(Provide plans for the implementation of the proposed standard, including any known systems or training requirements. Include the reliability risk(s) associated with the violation that the standard will mitigate, and the costs associated with implementation.)</i>	
Proposed Implementation	days after Board adoption or
on (date):	

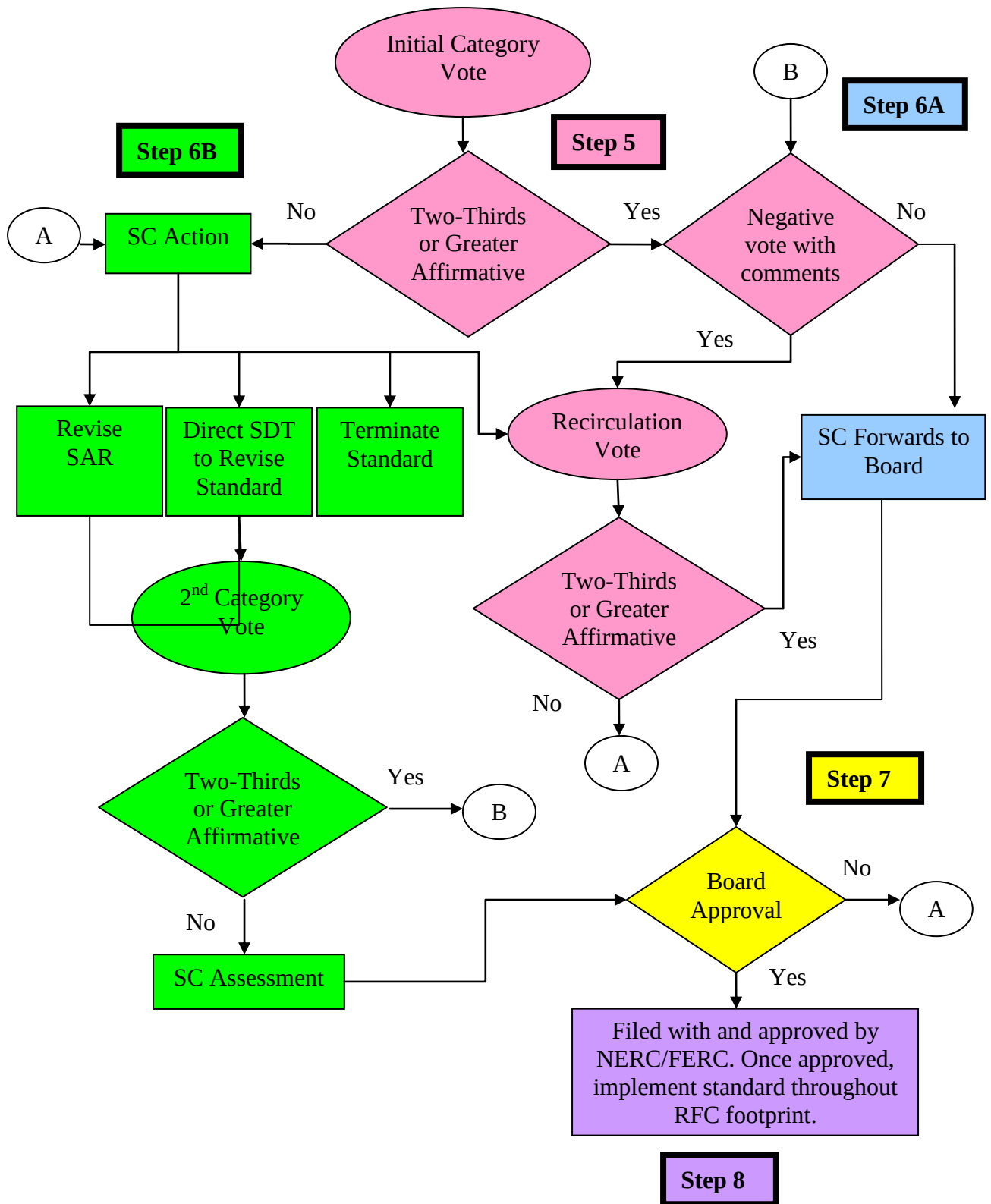
Assignments

	Assignment
Team Members	
ReliabilityFirst Staff	

Appendix C

Flowchart for Standards Process





Appendix D

Ballot Pool Categories

For the purposes of category Ballot Pool registration and voting, a person or entity may join the registered Ballot Pool to vote on standards, whether or not such person or entity is a member of ReliabilityFirst.

A corporation or other organization with integrated operations or with affiliates that qualifies to belong to more than one category (e.g., Transmission Owners and Load Serving Entities) may join and vote once in each category for which it qualifies, provided that each category constitutes a separate membership in the Ballot Body and the organization is represented in each category by a different representative. Affiliated entities are collectively limited to one membership in each category in the Ballot Pool for which they are qualified.

Category 1 – Transmission Owner, Transmission Operator, Transmission Service Provider

Category 2 – Generator Owner, Generator Operator

Category 3 – Load Serving Entity, Purchasing and Selling Entity, End User

Category 4 – Reliability Coordinator, Planning Coordinator, Transmission Planner, Resource Planner, Regional Transmission Organization, Balancing Authority, regulatory or governmental agency

Category 5 – Distribution Provider

Ballot Body Registration

Entities may register in the BB at any time during the Standards process. The SPM shall review all applications for joining the BB, and make a determination of whether they qualify for the self-selection category. In order to comment or vote you must have an active membership in the BB. When you submit your registration request to join the BB, you are placed in a “pending stage” until your account is activated. Activation of your account may take up to 24 hours. You will be unable to submit comments or join a Ballot Pool until your account is activated. The contact designated as primary representative to ReliabilityFirst is the voting member with the secondary contact as the backup.

Note: Registration for a BB is not the same as registration for the compliance registry. Although the terminology used to describe the BB categories in most cases has the same

meaning as the terms used in the NERC Functional Model, registration in a BB goes beyond the compliance registry in that entities smaller than those stated in the compliance registry guidelines are allowed to register in a BB. Entities shall have evidence that they qualify for the BB category they register in. Such evidence shall be available for the SPM review to verify BB registration and may include compliance registration.

Ballot Pool Formation

In order to participate in voting on a particular standard, an entity must join the Ballot Pool being established for the standard as follows:

- 1 – As early as the start of the first posting for comment, entities may join the Ballot Pool established for the eventual voting on the proposed standard being posted.
- 2 - By close of business of the seventh day of the 15 day pre ballot posting period, entities wishing to vote must have joined the Ballot Pool established for the eventual voting on the proposed standard being posted.

ReliabilityFirst Corporation Reliability Standards Development Procedure

Version ~~4~~³

Reliability*First* Corporation Reliability Standards Development Procedure

Table of Contents

Introduction	1
Background.....	2
Regional Reliability Standard Definition, Characteristics, and Elements	3
Roles in the Regional Reliability Standards Development Process.....	7
Regional Reliability Standards Development Process	8
Appendix A: Maintenance of Regional Reliability Standards Development Process.....	17
Appendix B: Standard Authorization Request.....	21
Appendix C: Flowchart for Standards Process	28
Appendix D: Ballot Pool Categories and Registration.....	30

ReliabilityFirst Corporation Reliability Standards Development Procedure

Introduction

This procedure establishes the process for adoption of a Regional Reliability Standard (hereinafter referred to as “Standard”) of the ReliabilityFirst Corporation (ReliabilityFirst) and the development of consensus for adoption, approval, revision, reaffirmation, and deletion of such Standards. ReliabilityFirst Standards provide for the reliable regional and sub-regional planning and operation of the Bulk Power System¹ (BPS), consistent with Good Utility Practice¹ within the ReliabilityFirst geographical footprint.

This procedure was developed under the direction of the ReliabilityFirst Board of Directors (Board), who may request changes to this ReliabilityFirst Reliability Standards Development Procedure (hereinafter referred to as “this Procedure”) as deemed appropriate. A procedure for revising this Procedure is contained in Appendix A. This Procedure is consistent with the North American Electric Reliability Corporation (NERC) Reliability Standards Development Procedure.

ReliabilityFirst standards shall be subject to approval by NERC, as the electric reliability organization, and by the Federal Energy Regulatory Commission (FERC) before becoming mandatory and enforceable under Section 215 of the FPA. No Standard shall be effective within the ReliabilityFirst area unless filed by NERC with FERC and approved by FERC. ~~The approval date of each ReliabilityFirst standard is upon ReliabilityFirst Board approval.~~ The effective date will depend on the implementation plan that is provided with each new or revised standard. ~~The ReliabilityFirst standard is mandatory and enforceable (without monetary penalties for non-compliance) upon the effective date after ReliabilityFirst Board approval for applicable entities that are members of ReliabilityFirst.~~³ The ReliabilityFirst standard is mandatory and enforceable (with monetary penalties for non-compliance) to all applicable Registered Entities within the ReliabilityFirst footprint upon approval by the FERC. ~~No Standard shall be effective within the ReliabilityFirst area unless filed by NERC with FERC and approved by FERC.~~ The effective date for non-members upon the FERC approval will be ~~determined by the implementation plan that is provided with each new or revised standard.~~

ReliabilityFirst Standards shall provide for as much uniformity as possible with NERC reliability standards across the interconnected BPS. A ReliabilityFirst Standard shall be more stringent than a NERC reliability standard, including a regional difference that addresses matters that the NERC reliability standard does not, or shall be a regional difference necessitated by a physical difference in the BPS. A ReliabilityFirst Standard

¹ As defined in the ReliabilityFirst By-laws

that satisfies the statutory and regulatory criteria for approval of proposed NERC reliability standards, and that is more stringent than a NERC reliability standard, would generally be acceptable.

ReliabilityFirst Standards, when approved by FERC, shall be made part of the body of NERC reliability standards and shall be enforced upon all applicable BPS owners, operators, and users within the ReliabilityFirst area, regardless of membership in the region.

Background

Regions may develop, through their own processes, separate “Regional Standards” (ReliabilityFirst Standards) that go beyond, add detail to or aid implementation of NERC reliability standards, or otherwise address issues that are not addressed in NERC reliability standards.

As a condition of ReliabilityFirst membership, all ReliabilityFirst Members² agree to adhere to the NERC reliability standards. As such, the ReliabilityFirst and its Members will adhere to the NERC reliability standards in addition to the ReliabilityFirst Standards. NERC reliability standards and the ReliabilityFirst Standards are both to be included within the ReliabilityFirst Compliance Program.

ReliabilityFirst Standards are intended to apply only to that part of the Eastern Interconnection within the ReliabilityFirst geographical footprint. The development of these ReliabilityFirst Standards is developed according to the following principles via the process contained within this Procedure:

- Developed in a fair and open process that provided an opportunity for all interested parties to participate;
- Does not have an adverse impact on commerce that is not necessary for reliability;
- Provides a level of BPS reliability that is adequate to protect public health, safety, welfare, and national security and would not have a significant adverse impact on reliability; and
- Based on a justifiable difference between Regions or between sub-Regions within the Regional geographic area.

² As defined in the ReliabilityFirst By-laws

Regional Reliability Standard Definition, Characteristics, and Elements

Definition of a Reliability Standard

As contained in the ReliabilityFirst By-laws, ReliabilityFirst “Regional Reliability Standard” shall mean a type of Reliability Standard that is applicable only within a particular Regional Entity or group of Regional Entities. A Regional Reliability Standard may augment, add detail to, or implement another Reliability Standard or cover matters not addressed by other Reliability Standards. A Regional Reliability Standard is not binding upon any Member or Registered Entity, nor is it effective or enforceable, until the Regional Reliability Standard has been s, upon-adoptedion by NERC and approved~~ed~~at by the Commission as a Reliability Standard enforced-within the applicable Regional Entity or Regional Entities pursuant to delegated authorities.

Inherent in this definition, a ReliabilityFirst Standard will define certain obligations or requirements of entities that own, operate, plan, and use the BPS within the ReliabilityFirst geographical footprint. These obligations or requirements as contained in the ReliabilityFirst Standards are to be measurable and consistent with Good Utility Practice. Standards are not to include processes or procedures that implement a Standard. In addition, obligations, requirements or procedures imposed upon ReliabilityFirst by NERC reliability standards are not to be ReliabilityFirst Standards, unless those obligations, requirements or procedures require the establishment of a “policy or standard” as defined by the ReliabilityFirst By-laws.

Characteristics of a Regional Reliability Standard

A Standard is policy, including adequacy criteria to provide for the reliable regional and sub-regional planning and operation of the BPS, consistent with Good Utility Practice

A Standard shall generally have the following characteristics:

- **Measurable** - A Standard shall establish technical or performance requirements that can be practically measured.
- **Relative to NERC Reliability Standards** - A Standard generally must go beyond, add detail to, or implement NERC Reliability Standards, or cover matters not addressed in NERC Reliability Standards.

Format Requirements of a Regional Reliability Standard

A Standard shall consist of the requirements shown in the Regional Reliability Standard Template. These requirements apply to the development and revision of Standards. These requirements are necessary to achieve Standards that are measurable, enforceable, and consistent. Supporting documents to aid in the implementation of a Standard may be referenced by the Standard but are not part of the Standard itself. The most current

version of the approved NERC Reliability Standard template and its associated elements posted on the NERC website will be used at the time of the development of a ReliabilityFirst Regional Reliability Standard if different from the elements listed below.

Regional Reliability Standard Format Requirement Template Example

Identification Number	A unique identification number assigned in accordance with an administrative classification system to facilitate tracking and reference ReliabilityFirst documentation.
Title	A brief, descriptive phrase identifying the topic of the Standard.
Applicability	Clear identification of the functional classes of entities responsible for complying with the Standard, noting any specific additions or exceptions. If not applicable to the entire ReliabilityFirst area, then a clear identification of the portion of the BPS to which the Standard applies. Any limitation on the applicability of the Standard based on electric facility requirements should be described.
Effective Date and Status	The effective date of the Standard <u>is the date of the FERC approval and the applicable implementation timeline.</u> ~~or, prior to approval of the Standard, the proposed effective date.~~
Purpose	The purpose of the Standard. The purpose shall explicitly state what outcome will be achieved or is expected by this Standard.
Requirement(s)	Explicitly stated technical, performance, and preparedness requirements. Each requirement identifies what entity is responsible and what action is to be performed or what outcome is to be achieved. Compliance is mandatory for each statement in the requirements section.

Risk Factor(s)	The potential reliability significance of each requirement, designated as a High, Medium, or Lower Risk Factor in accordance with the criteria listed below: A High Risk Factor requirement (a) is one that, if violated, could directly cause or contribute to BPS instability, separation, or a cascading sequence of failures, or could place the BPS at an unacceptable risk of instability, separation, or cascading failures; or (b) is a requirement in a planning timeframe that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly cause or contribute to BPS instability, separation, or a cascading sequence of failures, or could place the BPS at an unacceptable risk of instability, separation, or cascading failures, or could hinder restoration to abnormal condition. A Medium Risk Factor requirement (a) is a requirement that, if violated, could directly affect the electrical state or the capability of the BPS, or the ability to effectively monitor and control the BPS, but is unlikely to lead to BPS instability, separation, or cascading failures; or (b) is a requirement in a planning timeframe that, if violated, could, under emergency, abnormal, or restorative conditions anticipated by the preparations, directly affect the electrical state or capability of the BPS, or the ability to effectively monitor, control, or restore the BPS, but is unlikely, under emergency, abnormal, or restoration conditions anticipated by the preparations, to lead to BPS instability, separation, or cascading failures, nor to hinder restoration to a normal condition. A Lower Risk Factor requirement is administrative in nature and (a) is a requirement that, if violated, would not be expected to affect the electrical state or capability of the BPS, or the ability to effectively monitor and control the BPS; or (b) is a requirement in a planning time frame that, if violated, would not, under the emergency, abnormal, or restorative conditions anticipated by the preparations, be expected to affect the electrical state or capability of the BPS, or the ability to effectively monitor, control, or restore the BPS.
Measure(s)	Each requirement shall be addressed by one or more measurements that will be used to assess performance and outcomes for the purpose of determining compliance with the requirements stated above. Each measurement identifies to whom the measurement applies. Each measurement shall be tangible, and as objective as is practical. Achieving the full compliance level of each measurement is a necessary and sufficient indicator that the requirement was met.

Compliance Administration Elements

Compliance Monitoring Process	Defines for each measure: • The specific data or information that is required to measure performance or outcomes. • The entity that is responsible to provide the data or information for measuring performance or outcomes. • The process that will be used to evaluate information for the purpose of assessing performance or outcomes. • The entity that is responsible for evaluating information to assess performance or outcomes. • The time period in which performance or outcomes is measured, evaluated, and then reset. • Data retention requirements and assignment of responsibility for data archiving. • Violation severity levels.

Supporting Information Elements

Interpretations	Any ReliabilityFirst interpretations of the Standards that were developed, and approved in accordance with the “Interpretation of Standards” section of this Procedure, to expound on the application of the Standard for unusual or unique situations or provide clarifications.
Implementation Plan	Each ReliabilityFirst Standard shall have an associated implementation plan describing the effective date of the Standard or effective dates if there is a phased implementation. The implementation plan may also describe the implementation of the Standard in the compliance program and other considerations in the initial use of the Standard, such as necessary tools, training, etc. The implementation plan must be posted for at least one public comment period and be approved as part of the ballot of the standard.
Supporting References	This section references related documents that support reasons for, or provide additional information related to the Standard. Examples include, but are not limited to: • Glossary of Terms • Developmental history of the Standard and prior versions • Subcommittee(s) responsible for Standard • Notes pertaining to implementation or compliance • Standard references • Procedures/Practices • Training and/or Technical Reference

Roles in the Regional Reliability Standards Development Process

Process Roles

Originator - Any entity (person, organization, company, government agency, individual, etc.) that is directly and materially affected by the reliability of the ReliabilityFirst BPS, is allowed to request a Standard be developed or an existing Standard is modified, or deleted, by creating a Standards Authorization Request (SAR). See Appendix B.

Board – The ReliabilityFirst Board shall act on any proposed Standard that has gone through the process contained in this Procedure. Once the ReliabilityFirst Board approves a Standard, compliance with the Standard will be enforced consistent with the By-laws and the terms of the Standard.

Standards Committee (SC) - The ReliabilityFirst SC will consider which requests for new or revised Standards shall be assigned for development (or existing Standards

considered for deletion). The SC manages the Standards development process. The SC will advise the ReliabilityFirst Board on Standards presented for adoption by the ReliabilityFirst Board.

Standards Process Manager (SPM) – A person or persons on the ReliabilityFirst staff assigned the task of ensuring that the development, revision or deletion of Standards is in accordance with this Procedure. The SPM works to ensure the integrity of the process and consistency of quality and completeness of the Standards. The SPM facilitates the administration of all actions contained in all steps in the process.

Standards Process Staff – Employees of the ReliabilityFirst that work with or for the SPM.

Standard Drafting Team (SDT) – A team of technical experts, and typically including a member of the ReliabilityFirst Standards staff and the Originator, assigned the task of developing a proposed Standard based upon an approved SAR using the Standard development process contained in this Procedure.

Ballot Body (BB) – The Ballot Body comprises all entities that qualify for one or more of the categories and are registered with ReliabilityFirst as potential ballot participants in the voting on standards. The categories of registration within the Ballot Body and the registration process are described in Appendix D.

Ballot Pool – The Ballot Pool is comprised of those members of the Ballot Body that register to vote for each particular standard. A separate Ballot Pool is established for each standard up for vote. Only individuals who have joined the Ballot Pool for that particular standard are eligible to vote on a standard.

Reliability Committee (RC) – The ReliabilityFirst RC serves as a technical advisory body to address the reliability related activities required by the Reliability Standards via review and discussion of the regional activities as requested by the SC.

Regional Reliability Standard Development Process (Flow chart of Process shown in Appendix C)

Assumptions and Prerequisites

The ReliabilityFirst Regional Reliability Standards Development Process has the following characteristics:

- **Fair due process** - The ReliabilityFirst standards development process shall provide for reasonable notice and opportunity for public comment. At a minimum, the procedure shall include public notice of the intent to develop a standard, a public comment period on the

proposed standard, due consideration of those public comments, and a ballot of interested stakeholders.

- **Openness** - Participation is open to all Organizations who are directly and materially affected by the ReliabilityFirst region BPS reliability. There shall be no undue financial barriers to participation. Participation shall not be conditioned upon membership in the ReliabilityFirst, and shall not be unreasonably restricted on the basis of technical qualifications or other such requirements. Meetings of SDTs are open to the ReliabilityFirst membership and to others.
- **Balanced** - The ReliabilityFirst standards development process strives to have an appropriate balance of interests and shall not be dominated by any two interest categories and no single interest category shall be able to defeat a matter.
- **Inclusive** - Any entity (person, organization, company, government agency, individual, etc.) with a direct and material interest in the BPS in the ReliabilityFirst area shall have a right to participate by: a) expressing a position and its basis, b) having that position considered, and c) having the right to appeal.
- **Transparent** - All actions material to the development of ReliabilityFirst Standards shall be transparent. All standards development meetings shall be open and publicly noticed on ReliabilityFirst's Web site.
- Does not unnecessarily delay development of the proposed Standard.

Note: The term “days” refers to calendar days.

Each standard shall enable or support one or more of the reliability principles, thereby ensuring that each standard serves a purpose in support of the reliability of the regional BPS. Each standard shall also be consistent with all of the reliability principles, thereby ensuring that no standard undermines reliability through an unintended consequence.

While ReliabilityFirst Standards are intended to promote reliability, they must at the same time accommodate competitive electricity markets. Reliability is a necessity for electricity markets, and robust electricity markets can support reliability. Recognizing that BPS reliability and electricity markets are inseparable and mutually interdependent, all ReliabilityFirst Standards shall be consistent with NERC's market interface principles. Consideration of the market interface principles is intended to ensure that standards are written such that they achieve their reliability objective without causing undue restrictions or adverse impacts on competitive electricity markets.

ReliabilityFirst will coordinate with NERC such that the acknowledgement of receipt of a standard request identified in step 1, notice of comment posting period identified in step 4, and notice for vote identified in step 5 below are concurrently posted on both the ReliabilityFirst and NERC websites.

Step 1 - Development of a Standards Authorization Request (SAR) to Develop, Revise or Delete a Regional Reliability Standard

Any individual representing an organization (Originator) which is directly or materially impacted by the operation of the BPS within the geographical footprint of the ReliabilityFirst may request, via a submittal of a Standard Authorization Request (SAR) form, the development, modification, or deletion of a ReliabilityFirst Standard. Any such request shall be submitted to the ReliabilityFirst SPM, or his/her designee, or by another process as otherwise posted on the ReliabilityFirst website. The SAR form may be downloaded from the ReliabilityFirst website.

The SAR contains a description of the proposed Standard subject matter containing sufficiently descriptive detail to clearly define the purpose, scope, impacted parties, and other relevant information of the proposed Standard. The SPM will verify that the submitted SAR form has been adequately completed. The SPM may offer the Originator suggestions regarding changes and/or improvements to improve clarity and assist the ReliabilityFirst community to understand the Originator's intent and objectives. The Originator is free to accept or reject these suggestions. Within 15 days the SPM will electronically acknowledge receipt of the SAR.

The SPM will forward the adequately complete SAR to the ReliabilityFirst SC, at which time, the SC will, post the SAR for comments within 15 days, SARs will be posted and publicly noticed.

Comments on the SARs will be accepted for a 30-day period from the notice of posting. Comments will be accepted online using an internet-based application. The SPM will provide a copy of the comments to the Originator and the SC.

Based on the comments, the SC shall make available a consideration of comments report and determine the disposition of the SAR (within 60 calendar days following the SAR commenting period). The disposition decision and decision process shall use the normal "business rules and procedures" of the SC then in effect. The SC may take one of the following actions³ in accordance with the ReliabilityFirst Standards Committee Governance document:

- Accept the SAR as a candidate for: development of a new Standard, revision of an existing Standard or deletion of an existing Standard. The SC may, in its sole discretion, expand or narrow the scope of the SAR under consideration. The SC

³Actions by the Standards Committee may be appealed per the Appeals process in Appendix A

shall prioritize the development of SARs as may be required based on the number of SARs under development at any time.

- Reject the SAR. If the SC rejects a SAR, a written explanation for rejection will be delivered to the Originator within 30 days of the decision.
- Remand the SAR back to the Originator for redirection to the NERC process. In cases where there is a Reliability need identified in the SAR but it does not meet the criteria for Regional standards (more stringent reliability requirements than the NERC reliability standard or cover matters not covered by an existing NERC reliability standard), the Standards Committee will assist the Originator in submitting the SAR to NERC.
- Remand the SAR back to the Originator for additional work. The SPM will make reasonable efforts to assist the Originator in addressing the deficiencies identified by the SC. The Originator may then resubmit the modified SAR using the process above. The Originator may choose to withdraw the SAR from further consideration prior to re-submittal to the SC

Any SAR that is accepted by the SC for development of a Standard (or modification or deletion of an existing Standard) shall be posted for public viewing on the ReliabilityFirst website within 30 days of acceptance by the SC. The status of posted SARs will be publicly posted.

Any documentation of the deliberations of the SC concerning SARs shall be made available according to the “ReliabilityFirst Standards Committee Governance” document then in effect.

The SC shall submit a written report to the ReliabilityFirst Board on a periodic basis (at least at every regularly scheduled ReliabilityFirst Board meeting) showing the status of all SARs that have been brought to the SC for consideration.

Step 2 – *Formation of the Standard Drafting Team and Declaration of Milestone Date*

Upon acceptance by the SC of a SAR for development of a new Standard (or modification or deletion of an existing Standard), the SC shall direct the SPM to develop a qualified balance slate for the SDT using the specific directions and preferences of the SC. The SPM will send out self-nomination forms to solicit SDT nominees. The SDT will consist of a group of people (members of ReliabilityFirst and, as appropriate, non-members) who collectively have the necessary technical expertise and work process skills. The SPM will recommend a slate of ad-hoc individuals or a preexisting task force, work group or similar for the SDT based upon the SC’s desired SDT capabilities.

The SC may also direct the SPM to designate an existing ReliabilityFirst committee (or subset thereof) as the SDT augmented by other persons as may be appropriate for the

subject matter. The SC will insure that SDT membership includes all necessary administrative support. This support typically includes a ReliabilityFirst staff member and the Originator if he/she chooses to participate. The SC appoints the interim chair (should not be a staff person) of the SDT. The SDT will elect the permanent Chair and Vice-chair at its first meeting.

The SPM submits the proposed list of names of the SDT to the SC. The SC will either accept the recommendations of the SPM or modify the SDT slate, as it deems appropriate within 60 days of accepting a SAR for development.

Upon approval of the SDT slate, the SC will declare a preliminary date on which the SDT is expected to have ready a completed draft Standard and associated supporting documentation available for consideration by the ReliabilityFirst membership.

Step 3 – Work and Work Product of the Standard Drafting Team

The SDT will then develop a work plan for completing the Standard development work, including the establishment of milestones for completing critical elements of the work in sufficient detail to ensure that the SDT will meet the deadline established by the SC or the SDT shall propose an alternative date. This plan is then delivered to the SC for its concurrence.

The SDT is to meet, either in person or via electronic means as necessary, establish sub-work teams (made up of members of the SDT) as necessary, and performs other activities to address the parameters of the SAR and the milestone date(s) established by the SC.

The work product of the SDT will consist of the following:

- A draft Standard consistent with the SAR on which it was based.
- An assessment of the impact of the SAR on neighboring regions, and appropriate input from the neighboring regions if the SAR is determined to impact any neighboring region.
- An implementation plan, including the nature, extent and duration of field-testing, if any.
- Identification of any existing Standard that will be deleted, in part or whole, or otherwise impacted by the implementation of the draft Standard.
- Technical reports, white papers and/or work papers that provide technical support for the draft Standard under consideration.
- Document the perceived reliability impact should the Standard be approved.

Upon completion of these tasks, the SDT submits these documents to the SC, which will verify that the proposed Standard is consistent with the SAR on which it was developed

The SDT regularly (at least once each month) informs the SC of its progress in meeting a timely completion of the draft Standard. The SDT may request of the SC scope changes of the SAR at any point in the Standard development process.

The SC may, at any time, exercise its authority over the Standards development process by directing the SDT to move to Step 4 and post for comment the current work product. If there are competing drafts, the SC may, at its sole discretion, post the version(s) of the draft Standard for comment on the ReliabilityFirst website. The SC may take this step at any time after a SDT has been commissioned to develop the Standard.

Step 4 – *Comment Posting Period*

At the direction from the SC, the SPM then facilitates the posting of the draft Standard on the ReliabilityFirst website, along with a draft implementation plan and supporting documents, for a 30-day comment period. The SPM shall also inform ReliabilityFirst Members and other potentially interested entities inside or outside of ReliabilityFirst of the posting using typical membership communication procedures then currently in effect or by other means as deemed appropriate. As early as the start of the first posting for comment, entities may join the Ballot Pool established for the eventual voting on the proposed standard. The Ballot Pool category description and associated requirements are in Appendix D.

Within 30 days of the conclusion of 30-day comment posting period the SDT shall convene and consider changes to the draft Standard, the implementation plan and/or supporting technical documents based upon comments received. Based upon these comments, the SDT may elect to return to step 3 to revise the draft Standard, implementation plan and/or supporting technical documentation.

The SDT shall prepare a “modification report” summarizing the comments received and the changes made as a result of these comments. The modification report also summarizes comments that were rejected by the SDT and the reason(s) that these comments were rejected, in part or whole. Responses to all comments will be posted on the ReliabilityFirst website no later than the next posting of the proposed Standard.

Step 5 – *Posting for Voting by ReliabilityFirst Registered Ballot Body*

Upon recommendation of the SDT, and if the SC concurs that all of the requirements for development of the Standard have been met, the SPM will post the revised draft Standard, implementation plan, supporting technical documentation and the “modification report”. Once the notice for a vote has been issued, no substantive modifications may be made to the proposed standard unless the revisions are posted and a new notice of the vote is issued.

Entities may register in the BB at any time during the Standards process. The BB category description and associated rules are in Appendix D.

By 11:59 PM Central Prevailing Time (CPT) of the seventh day of the 15 day pre-ballot posting period, registered BB members intending to vote on the proposed standard must have joined the Ballot Pool established for the eventual voting on the proposed standard being posted. The SPM will schedule a Vote by the Ballot Pool which is to be scheduled to commence no sooner than 15 days and no later than 30 days following this posting. The Vote by the Ballot Pool is an advisory to the ReliabilityFirst Board.

The Ballot Pool shall be allowed to vote over a period of 15 days. Votes will be submitted electronically, but may be submitted through other means as approved by the SC.

All BB members are eligible to participate in voting on proposed new Standards, Standard revisions or Standard deletions. There is a requirement to join a Ballot Pool to participate in voting for each standard.

The voting results will be composed of only the votes from BB entities that have joined the Ballot Pool for the standard being voted on and responding within the voting period. Votes may be accompanied by comments explaining the vote, but are not required. All comments shall be responded to and posted to the ReliabilityFirst website prior to going to the SC or Board.

Step 6A – Voting Receives Two-Thirds or Greater Majority of Affirmative Category Votes

A two-thirds or greater majority⁴ of votes within a category determines the vote for that category. The Initial ballot has passed if there is a two-thirds or greater affirmative majority of category votes (only those categories with votes cast will be considered) during the 15-day voting period and a quorum⁵ is met.

If there is at least one (1) Negative vote with comment during the initial ballot, then the standard will be posted for a 10-day Recirculation ballot. If there are no Negative votes with comments, the SC will forward the Standard to the ReliabilityFirst Board for action (Step 7). In the recirculation ballot, members of the Ballot Pool shall again be presented the proposed standard (that has not been significantly changed from the previous ballot) along with the reasons for negative votes, the responses, and any resolution of the differences. An insignificant revision is a revision that does not change the scope, applicability, or intent of any requirement and includes but is not limited to things such as correcting the numbering of a requirement, correcting the spelling of a word, adding an obviously missing word, or rephrasing a requirement for improved clarity. Where there is a question as to whether a proposed modification is “substantive” the Standards Committee shall make the final determination. All members of the Ballot Pool shall be permitted to reconsider and change their vote from the prior ballot. Members of the Ballot Pool who did not respond to the prior ballot shall be permitted to vote in the

⁴ For the purposes of determining majority within a category, an abstention is not considered a vote.

⁵ A quorum is achieved when three-fourths (75%) or greater of the ballot pool casts a vote.

recirculation ballot. In the recirculation ballot, Ballot Pool members may indicate a revision to their original vote otherwise their vote shall remain the same as in their prior ballot.

Upon successful completion of the initial and recirculation voting periods, the SC will forward the Standard to the ReliabilityFirst Board for action (Step 7).

Step 6B – Voting Does Not Receive Two-Thirds or Greater Majority of Affirmative Category Votes or a Quorum⁵ is Not Met

If a draft Standard does not receive a two-thirds or greater affirmative majority of votes determined for each category (only those categories with votes cast will be considered) or does not reach quorum during the 15-day Initial voting period, the SC may:

- Direct the SDT to respond to ballot comments and post the standard for a 10-day Recirculation ballot (as discussed in Step 6A) to determine if the response to comments alleviates reasons for the Negative initial ballots.
- Direct the existing SDT to reconsider or modify certain aspects of the draft Standard and/or implementation plan. The resulting draft Standard and/or implementation plan will be posted for a second initial voting period. The SC may require a second comment period prior to the second voting period. The second posting of the draft Standard, implementation plan, and supporting documentation shall be within 60 days of the SC action.
 - If there is a two-thirds or greater affirmative majority of categories with votes cast and a quorum is met during the second initial ballot and second recirculation ballot, the SC will forward it to the ReliabilityFirst Board for action (Step 7).
 - If a draft Standard does not receive a two-thirds or greater majority of affirmative category votes cast during the second initial ballot or a quorum is not met, the SC will refer the draft Standard and implementation plan to the ReliabilityFirst Board. The SC may also submit an assessment, opinion and recommendations to the ReliabilityFirst Board (Step 7).
- Revise the SAR on which the draft Standard was based and remand the development work back to the original SDT or a newly appointed SDT. The resulting draft Standard and/or implementation plan will be posted for a second voting period. The SC may require a second comment period prior to a second voting period. The second posting of the draft Standard, implementation plan, and supporting documentation shall be within 60 days of the SC action.
 - If there is a two-thirds or greater affirmative majority of categories with votes cast and a quorum is met during the second initial ballot and second

recirculation ballot, the SC will forward it to the ReliabilityFirst Board for action (Step 7).

- If a draft Standard does not receive a two-thirds or greater majority of affirmative category votes cast during the second voting period or a quorum is not met, the SC will refer the draft Standard and implementation plan to the ReliabilityFirst Board. The SC may also submit an assessment, opinion and recommendations to the ReliabilityFirst Board (Step 7).
- Recommend termination of all work on the development of the Standard action under consideration and so notify the ReliabilityFirst Board.

Step 7 – Action by the ReliabilityFirst Board

A draft Standard submitted to the ReliabilityFirst Board for action must be publicly posted at least 30 days prior to action by the Board. At a regular or special meeting, the ReliabilityFirst Board shall consider adoption of the draft Standard. The Board will consider the results of the voting and dissenting opinions. The Board will consider any advice offered by the SC.

Draft Standards that received a two-thirds or greater of categories with votes cast shall be delivered to the ReliabilityFirst Board for their action. The ReliabilityFirst Board shall be provided with an “informational package” which includes:

- The draft Standard and any modification or deletion of other related existing Standard(s)
- Implementation Plan (including recommending field testing and effective dates)
- Technical Documentation supporting the draft Standard
- A summary of the vote and summary of the comments and responses that accompanied the votes.

The ReliabilityFirst Board is expected to either:

- Approve the draft Standard action with only minor or no modification. Under no circumstances may the Board substantively modify the proposed regional reliability standard.
- Remand to the SC with comments and instructions, or
- Disapprove the draft Standard action without recourse.

Draft Standards that did not receive a two-thirds or greater of categories with votes cast in the second voting period shall be delivered to the ReliabilityFirst Board for their action. The ReliabilityFirst Board shall be provided with an “informational package”.

The ReliabilityFirst Board is expected to either:

- Approve the draft Standard action with only minor or no modification. Under no circumstances may the Board substantively modify the proposed regional reliability standard.
- Remand to the SC with comments and instructions, or
- Disapprove the draft Standard action without recourse.

Once a regional ReliabilityFirst Standard is approved by the Board, the standard will be submitted to NERC for approval and filing with FERC.

Step 8 - Implementation of a Regional Reliability Standard

Upon approval of a draft Standard action by the FERC, the SPM will notify the membership and applicable entities within the ReliabilityFirst footprint upon ReliabilityFirst Board approval of the standard of the effective date through the normal and customary membership communication procedures and processes then in effect. The SPM will also notify the ReliabilityFirst Compliance Staff for integration into the ReliabilityFirst Compliance Program.

~~The approval date of each ReliabilityFirst standard is upon Board approval. The effective date will depend on the implementation plan that is provided with each new or revised standard. The ReliabilityFirst standard is mandatory and enforceable (without monetary penalties for non-compliance) upon the effective date after ReliabilityFirst Board approval for applicable entities that are members of ReliabilityFirst.³~~

~~ReliabilityFirst standards shall be subject to approval by NERC, as the electric reliability organization, and by the Federal Energy Regulatory Commission (FERC) before becoming mandatory and enforceable under Section 215 of the FPA. Upon approval of a ReliabilityFirst standard action by FERC, it is mandatory and enforceable (with monetary penalties for non-compliance) to all applicable entities within the ReliabilityFirst footprint. The effective date for non-members upon the FERC approval will be determined by the implementation plan that is provided with each new or revised standard.~~

³ ~~By applying for and becoming a Regular or Associate Member of the Corporation, each Member agrees to comply with all Reliability Standards, all NERC standards and requirements, and the other obligations of Members of the Corporation set forth in the ReliabilityFirst Bylaws or duly adopted by the Board in order to achieve the purposes of the Corporation.~~

Appendix A

Maintenance of Regional Reliability Standards Development Process

Significant changes to this Procedure shall begin with the preparation of a SAR and be handled using the same procedure as a request to add, modify, or delete a Standard.

The ReliabilityFirst SC has the authority to make ‘minor’ changes to this Procedure as deemed appropriate by the SC and subject to the SC voting practices and procedures according to the “ReliabilityFirst Standards Committee Governance” document. The SC shall promptly notify the ReliabilityFirst Board of such ‘minor’ changes to this Procedure for their review and concurrence at the next ReliabilityFirst Board meeting.

Maintenance of Regional Reliability Standards

The SC shall ensure that each Standard shall be reviewed at least once every five years from the effective date of the Standard or the latest revision to the Standard, whichever is the later. The review process shall be conducted by soliciting comments from the stakeholders. If no changes are warranted, the SC shall recommend to the ReliabilityFirst Board that the Standard be reaffirmed. If the review indicates a need to revise or delete a Standard, a SAR shall be prepared and submitted in accordance with the standards development process contained in this Procedure.

Urgent Action

Under certain conditions, the SC may designate a proposed Standard or revision to a Standard as requiring urgent action. Urgent action may be appropriate when a delay in implementing a proposed Standard or revision could materially impact reliability of the BPS. The SC must use its judgment carefully to ensure an urgent action is truly necessary and not simply an expedient way to change or implement a Standard.

A requester prepares a SAR and a draft of the proposed Standard and submits both to the SPM. The SAR must include a justification for urgent action. The SPM submits the request to the SC for its consideration. If the SC designates the requested Standard or revision as an urgent action item, then the SPM shall immediately post the draft for pre-ballot review. This posting requires a minimum 30-day posting period before the ballot and applies the same voting procedure as detailed in Step 5. Processing will continue as outlined in the subsequent steps. In the event additional drafting is required, a SDT will be assembled as outlined in the Procedure.

Any Standard approved as an urgent action shall have a termination date specified that shall not exceed one year from the approval date. Should there be a need to make the Standard permanent, then the Standard would be required to go through the full Standard

development process. All urgent action Standards require ReliabilityFirst Board, NERC and FERC approval, as outlined for Standards in the regular process.

Urgent actions that expire may be renewed using the urgent action process again, in the event a permanent Standard is not adopted. In determining whether to authorize an urgent action Standard for a renewal ballot, the SC shall consider the impact of the Standard on the reliability of the BPS and whether expeditious progress is being made toward a permanent replacement Standard. The SC shall not authorize a renewal ballot if there is insufficient progress toward adopting a permanent replacement Standard or if the SC lacks confidence that a reasonable completion date is achievable. The intent is to ensure that an urgent action Standard does not in effect take on a degree of permanence due to the lack of an expeditious effort to develop a permanent replacement Standard. With these principles, there is no predetermined limit on the number of times an urgent action may be renewed. However, each urgent action Standard renewal shall be effective only upon approval by the ReliabilityFirst Board, NERC and FERC.

Any person or entity, including the SDT working on a permanent replacement Standard, may at any time submit a SAR proposing that an urgent action Standard become a permanent Standard by following the full Standards process.

Interpretations of Standards

All persons who are directly and materially affected by the reliability of ReliabilityFirst BPS shall be permitted to request an interpretation of the standard. The person requesting an interpretation will send a request to the SPM explaining the specific circumstances surrounding the request and what clarifications are required as applied to those circumstances. The request should indicate the material impact to the requesting party or others caused by the lack of clarity or a possibly incorrect interpretation of the standard.

The SPM, along with guidance from the SC, will assemble a team with the relevant expertise to address the request. The Interpretation Drafting Team (IDT) typically consists of members from the original SDT. The SPM submits the proposed list of names of the IDT to the SC. The SC will either accept the recommendations of the SPM or modify the IDT slate.

As soon as practical (not more than 45 days), the team will prepare an initial draft interpretation of the standard addressing the issues raised. Once the IDT has completed the initial draft interpretation, the team will post the draft for a 30-day informal⁶ stakeholder comment period. The IDT will review the stakeholder feedback and may make changes before preparing a final draft of the interpretation. The IDT will then

⁶ An informal comment period does not require the IDT to respond to every stakeholder comment and is only used to make potential changes for the final draft of the interpretation.

forward the draft interpretation to the SPM. The SPM will forward the interpretation to the Reliability Committee (RC). Barring receipt of an opinion from the RC within 21 calendar days, that the interpretation is not technically appropriate for the Standard, respectively, the SPM will forward the interpretation to the SC. The SC will determine if the interpretation is consistent with the Standard and does not add additional requirements to the standard. The SC will forward the interpretation to the ReliabilityFirst Board for informational purposes as being appended to the approved Standard.

Note: In the event that the RC determines that the interpretation makes the standard technically inappropriate the RC shall provide an explanation of its reasoning to the SPM and IDT for inclusion in a subsequent revision. In either case, the IDT and SPM will continue to re-circulate the interpretation as stated above.

The interpretation will stand until such time as the standard is revised through the normal process, at which time the standard will be modified to incorporate the clarifications provided by the interpretation.

Appeals

Persons who have directly and materially affected interests and who have been or will be adversely affected by any substantive or procedural action or inaction related to the development, approval, revision, reaffirmation, or withdrawal of a Standard shall have the right to appeal. This appeals process applies only to the Standards process as defined in this Procedure.

The burden of proof to show adverse effect shall be on the appellant. Appeals shall be made within 30 days of the date of the action purported to cause the adverse effect, except appeals for inaction, which may be made at any time. In all cases, the request for appeal must be made prior to the next step in the process.

The final decisions of any appeal shall be documented in writing and made public.

The appeals process has two levels, with the goal of expeditiously resolving the issue to the satisfaction of the participants:

Level 1 Appeal

Level 1 is the required first step in the appeals process. The appellant submits a complaint in writing to the SPM that describes the substantive or procedural action or inaction associated with a Standard or the standards process. The appellant describes in the complaint the actual or potential adverse impact to the appellant. Assisted by any necessary staff and committee resources, the SPM shall prepare a written response addressed to the appellant as soon as practical but not more than 45-days after receipt of the complaint. If the appellant accepts the response as a satisfactory resolution of the

issue, both the complaint and response will be made a part of the public record associated with the standard.

Level 2 Appeal

If after the Level 1 Appeal the appellant remains unsatisfied with the resolution, as indicated by the appellant in writing to the SPM, the SPM shall convene a Level 2 Appeals Panel. This panel shall consist of five members total appointed by the ReliabilityFirst Board.

In all cases, Level 2 Appeals Panel members shall have no direct affiliation with the participants in the appeal.

The SPM shall post the complaint and other relevant materials and provide at least 30-days notice of the meeting of the Level 2 Appeals Panel. In addition to the appellant, any person that is directly and materially affected by the substantive or procedural action or inaction referenced in the complaint shall be heard by the panel. The panel shall not consider any expansion of the scope of the appeal that was not presented in the Level 1 Appeal. The panel may in its decision find for the appellant and remand the issue to the SC with a statement of the issues and facts in regard to which fair and equitable action was not taken. The panel may find against the appellant with a specific statement of the facts that demonstrate fair and equitable treatment of the appellant and the appellant's objections. The panel may not, however, revise, approve, disapprove, or adopt a reliability standard. The actions of the Level 2 Appeals Panel shall be publicly posted.

In addition to the foregoing, a procedural objection that has not been resolved may be submitted to the ReliabilityFirst Board for consideration at the time the Board decides whether to adopt a particular reliability standard. The objection must be in writing, signed by an officer of the objecting entity, and contain a concise statement of the relief requested and a clear demonstration of the facts that justify that relief. The objection must be filed no later than 30-days after the announcement of the vote on the Standard in question.

Appendix B

Standard Authorization Request

The SC shall be responsible for implementing and maintaining this form as needed to support the information requirements of the standards development process in this Procedure. Changes to this form are considered minor, and therefore subject to only the approval of the SC.

ReliabilityFirst Standard Authorization Request Form

**ReliabilityFirst
will complete**

Title of Proposed Standard
Request Date

ID
Authorized for Posting
Authorized for Development

SAR Originator Information

Name	SAR Type (Check box for one of these selections.)	
Company	☐	New Standard
Telephone	☐	Revision to Existing Standard
Fax	☐	Withdrawal of Existing Standard
E-mail	☐	Urgent Action

Purpose (Provide one or two sentences.)

Industry Need (Provide one or two sentences.)

Brief Description (A few sentences or a paragraph.)

Reliability Functions

The Standard will Apply to the Following Functions (Check box for each one that applies.)

	Reliability Authority	Ensures the reliability of the bulk transmission system within its Reliability Authority area. This is the highest reliability authority.
	Balancing Authority	Integrates resource plans ahead of time, and maintains load-interchange-resource balance within its metered boundary and supports system frequency in real time
	Generator Owner	Owns and maintains generating units
	Interchange Authority	Authorizes valid and balanced Interchange Schedules
	Planning Authority	Plans the BPS
	Resource Planner	Develops a long-term (generally one year and beyond) plan for the resource adequacy of specific loads (customer demand and energy requirements) within a Planning Authority Area
	Transmission Planner	Develops a long-term (generally one year and beyond) plan for the reliability (adequacy) of the interconnected bulk electric transmission systems within its portion of the Planning Authority Area
	Transmission Service Provider	Provides transmission services to qualified market participants under applicable transmission service agreements
	Transmission Owner	Owns transmission facilities
	Transmission Operator	Operates and maintains the transmission facilities, and executes switching orders
	Distribution Provider	Provides and operates the “wires” between the transmission system and the customer

	Generator Operator	Operates generating unit(s) and performs the functions of supplying energy and Interconnected Operations Services
	Purchasing-Selling Entity	The function of purchasing or selling energy, capacity and all necessary Interconnected Operations Services as required
	Load-Serving Entity	Secures energy and transmission (and related generation services) to serve the end user
	Market Operator	Integrates energy, capacity, balancing, and transmission resources to achieve an economic, reliability-constrained dispatch of resources. The dispatch may be either cost-based or bid-based
	Regional Reliability Organizations	An entity that ensures that a defined area of the BPS is reliable, adequate and secure. A member of the North American Electric Reliability Council. The Regional Reliability Organization can serve as the Compliance Monitor

NOTE: The SDT may find it necessary to modify the initial reliability function responsibility assignment as a result of the standards development and comments received.

Reliability Principles

<i>Applicable Reliability Principles (Check box for all that apply.)</i>	
	1. Interconnected BPS shall be planned and operated in a coordinated manner to perform reliably under normal and abnormal conditions as defined in the NERC Standards.
	2. The frequency and voltage of interconnected BPS shall be controlled within defined limits through the balancing of real and reactive power supply and demand.
	3. Information necessary for the planning and operation of interconnected BPS shall be made available to those entities responsible for planning and operating the systems reliably.
	4. Plans for emergency operation and system restoration of interconnected BPS shall be developed, coordinated, maintained, and implemented.
	5. Facilities for communication, monitoring, and control shall be provided, used, and maintained for the reliability of interconnected BPS.
	6. Personnel responsible for planning and operating interconnected BPS shall be trained, qualified, and have the responsibility and authority to implement actions.
	7. The security of the interconnected BPS shall be assessed, monitored, and maintained on a wide-area basis.

Market Interface Principles

<i>Does the proposed Standard comply with all of the following Market Interface Principles?</i>	
Recognizing that reliability is an essential requirement of a robust North American economy:	
yes or no	1. A reliability standard shall not give any market participant an unfair competitive advantage.
yes or no	2. A reliability standard shall neither mandate nor prohibit any specific market structure.
yes or no	3. A reliability standard shall not preclude market solutions to achieving compliance with that standard.
yes or no	4. A reliability standard shall not require the public disclosure of commercially sensitive information. All market participants shall have equal opportunity to access commercially non-sensitive information that is required for compliance with reliability standards.

Detailed Description (Provide enough detail so that an independent entity familiar with the industry could draft a Standard based on this description.)

Related Standards (NERC and Regional)

Standard No.	Explanation

Related SARs

SAR ID	Explanation

Implementation Plan

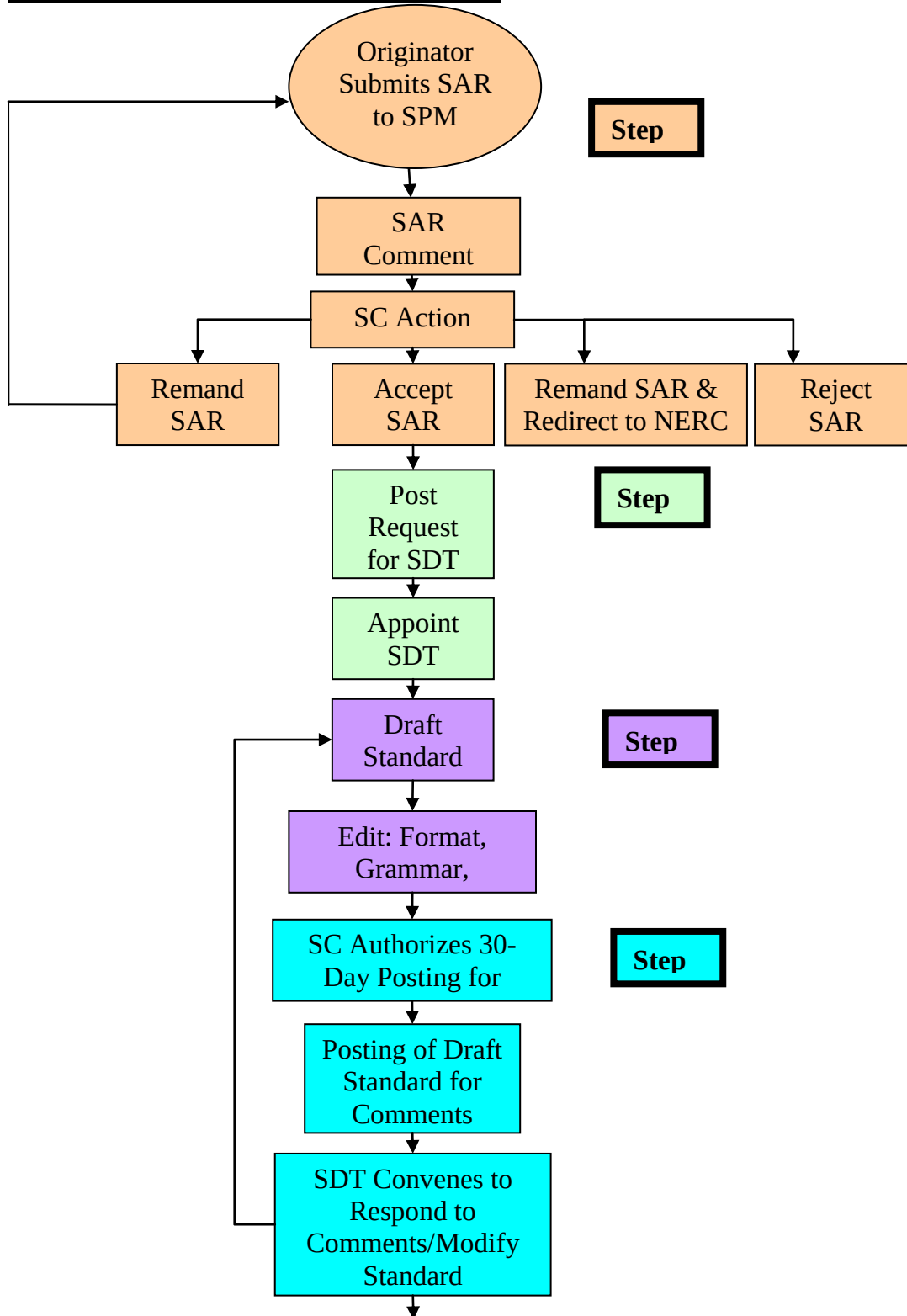
Description <i>(Provide plans for the implementation of the proposed standard, including any known systems or training requirements. Include the reliability risk(s) associated with the violation that the standard will mitigate, and the costs associated with implementation.)</i>
Proposed Implementation days after Board adoption or on (date):

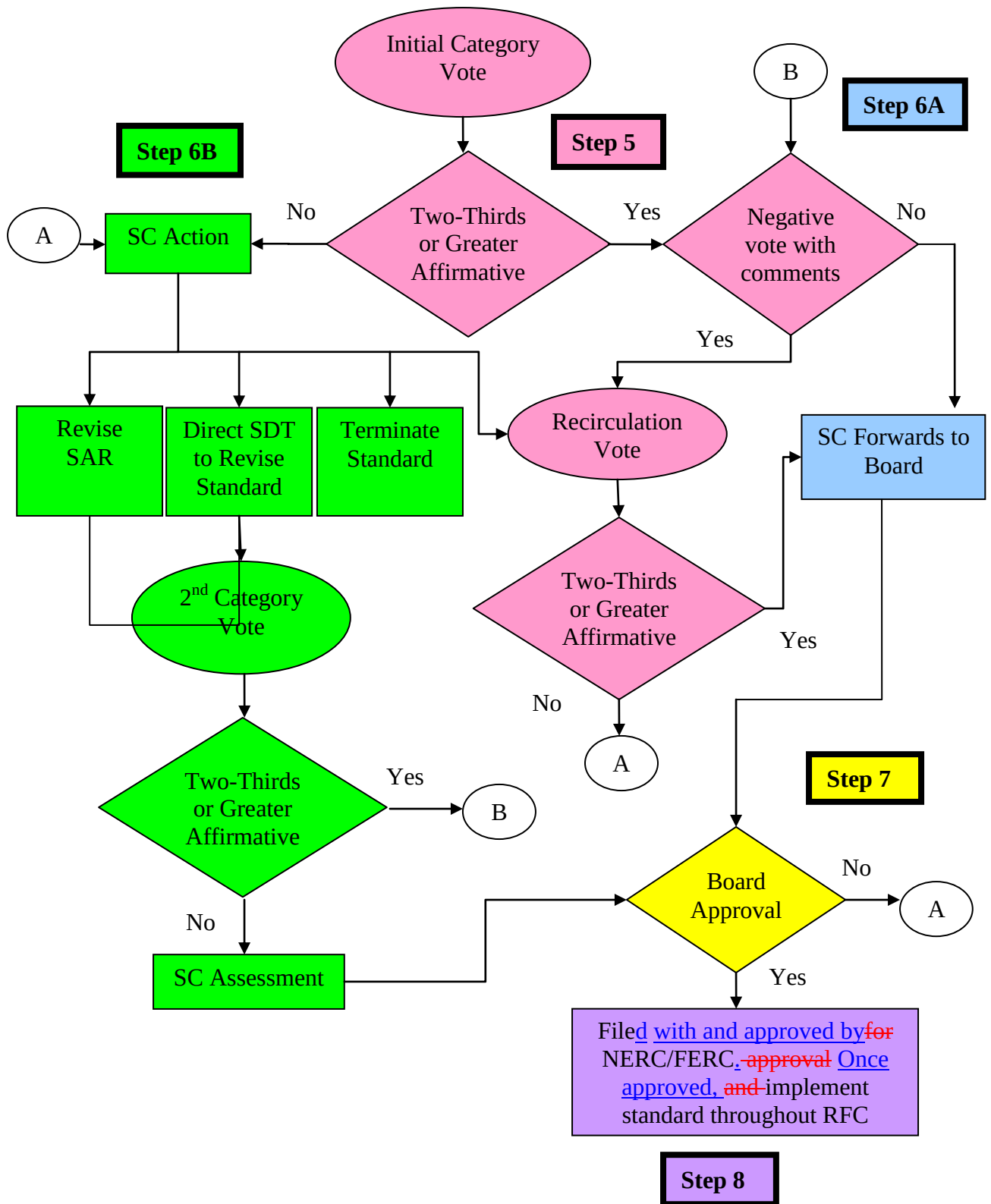
Assignments

	<i>Assignment</i>
Team Members	
ReliabilityFirst Staff	

Appendix C

Flowchart for Standards Process





Appendix D

Ballot Pool Categories

For the purposes of category Ballot Pool registration and voting, a person or entity may join the registered Ballot Pool to vote on standards, whether or not such person or entity is a member of ReliabilityFirst.

A corporation or other organization with integrated operations or with affiliates that qualifies to belong to more than one category (e.g., Transmission Owners and Load Serving Entities) may join and vote once in each category for which it qualifies, provided that each category constitutes a separate membership in the Ballot Body and the organization is represented in each category by a different representative. Affiliated entities are collectively limited to one membership in each category in the Ballot Pool for which they are qualified.

Category 1 – Transmission Owner, Transmission Operator, Transmission Service Provider

Category 2 – Generator Owner, Generator Operator

Category 3 – Load Serving Entity, Purchasing and Selling Entity, End User

Category 4 – Reliability Coordinator, Planning Coordinator, Transmission Planner, Resource Planner, Regional Transmission Organization, Balancing Authority, regulatory or governmental agency

Category 5 – Distribution Provider

Ballot Body Registration

Entities may register in the BB at any time during the Standards process. The SPM shall review all applications for joining the BB, and make a determination of whether they qualify for the self-selection category. In order to comment or vote you must have an active membership in the BB. When you submit your registration request to join the BB, you are placed in a “pending stage” until your account is activated. Activation of your account may take up to 24 hours. You will be unable to submit comments or join a Ballot Pool until your account is activated. The contact designated as primary representative to ReliabilityFirst is the voting member with the secondary contact as the backup.

Note: Registration for a BB is not the same as registration for the compliance registry. Although the terminology used to describe the BB categories in most cases has the same

meaning as the terms used in the NERC Functional Model, registration in a BB goes beyond the compliance registry in that entities smaller than those stated in the compliance registry guidelines are allowed to register in a BB. Entities shall have evidence that they qualify for the BB category they register in. Such evidence shall be available for the SPM review to verify BB registration and may include compliance registration.

Ballot Pool Formation

In order to participate in voting on a particular standard, an entity must join the Ballot Pool being established for the standard as follows:

- 1 – As early as the start of the first posting for comment, entities may join the Ballot Pool established for the eventual voting on the proposed standard being posted.
- 2 - By close of business of the seventh day of the 15 day pre ballot posting period, entities wishing to vote must have joined the Ballot Pool established for the eventual voting on the proposed standard being posted.



SUPPLEMENTAL MEMORANDUM

AMENDMENTS TO BYLAWS OF THE CORPORATION AND CERTIFICATE OF INCORPORATION

The following is a listing of proposed amendments to the Bylaws and corresponding changes in the Certificate of Incorporation of ReliabilityFirst for consideration. The proposed amendments are grouped by: (1) changes relating to Regional Reliability Standards; (2) changes relating to Member action, and (3) changes relating to Directors. References to changes in the Bylaws and/or the Certificate of Incorporation are shown in the left column.

1. Changes Relating to Regional Reliability Standards

Bylaws or Certificate of Incorporation Section Amended	Proposed Amendment	Issue
Section 1.24 of the Bylaws and ARTICLE FIFTH, Paragraph A of the Certificate of Incorporation	“Regional Reliability Standard” shall mean a type of Reliability Standard that is applicable only within a particular Regional Entity or group of Regional Entities. A Regional Reliability Standard may augment, add detail to, or implement another Reliability Standard or cover matters not addressed by other Reliability Standards. <u>A Regional Reliability Standard is not binding upon any Member or Registered Entity, nor is it effective or enforceable, until the Regional Reliability Standard Regional Reliability Standards, upon has been adopted adoption</u> by NERC and <u>approved by approval</u> the Commission, <u>shall be as a</u> Reliability Standard <u>s and shall be enforced</u> within the applicable Regional Entity or Regional Entities pursuant to delegated authorities.	This change is to clarify that Regional Reliability Standards are binding and enforceable on Members and Registered Entities only after they are adopted by NERC and approved by FERC, not when approved by the Board.
Section 2.2(b) of the Bylaws	<u>Enforcement</u> . The Corporation shall enforce Reliability Standards (including <u>Regional Reliability Standards and</u> Regional Variances) within the Region through the Corporation’s compliance enforcement program.	The change further reflects the changes made to the definition of “Regional Reliability Standard” above.

2. Changes Relating to Member Action by Written Ballot

Bylaws or Certificate of Incorporation Section Amended	Proposed Amendment	Issue
Section 6.8 of the Bylaws	<u>Action by Written Ballot.</u> All elections of directors shall be by written ballot. ~~Any other action that may be taken at a regular or special meeting of Members or any Industry Sector may be taken without a meeting or during a meeting if the Corporation mails or delivers a written ballot to every Regular Member entitled to vote on the matter. Approval by written ballot is valid only when the number of votes cast by ballot equals or exceeds the quorum required to be present at a meeting authorizing the action, and the number of approvals equals or exceeds the number of votes that would be required to approve the matter at a meeting at which the total number of votes cast was the same as the number of votes cast by ballot. Solicitations for votes by written ballot must: (i) indicate the number of responses needed to meet the quorum requirements; (ii) state the percentage of approvals necessary to approve the matter; (iii) specify the time by which a ballot must be received by the Corporation in order to be counted; and (iv) may not be revoked once received. If authorized by the Board, t~~The requirement of a written ballot shall be satisfied by a ballot submitted by electronic transmission provided that any such electronic transmission must either set forth or be submitted with information from which it can be determined that	This change eliminates the ability of Members to take action by written ballot without a meeting. Member action must take place at an annual or special meeting at which a quorum of Members is present. Written ballots will continue to be required for the election of directors provided the written ballots are submitted at a meeting.

Bylaws or Certificate of Incorporation Section Amended	Proposed Amendment	Issue
	the electronic transmission was authorized by the Member.	

3. Changes Relating to Nomination of At-large Directors, Director Resignations and Vacancies

Bylaws or Certificate of Incorporation Section Amended	Proposed Amendment	Issue
Section 7.4(e) of the Bylaws	Industry Sectors shall elect their respective sector and at-large directors from among individuals holding senior management positions in Member organizations. Any sector-elected or at-large director whose Member organization changes Industry Sectors or who ceases to hold a senior management position in a Member organization shall continue to serve out his or her remaining term, unless such director resigns or is removed. ~~When selecting at-large directors, Industry Sectors shall consider such factors as the geographic and functional representation of the Board.~~ No two directors may be employees of a single Member or any Affiliate or Related Party of a Member or any Affiliate.	The subject language is deleted in Section 7.4(e) and moved Section 7.4(g) to clarify that it is the responsibility of the Nominating and Governance Committee to consider geographic and functional factors when nominating at-large directors to the Board.
Section 7.4(g) of the Bylaws	At-large and independent directors shall be nominated by the nominating and governance committee of the Board. <u>When nominating at-large directors, the nominating and governance committee shall consider such factors as the geographic and functional representation of the Board.</u> The nominating and governance committee shall seek out for nomination independent directors from diverse backgrounds, who will contribute to the effective functioning of the Board	See above.

Bylaws or Certificate of Incorporation Section Amended	Proposed Amendment	Issue
	and the Corporation by bringing a broad range of industry expertise, viewpoints, experiences, skill sets and knowledge. If an incumbent independent director is not re-nominated, the nominating and governance committee will use reasonable efforts to ensure that diverse candidates are in the pool of potential nominees for the open independent director position and may retain an independent consultant to identify individuals qualified and willing to serve as an independent director.	
Section 7.7(a) of the Bylaws	<u>Resignations.</u> A director may resign ~~at any time~~ from the Board upon notice given in writing or by electronic transmission to the Corporation. Such resignation shall take effect at the time <u>identified in the notice as the effective date of resignation of its receipt by the Corporation.</u>	The changes to Sections 7.7(a) and 7.7(b) below allows a resigning director to designate a future effective date, which will provide the Members and the Board greater flexibility in filling the resulting vacancy as of the date of resignation.
Section 7.7(b) of the Bylaws	<u>Vacancies.</u> <u>If a notice of resignation provides that the effective date of resignation will occur on a future date within an unexpired term, the Industry Sector or Industry Sectors, as applicable, may elect a successor director to fill the impending vacancy prior to the effective date of the resignation, in accordance with the procedures and requirements set forth above. The successor director elected by the Industry Sector or Industry Sectors, as applicable, shall commence on the effective date of the resigning director's resignation and hold office for the</u>	See above.

Bylaws or Certificate of Incorporation Section Amended	Proposed Amendment	Issue
	<u>unexpired term of the vacated directorship replaced.</u> <u>If a successor Industry Sector or at-large director is not elected prior to the resignation effective date, or if</u> ~~If~~ an Industry Sector or at-large director resigns, dies or otherwise becomes incapacitated or is removed during the term of office for which elected, the directorship shall thereupon be vacant and shall be filled by the Industry Sector or Industry Sectors, as applicable, in accordance with the procedures and requirements set forth above. The successor director elected by the Industry Sector <u>or Industry Sectors, as applicable,</u> shall hold office for the unexpired term of the vacated directorship replaced. If <u>a successor independent director is not elected prior to the resignation effective date, or if</u> an independent director resigns, dies or otherwise becomes incapacitated or is removed during the term of office for which elected or ceases to be independent, as determined by the Board, his or her directorship shall thereupon be vacant and may be filled by <u>resolution of the Board and any independent director so chosen shall hold office</u> until the next annual meeting of Members, at which time a permanent successor shall be elected by the Industry Sectors for the remainder of the unexpired term. Upon an increase in the number of directors on the Board in accordance with Section 7.4(a) of these Bylaws, the independent directorship created thereby may be filled by resolution	



Bylaws or Certificate of Incorporation Section Amended	Proposed Amendment	Issue
	of the Board and any independent director so chosen shall hold office until the next annual meeting of Members, at which time a permanent successor shall be elected by the Industry Sectors for the remainder of such director's unexpired term.	

12/01/2011



AMENDED AND RESTATED BYLAWS

OF

ReliabilityFirst Corporation

a Delaware nonprofit corporation

Adopted December 19, 2006

Amended September 21, 2007¹

Amended December 6, 2007²

Amended May 22, 2008³

Amended December 4, 2008⁴

Amended December 1, 2011⁵

¹ Section 5.9.2

² Sections 1.2, 1.26, 16.1

³ Sections 1.12, 7.13, 7.14

⁴ Sections 5.8, 6.8, 6.9, 6.10.2, 6.10.4, 7.4, 7.5, 7.7, 7.9, 7.11, 7.13

⁵ Sections 1.24, 2.2, 6.8, 7.4, 7.7

TABLE OF CONTENTS

ARTICLE I. DEFINITIONS	5
Section 1.1. Act.....	5
Section 1.2. Adjunct Member	5
Section 1.3. Affiliate	5
Section 1.4. Associate Member	5
Section 1.5. Board.....	5
Section 1.6. Bulk Power System.....	5
Section 1.7. Certificate of Incorporation.....	5
Section 1.8. Commission.....	6
Section 1.9. Delegation Agreement.....	6
Section 1.10. Electronic Transmission	6
Section 1.11. ERO	6
Section 1.12. Hearing Body..	6
Section 1.13. Industry Sector.....	6
Section 1.14. Large LSEs.....	6
Section 1.15. Medium LSEs.....	6
Section 1.16. Members.....	6
Section 1.17. NERC	6
Section 1.18. NERC Rules.....	7
Section 1.19. Net Energy for Load.....	7
Section 1.20. Person.....	7
Section 1.21. Region.....	7
Section 1.22. Regional Entity.....	7
Section 1.23. Regional Variance	7
Section 1.24. Regional Reliability Standard	7
Section 1.25. Regular Member	7
Section 1.26. Regulatory Participant	8
Section 1.27. Related Party	8
Section 1.28. Reliability Coordinator	8
Section 1.29. Reliability Standard	8
Section 1.30. Reliable Operation	8
Section 1.31. RTOs	8
Section 1.32. Small LSEs.....	8
Section 1.33. Suppliers.....	9
Section 1.34. Transmission Companies	9
ARTICLE II. PURPOSE AND ACTIVITIES	9
Section 2.1. Purpose.....	9
Section 2.2. Activities.....	9
Section 2.3. Not-for-Profit Corporation.....	10
ARTICLE III. POWERS	10
Section 3.1. Powers	10
ARTICLE IV. OFFICES	11
Section 4.1. Principal Office.....	11
ARTICLE V. MEMBERS	11

Section 5.1.	General	11
Section 5.2.	Classes of Members	11
5.2.1	Regular Members.....	11
5.2.2	Associate Members	11
5.2.3	Adjunct Members	11
Section 5.3.	Qualifications of Members	11
Section 5.4.	Admission of Members.....	11
Section 5.5.	Voting Rights.....	12
Section 5.6.	Transfer of Membership	12
Section 5.7.	Obligations of Members	12
Section 5.8.	Withdrawal.....	12
Section 5.9.	Funding and Dues.....	12
5.9.1	NERC Funding.....	12
5.9.2	Application Fee, User-Fees and Other Charges.....	13
Section 5.10.	Penalties	13
ARTICLE VI.	MEETING OF MEMBERS	13
Section 6.1.	Annual Meeting of Members	13
Section 6.2.	Special Meetings of Members.....	13
Section 6.3.	Location of Meetings of Members	14
Section 6.4.	Notice of Meetings	14
6.4.1	Notice Requirements	14
6.4.2	Waiver of Notice; Objections	14
Section 6.5.	Record Date	14
Section 6.6.	Right to Vote; Act of Members	15
6.6.1	Industry Sector Voting	15
6.6.2	Act of Members.....	15
6.6.3	Special Voting Requirements.....	15
Section 6.7.	Quorum	15
Section 6.8.	Action by Written Ballot	15
Section 6.9.	Action by Electronic Communication	15
Section 6.10.	Member Representatives; Proxies	16
6.10.1	Designation of Representative	16
6.10.2	Authorization	16
6.10.3	Effective Period.....	16
6.10.4	Revocation.....	16
Section 6.11.	Public Notice of Member Meetings.....	16
Section 6.12.	Posting of Minutes.....	17
Section 6.13.	Reimbursement of Member Expenses	17
ARTICLE VII.	BOARD OF DIRECTORS.....	17
Section 7.1.	General	17
Section 7.2.	Management of Corporation.....	17
Section 7.3.	Voting	17
Section 7.4.	Composition of the Board	18
Section 7.5.	Terms of Directors.....	19
Section 7.6.	Reimbursement	19
Section 7.7.	Resignations; Vacancies.....	19

Section 7.8.	Meetings; Notice; Waiver	20
Section 7.9.	Quorum	21
Section 7.10.	Board Action.....	21
Section 7.11.	Action Without a Meeting	21
Section 7.12.	Action by Electronic Communication	21
Section 7.13.	Board Committees	22
Section 7.14.	Hearing Body	22
7.14.1	Quorum	22
7.14.2	Voting	22
Section 7.15.	Public Notice of Board Meetings.....	22
Section 7.16.	Posting of Minutes ²³	
Section 7.17.	Compensation of Directors	23
ARTICLE VIII.	ORGANIZATIONAL GROUPS.....	23
Section 8.1.	Establishment of Organizational Groups.....	23
Section 8.2.	Reimbursement	23
ARTICLE IX.	OFFICERS	23
Section 9.1.	Officers.....	23
Section 9.2.	Election and Term of Office	23
Section 9.3.	Removal.....	24
Section 9.4.	Vacancies	24
Section 9.5.	President.....	24
Section 9.6.	Vice Presidents.....	24
Section 9.7.	Secretary	24
Section 9.8.	Treasurer	25
ARTICLE X.	CERTIFICATES OF MEMBERSHIP	25
Section 10.1.	Certificates of Membership.....	25
ARTICLE XI.	BOOKS AND RECORDS.....	25
Section 11.1.	Books and Records; Financial Statements	25
ARTICLE XII.	FISCAL YEAR	26
Section 12.1.	Fiscal Year.....	26
ARTICLE XIII.	TRANSFER OF ASSETS	26
Section 13.1.	Member Approval Not Required	26
Section 13.2.	Member Approval Required.....	26
ARTICLE XIV.	CONTRACTS, CHECKS, DEPOSITS, AND GIFTS	26
Section 14.1.	Contracts	26
Section 14.2.	Checks, Drafts, or Orders	26
Section 14.3.	Deposits.....	27
Section 14.4.	Gifts	27
ARTICLE XV.	INSURANCE, LIMITATION ON LIABILITY AND INDEMNIFICATION	27
Section 15.1.	Insurance	27
Section 15.2.	Limitations on Liability	27
Section 15.3.	Right to Indemnification.....	27
15.3.1	Indemnified Persons	27

15.3.2	Denial of Authorization for Certain Proceedings	27
15.3.3	Certain Defined Terms	28
15.3.4	Expenses	28
15.3.5	Protection of Rights.....	28
15.3.6	Miscellaneous	29
ARTICLE XVI. TRANSITION.....		30
Section 16.1.	Transition Standards.....	30
ARTICLE XVII. PARTICIPATION BY REGULATORY PARTICIPANTS.....		31
Section 17.1.	Regulatory Participants	31
ARTICLE XVIII. BUDGET AND BUSINESS PLAN		31
Section 18.1.	Budget and Business Plan.....	31
ARTICLE XIX. AMENDMENT OF BYLAWS.....		31
Section 19.1.	Amendment Of Bylaws.....	31

**AMENDED AND RESTATED
BYLAWS OF
ReliabilityFirst Corporation
a Delaware nonprofit corporation
(the “Corporation”)**

[As adopted by the Members on December 19, 2006,
amended by the Board of Directors on September 21, 2007,
amended by the Members on December 6, 2007,
amended by the Board of Directors on May 22, 2008,
amended by the Members on December 4, 2008,
and amended by the Members on December 1, 2011]

**ARTICLE I.
DEFINITIONS**

Section 1.1. Act. “Act” shall mean Section 215 of the Federal Power Act (16 U.S.C. §824n).

Section 1.2. Adjunct Member. “Adjunct Member” shall mean any entity that does not qualify to join an Industry Sector but has been approved for membership. Adjunct Members may include Regulatory Participants.

Section 1.3. Affiliate. “Affiliate” shall mean, with respect to any entity, any other entity that, directly or indirectly, through one or more intermediaries, controls, or is controlled by, or is under common control with, such entity, as determined in the sole discretion of the Board of the Corporation. For this purpose, “control” may be presumed by the direct or indirect ownership of ten percent (10%) or more of the outstanding voting capital stock or other equity interests having ordinary voting power.

Section 1.4. Associate Member. “Associate Member” shall mean any entity that has joined an Industry Sector and is an Affiliate or Related Party of a Regular Member.

Section 1.5. Board. “Board” shall mean the Board of Directors of the Corporation.

Section 1.6. Bulk Power System. “Bulk Power System” shall mean facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof) and electric energy from generation facilities needed to maintain transmission system reliability, but does not include facilities used in the local distribution of electricity.

Section 1.7. Certificate of Incorporation. “Certificate of Incorporation” shall mean the Certificate of Incorporation of the Corporation filed with the Delaware Secretary of State, as from time to time amended.

Section 1.8. Commission. “Commission” shall mean the Federal Energy Regulatory Commission.

Section 1.9. Delegation Agreement. “Delegation Agreement” shall mean the delegation agreement, as supplemented or amended from time to time, between NERC and the Corporation pursuant to which NERC has delegated its authority to the Corporation to propose and enforce Reliability Standards within the Region.

Section 1.10. Electronic Transmission. “Electronic transmission” shall mean any form of communication, not directly involving the physical transmission of paper, that creates a record that may be retained, retrieved and reviewed by a recipient thereof, and that may be directly reproduced in paper form by such a recipient through an automated process.

Section 1.11. ERO. “ERO” shall mean the electric reliability organization established under the Act to enforce Reliability Standards applicable to all owners, operators and users of the Bulk Power System in North America.

Section 1.12. Hearing Body. “Hearing Body” shall mean a group established with authority to conduct and render decisions in a formal compliance hearing of an entity registered in the NERC compliance registry who is the subject of a notice of alleged violation, proposed penalty or sanction, contested mitigation plan or contested remedial action directive.

Section 1.13. Industry Sector. “Industry Sector” shall mean a group of Bulk Power System owners, operators or users in the Region with substantially similar interests as pertinent to the purposes and operations of the Corporation of the Bulk Power System. The Industry Sectors shall consist of the following: (1) Suppliers, (2) Transmission Companies, (3) RTOs, (4) Small LSEs, (5) Medium LSEs, and (6) Large LSEs.

Section 1.14. Large LSEs. “Large LSEs” shall mean entities that serve, or whose Related Parties serve, end use load with annual energy delivery to such load in the Region of 50,000 GWh or greater.

Section 1.15. Medium LSEs. “Medium LSEs” shall mean entities that serve, or whose Related Parties serve, end use load with annual energy delivery to such load in the Region between 10,000 GWh and 50,000 GWh.

Section 1.16. Members. “Members” shall mean Regular Members, Associate Members and Adjunct Members.

Section 1.17. NERC. “NERC” shall mean the North American Electric Reliability Corporation, or any successor entity, which has been certified by the Commission as the ERO pursuant to the Act to establish and enforce Reliability Standards for the Bulk Power System.

Section 1.18. NERC Rules. “NERC Rules” shall mean the NERC Rules of Procedure as approved by the Commission.

Section 1.19. Net Energy for Load. “Net Energy for Load” shall mean net generation of an electric system plus energy received from others less energy delivered to others through interchange. It includes system losses, but excludes energy required for storage of energy at energy storage facilities. Calculations of net energy for load for all purposes under these Bylaws shall be based on the most recent calendar year for which data on net energy for load of the Region is available.

Section 1.20. Person. “Person” shall mean a natural person, corporation, cooperative, partnership, association, or other private or public entity.

Section 1.21. Region. “Region” shall mean the geographic boundaries of the Corporation described in the Delegation Agreement.

Section 1.22. Regional Entity. “Regional Entity” shall mean any entity with which NERC has entered into a delegation agreement to delegate, or which the Commission or a governmental authority in Canada or Mexico has directly assigned, enforcement authority for reliability standards for the Bulk Power System in a defined geographic area of North America.

Section 1.23. Regional Variance. “Regional Variance” shall mean an aspect of a Reliability Standard that applies only within a particular Regional Entity or group of Regional Entities. A Regional Variance may be used to qualify how a particular Regional Entity or Regional Entities achieves the objectives of a Reliability Standard or may establish different measures or performance criteria as necessary to achieve reliability within the particular Regional Entity or group of Regional Entities. A Regional Variance may not be inconsistent with any Reliability Standard as it would otherwise exist without the Regional Variance. Such a Regional Variance may be proposed by a Regional Entity and, if adopted by NERC and approved by the Commission, shall be enforced within the applicable Regional Entity or Regional Entities pursuant to delegated authority.

Section 1.24. Regional Reliability Standard. “Regional Reliability Standard” shall mean a type of Reliability Standard that is applicable only within a particular Regional Entity or group of Regional Entities. A Regional Reliability Standard may augment, add detail to, or implement another Reliability Standard or cover matters not addressed by other Reliability Standards. A Regional Reliability Standard is not binding upon any Member or Registered Entity, nor is it effective or enforceable, until the Regional Reliability Standard has been adopted by NERC and approved by the Commission as a Reliability Standard within the applicable Regional Entity or Regional Entities pursuant to delegated authorities.

Section 1.25. Regular Member. “Regular Member” shall mean any entity that has joined an Industry Sector that either (i) has no Affiliates or Related Parties that are

Members or (ii) is the entity designated to be the Regular Member by any related group of Associate Members.

Section 1.26. Regulatory Participant. “Regulatory Participant” shall mean any state, District of Columbia or any provincial regulatory agency in the Region exercising authority over the rates, terms or conditions of electric service of an entity other than itself within the Region, or the planning, siting, construction or operation of electric facilities of an entity other than itself within the Region, as well as the Commission, regional advisory bodies that may be established by the Commission, or any federal regulator or agency or any entity authorized by any state, the District of Columbia or any province to represent utility consumers.

Section 1.27. Related Party. “Related Party” shall mean, solely for purposes of the governance provisions of these Bylaws, any entity that is registered as part of another entity or is registered for other entities in the NERC Compliance Registry. For purposes of these Bylaws, a representative of a state or federal government agency shall not be deemed a Related Party with respect to each other, and a public body’s regulatory authority, if any, over a Member shall not be deemed to make it a Related Party with respect to that Member.

Section 1.28. Reliability Coordinator. “Reliability Coordinator” shall mean any entity that is recognized as a reliability coordinator by NERC in the Region that does not otherwise qualify as a Transmission Company or RTO.

Section 1.29. Reliability Standard. “Reliability Standard” shall mean a requirement to provide for Reliable Operation of the Bulk Power System, including, without limitation, the foregoing requirements for the operation of existing Bulk Power System facilities, including cyber security protection, and the design of planned additions or modifications to such facilities to the extent necessary for reliable operation of the Bulk Power System, but shall not include any requirement to enlarge Bulk Power System facilities or to construct new transmission capacity or generation capacity.

Section 1.30. Reliable Operation. “Reliable Operation” shall mean operating the elements of the Bulk Power System within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failure of the Bulk Power System will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements.

Section 1.31. RTOs. “RTOs” shall mean PJM Interconnection L.L.C. and Midwest Independent Transmission System Operator, Inc., or such other entity that has been recognized by the Commission as a regional transmission operator or recognized functional equivalent in the Region.

Section 1.32. Small LSEs. “Small LSEs” shall mean (i) owners or operators of entities (or their representatives) that serve, or whose Related Parties serve, end use load with annual energy delivery to such load in the Region of 10,000 GWh or less, and

(ii) end-use customers interconnected with the Bulk Power System with load of at least 100 MW at one location in the Region.

Section 1.33. Suppliers. “Suppliers” shall mean owners or operators of electric generation connected to the transmission system and wholesale power marketers in the Region.

Section 1.34. Transmission Companies. “Transmission companies” shall mean (i) owners (or those with ownership entitlement), planners and operators of transmission facilities included in the Bulk Power System in the Region and (ii) Reliability Coordinators.

ARTICLE II. PURPOSE AND ACTIVITIES

Section 2.1. Purpose. The business or purposes to be conducted or promoted by the Corporation are:

- (a) to be a Regional Entity and exercise enforcement authority for Reliability Standards for the Bulk Power System in the Region pursuant to the Delegation Agreement;
- (b) to carry out certain of NERC’s activities that are in furtherance of NERC’s responsibilities as the ERO under the Act or in support of delegated functions, as specified in the NERC Rules or the Delegation Agreement; and
- (c) to engage in any other lawful act or activity for which not for profit corporations may be organized under the Delaware General Corporation Law.

The Corporation shall be exempt from federal income taxation pursuant to Section 501(c) of the Internal Revenue Code of 1986, as amended (hereinafter the “Code”) as an organization described in Section 501(c)(6) of the Code. The Corporation shall not engage directly or indirectly in any activity which would invalidate its status as an organization exempt from taxation under Section 501(a) of the Code as an organization described in Section 501(c)(6) of the Code. No part of the net income to the Corporation shall inure to the benefit of or be distributed to its directors, officers, members or other private persons, except that the Corporation shall be authorized and empowered to pay reasonable compensation for services actually rendered.

Section 2.2. Activities. In support and furtherance of its purpose, and in accordance with and at all times subject to the NERC Rules and the Delegation Agreement, the Corporation’s responsibilities shall include, but not be limited to, the following:

- (a) Reliability Standards. The Corporation shall:

(1) propose Reliability Standards, Regional Variances or modifications thereof to NERC; and

(2) develop Regional Reliability Standards through the Corporation's standards development procedure.

(b) Enforcement. The Corporation shall enforce Reliability Standards (including Regional Variances) within the Region through the Corporation's compliance enforcement program.

(c) Delegation-Related Services. The Corporation, on behalf of NERC, shall carry out certain of NERC's activities that are in furtherance of NERC's responsibilities as the ERO under the Act or in support of delegated functions, including:

(1) Organization registration and certification.

(2) Reliability readiness audit and improvement.

(3) Reliability assessment and performance analysis.

(4) Training and education.

(5) Situational awareness and infrastructure security.

(d) Budget. The Corporation shall prepare and submit a budget to NERC for the amount of costs the Corporation will incur in support of delegated functions that are in furtherance of NERC's responsibilities as the ERO under the Act.

(e) Non-delegated Functions. The Corporation may conduct such other activities for or on behalf of the Members that are not delegated to the Corporation by NERC under the Delegation Agreement if authorized by the Board and not inconsistent with the Act, NERC Rules, the Delegation Agreement or these Bylaws.

Section 2.3. Not-for-Profit Corporation. The Corporation is operated as a Delaware non-stock nonprofit corporation and is organized pursuant to the general corporation law of the State of Delaware.

ARTICLE III. POWERS

Section 3.1. Powers. The Corporation shall have the power to engage in any lawful act or activity for which corporations may be organized under the general corporation law of the State of Delaware, subject to any limitations provided in applicable federal, provincial or state law or in the Certificate of Incorporation or these Bylaws.

ARTICLE IV. OFFICES

Section 4.1. Principal Office. The principal office of the Corporation shall be located initially within the Region, at such location as the Board may from time to time determine, giving consideration to the total cost to the Corporation and convenience of travel for staff, Members and Regulatory Participants. Once established, the principal office may remain in its location, even if outside the Region.

ARTICLE V. MEMBERS

Section 5.1. General. The terms and conditions of membership in the Corporation shall be as provided in the Certificate of Incorporation and these Bylaws if not inconsistent therewith. All Regular Members and Associate Members shall be required to join a single Industry Sector.

Section 5.2. Classes of Members. The Corporation shall have three (3) classes of Members: Regular Members, Associate Members and Adjunct Members.

5.2.1 Regular Members. Except as set forth in Sections 5.5 and 6.5 of these Bylaws, Regular Members shall have the right to vote on all matters within their Industry Sector. Regular Members shall have all the rights and obligations of being a Member in the Corporation.

5.2.2 Associate Members. Associate Members shall not be entitled to vote within their Industry Sector or for any other purpose as a Member. Associate Members shall otherwise have all the rights and obligations of being a Member in the Corporation.

5.2.3 Adjunct Members. Adjunct Members shall not be entitled to vote for any purpose as a Member. Adjunct Members shall otherwise have all the rights of being a Member in the Corporation.

Section 5.3. Qualifications of Members. Any entity eligible to join an Industry Sector may be a Regular Member or Associate Member of the Corporation. Any entity not eligible to join an Industry Sector may be an Adjunct Member of the Corporation.

Section 5.4. Admission of Members. New Members may join the Corporation upon submittal of an application, in a form approved by the Board, and upon payment of such fees or charges, if any, as may be established by the Board or required by NERC. Each Regular Member and Associate Member shall designate the Industry Sector it wishes to join. A Regular Member and Associate Member may change its Industry Sector designation once each calendar year upon notice to the Corporation. Such notice must be provided to the Secretary of the Corporation at least sixty (60) days before an annual or other meeting of Members if the change is to be effective for such meeting. The President shall review a membership application and may request demonstration by the applicant that it qualifies for membership in a particular Industry Sector. Any dispute with respect to a Regular Member's or Associate Member's

qualifications for a particular Industry Sector shall be resolved by the Board. The President shall have authority to approve an application for membership, subject to review by the Board.

Section 5.5. Voting Rights. Each Regular Member in good standing shall be entitled to one vote in the Industry Sector in which it belongs on all matters submitted to a vote of Members. The Board may suspend voting rights for a Regular Member delinquent by more than 60 days in payment of any penalties or because of the Regular Member's failure to meet other obligations to the Corporation. Except with respect to the election of Industry Sector directors as described elsewhere in the Certificate of Incorporation and these Bylaws, matters properly brought before the Members at an annual or special meeting shall be acted upon by the Industry Sectors voting together as a single class. The vote of each Industry Sector shall be split into an affirmative component based on votes for the matter(s) presented, and a negative component based on votes against the matter(s) presented, in direct proportion to the votes cast within the Industry Sector for and against the matter presented, rounded to two decimal places. If authorized in advance by the Board, voting may be held electronically under such terms and conditions as are approved by the Board.

Section 5.6. Transfer of Membership. A Member of the Corporation may not transfer its membership or a right arising from it except to any Person succeeding to all or substantially all of the assets of the Member. If challenged, the President shall have authority to approve any such transfer, subject to review by the Board.

Section 5.7. Obligations of Members. By applying for and becoming a Regular or Associate Member of the Corporation, each Member agrees to comply with all Reliability Standards, all NERC standards and requirements, and the other obligations of Members of the Corporation set forth in these Bylaws or duly adopted by the Board in order to achieve the purposes of the Corporation. A Regular or Associate Member also agrees to obligate all of its Affiliates that have an impact on reliability in the Region to comply with all Reliability Standards and NERC standards and requirements. These obligations include but are not limited to: (a) obligations to provide data and information needed to perform the functions of the Corporation, (b) payment of any authorized penalties resulting from non-compliance with Reliability Standards, (c) in the case of Regular Members, electing the Board, and (d) providing qualified candidates to serve on organizational working groups. Adjunct Members agree to provide data and information needed to perform the functions of the Corporation.

Section 5.8. Withdrawal. A Member may withdraw from participation in the Corporation upon notice given in writing or by electronic transmission to the Corporation. Such notice shall specify a date, not earlier than thirty (30) days from the date of notice, on which the withdrawal shall become effective.

Section 5.9. Funding and Dues.

5.9.1 NERC Funding. In accordance with and at all times subject to the NERC Rules and the Delegation Agreement, the Corporation shall equitably allocate its dues,

fees and other charges for the delegated functions conducted by the Corporation among all end users. The Corporation shall submit to NERC annually a list of all load-serving entities within the Region. NERC will bill all load-serving entities in the Region for the Corporation's costs for the delegated functions based on Net Energy for Load and be responsible for collection.

5.9.2 Application Fee, User-Fees and Other Charges. The Corporation may charge a nominal fee, which shall be determined by the President, for the submission of applications for membership. The Board of Directors may from time to time fix the amount of user-fees or other charges, if any, for activities that are not delegated to the Corporation by NERC under the Delegation Agreement and determine the methods of collection from entities that choose to participate in such activities.

Section 5.10. Penalties. If the Corporation initiates an investigation that leads to the imposition of a penalty, the Corporation shall receive any penalty monies that results from the investigation. All monies which the Corporation collects from the issuance of penalties shall be applied as a general offset to the Corporation's budget requirements for the subsequent fiscal year. Funds from financial penalties shall not be directly applied to any program maintained by the Corporation.

ARTICLE VI. MEETING OF MEMBERS

Section 6.1. Annual Meeting of Members. The Members shall hold an annual meeting in December of each year, or at such other time specified by the Board. At the annual meeting of Members: (i) each Industry Sector shall elect the successor(s), if any, for any director(s) from their Industry Sector whose term will expire before the next annual meeting of the Members, provided however, that any Industry Sector may elect a successor director representing such Industry Sector prior to such annual meeting, in accordance with the provisions of this Article VI, in which case the election of such succeeding director(s) shall be reported to the Corporation at such annual meeting; (ii) the President and Treasurer shall report on the activities and financial condition of the Corporation; (iii) the Industry Sectors shall elect a slate of at-large and independent directors to fill vacancies or expiring terms; and (iv) the Industry Sectors shall consider and act upon such other matters as are consistent with the notice of the annual meeting. The failure to hold an annual meeting in accordance with these Bylaws shall not affect the validity of a corporate action.

Section 6.2. Special Meetings of Members. Special meetings of the Members may be called by six (6) directors on the Board, by the President, or by Members if at least ten percent (10%) of the Regular Members sign, date, and deliver to the President one or more written demands for a special meeting describing the purpose for which it is to be held. Within fifteen (15) days after receipt of a demand for a special meeting from Regular Members, the President shall cause a special meeting to be called and held on notice in accordance with Section 6.4 of these Bylaws. If the President fails to cause a special meeting to be called and held as required by this Section 6.2, a Regular Member making the demand may call the meeting by giving notice under Section 6.4.

In either event, notice of the meeting and the costs of the meeting shall be at the expense of the Corporation. The business transacted at a special meeting is limited to the purposes stated within the notice of the meeting. Business transacted at a special meeting that is not included in those stated purposes is voidable by or on behalf of the Corporation, unless ninety percent (90%) of the Regular Members entitled to vote were present at such meeting or have waived notice of the meeting under Section 6.4.

Section 6.3. Location of Meetings of Members. Meetings of Members shall be held at a location designated by the President or the Board. If a Regular Member calls a meeting pursuant to Section 6.2, the Regular Members making the demand for the meeting may designate the location, provided the meeting must be held within the Region and in a facility of appropriate size to accommodate the Members.

Section 6.4. Notice of Meetings.

6.4.1 Notice Requirements. Notice of meetings of Members must be given at least five (5) days before the date of a meeting and not more than sixty (60) days before the date of a meeting. The notice must contain the date, time and place of the meeting, instructions for electronic attendance or voting, if applicable, and an agenda of the matters upon which action may be taken at the meeting. A matter may be added to the agenda of a meeting at the meeting upon the affirmative vote of three-quarters (3/4) of the Industry Sector votes cast on a motion to amend the agenda. If the meeting is an adjourned meeting and the date, time and place of the meeting were announced at the time of the adjournment, notice is not required unless a new record date for the adjourned meeting is or must be fixed. Notice shall be deemed given by the Corporation to the Members when (a) posted on the Corporation's public website in a reasonably prominent location, and (b) sent by mail, facsimile or reputable overnight delivery service or by electronic transmission to each Member's representative authorized pursuant to Section 6.10.1

6.4.2 Waiver of Notice; Objections. A Member may waive notice of a meeting of Members. A waiver of notice by a Member entitled to notice is effective whether given before, at, or after the meeting, and whether given in writing, or by attendance. Attendance by a Member at a meeting is a waiver of notice of that meeting, unless the Member objects at the beginning of the meeting to the transaction of business because the meeting is not lawfully called or convened, or objects before a vote on an item of business because the item may not lawfully be considered at that meeting and does not participate in the consideration of the item at that meeting.

Section 6.5. Record Date. The Board may fix a date not more than sixty (60) days before the date of a meeting of Members as the date for the determination of the Members entitled to notice of and entitled to vote at the meeting. When a date is so fixed, only Members on that date are entitled to notice and to vote at the meeting unless the Board fixes a new date for determining the right to notice and to vote, which it must do if the meeting is adjourned to a date more than sixty (60) days after the record date for determining Members entitled to notice of the original meeting.

Section 6.6. Right to Vote; Act of Members.

6.6.1 Industry Sector Voting. Voting of the Members shall be by Industry Sector, with each Industry Sector entitled to cast one vote. Each Member entitled to vote in an Industry Sector shall be entitled to cast one vote in its Industry Sector. The vote of each Industry Sector shall be split into an affirmative component based on votes for the pending motion, and a negative component based on votes against the pending motion, in direct proportion to the votes cast within the Industry Sector for and against the pending motion, rounded to two decimal places. To the extent practicable, all Member votes may be held electronically under such terms and conditions as are approved by the Board.

6.6.2 Act of Members. If a quorum is present, except with respect to any matter described in Section 6.6.3, a majority of the Industry Sector votes cast on the matter shall be the act of the Members.

6.6.3 Special Voting Requirements. Notwithstanding any other provision of these Bylaws, and except as set forth in the Certificate of Incorporation and Section 13.2 of these Bylaws, two-thirds (2/3) of the Industry Sector votes cast shall be required to:

(a) Amend the Bylaws, except as otherwise provided in Section 19.1 of these Bylaws. The substance of the proposed amendment must be contained in the notice of the meeting at which the vote will be taken; however, the Members may modify a proposed Bylaw amendment at the meeting.

(b) Approve any proposal to terminate the Corporation.

Section 6.7. Quorum. A quorum for a meeting of Members is a majority of the Regular Members entitled to vote in each Industry Sector at the meeting. A quorum for a meeting of an Industry Sector is a majority of the Regular Members of that Industry Sector entitled to vote at the meeting. In both cases, electronic participation is acceptable if authorized by the Board. A quorum is necessary for the transaction of business at a meeting of Members or of any Industry Sector. If a quorum is not present, a meeting may be adjourned for that reason by the Industry Sectors or Regular Members then represented or present.

Section 6.8. Action by Written Ballot. All elections of directors shall be by written ballot. The requirement of a written ballot shall be satisfied by a ballot submitted by electronic transmission provided that any such electronic transmission must either set forth or be submitted with information from which it can be determined that the electronic transmission was authorized by the Member.

Section 6.9. Action by Electronic Communication. A conference among Members by a means of communication through which the participants may simultaneously hear each other during the conference is a meeting of the Members, if the same notice is given of the conference as would be required for a meeting and if the number of persons participating in the conference is a quorum. Participation in a

meeting by this means is personal presence at the meeting. A Member may participate in a meeting of the Members by a means of communication through which the Member, other persons participating, and all persons physically present at the meeting may simultaneously communicate with each other during the meeting. Participation in a meeting by this means constitutes personal presence at the meeting.

Section 6.10. Member Representatives; Proxies.

6.10.1 Designation of Representative. Each year prior to the annual meeting of Members, each Regular Member shall designate the individual authorized to vote on Corporation matters on behalf of the Member, in accordance with procedures approved by the Board. A Regular Member may change such designation at any time by providing at least twenty-four (24) hour written notice to the Secretary of the Corporation. Such notice may be provided by electronic transmission.

6.10.2 Authorization. The individual designated to vote by a Regular Member may appoint a proxy to vote or otherwise act for the Regular Member at any meeting by signing an appointment form either personally or by an attorney so designated by the Regular Member. Such authorization may be in writing or by means of electronic transmission to the person who will be the holder of the proxy, provided that such electronic transmission must either set forth or be submitted with information from which it can be determined that the electronic transmission was authorized by the Member representative.

6.10.3 Effective Period. An appointment of a proxy is effective when received by the Secretary or other officer or agent authorized to tabulate votes. An appointment is valid for the next regular or specially scheduled meeting or ballot by electronic transmission. However, a proxy is not valid for more than sixty (60) days from its date of execution.

6.10.4 Revocation. An appointment of a proxy is revocable by a Regular Member. Appointment of a proxy is revoked by the person appointing the proxy either by open declaration at a meeting or by signing and delivering a revocation in writing or by electronic transmission to the Secretary or other officer or agent authorized to tabulate proxy votes. This may be done either in a statement that the appointment of the proxy is revoked or by a subsequent appointment that shall serve to cancel all prior proxies.

Section 6.11. Public Notice of Member Meetings. Notice to the public of the dates, times and places of meetings of the Members, and all nonconfidential material provided to the Members, shall be posted on the Corporation's website at approximately the same time that notice is given to the Members. Meetings of the Members shall be open to the public, subject to reasonable limitations due to the availability and size of meeting facilities; provided, that the meeting may be held in or adjourn to closed session to discuss matters of a confidential nature, including, but not limited to, personnel matters, compliance and enforcement matters, litigation or

commercially sensitive or critical infrastructure information of a Member or other Person.

Section 6.12. Posting of Minutes. Minutes of meetings of Members shall be posted on the Corporation's website when available.

Section 6.13. Reimbursement of Member Expenses. The Corporation will be under no obligation to reimburse Members for expenses associated with their attendance at regular or special Member meetings.

ARTICLE VII. BOARD OF DIRECTORS

Section 7.1. General. The composition of the Board and the terms of office of the directors, the manner of their nomination, election or appointment, and other terms and conditions of their service, shall be as provided in the Certificate of Incorporation and these Bylaws if not inconsistent therewith.

Section 7.2. Management of Corporation. The business of the Corporation shall be managed under the direction of the Board. Specific functions of the Board shall include, but not be limited to:

- (a) govern the Corporation and oversee all of its activities;
- (b) establish and oversee all organizational groups;
- (c) approve, revise and enforce Reliability Standards utilizing a fair, open, balanced and inclusive process;
- (d) establish compliance monitoring procedures and requirements, and penalties and sanctions for non-compliance consistent with applicable NERC Rules;
- (e) impose penalties and sanctions consistent with the NERC Rules and the procedures approved by the Board;
- (f) establish and approve an annual budget for submission to NERC;
- (g) hire the Corporation's president and approve his or her salary;
- (h) annually at the first regular Board meeting following the annual meeting of Members, elect a Chair ("Chair") and a vice-chair from among the directors on the Board; and
- (i) establish Board committees as appropriate.

Section 7.3. Voting. Each director shall have one vote with respect to decisions of the Board.

Section 7.4. Composition of the Board.

(a) The Board shall consist of fourteen (14) or fifteen (15) directors which number shall be established from time to time by resolution of the Board, which resolution shall in no event have the effect of terminating the term of any incumbent director.

(b) Eight directors shall be elected by the Industry Sectors as follows:

- (i) Suppliers shall elect two (2) directors;
- (ii) Transmission Companies shall elect two (2) directors;
- (iii) RTOs shall select one (1) director;
- (iv) Small LSEs shall elect one (1) director;
- (v) Medium LSEs shall elect one (1) director; and
- (vi) Large LSEs shall elect one (1) director.

(c) Three (3) directors shall be at-large. At-large directors shall be elected by all of the Industry Sectors voting together as a single class.

(d) Three (3) directors, if the Board consists of fourteen (14) directors, and four (4) directors, if the Board consists of fifteen (15) directors, shall be independent from the Corporation and any Member or any Affiliate or Related Party of any Member. Independent directors shall be elected by all of the Industry Sectors voting together as a single class.

(e) Industry Sectors shall elect their respective sector and at-large directors from among individuals holding senior management positions in Member organizations. Any sector-elected or at-large director whose Member organization changes Industry Sectors or who ceases to hold a senior management position in a Member organization shall continue to serve out his or her remaining term, unless such director resigns or is removed. No two directors may be employees of a single Member or any Affiliate or Related Party of a Member or any Affiliate.

(f) An independent director is a person (i) who is not an officer or employee of the Corporation, an officer, director, or employee of a Member, or an officer, director or employee of any entity that would reasonably be perceived as having a direct financial interest in the outcome the Board's decisions, or (ii) who does not have a relationship that would interfere with the exercise of independent judgment in carry out the responsibilities of a director. The Board may adopt additional standards for director independence not inconsistent herewith.

(g) At-large and independent directors shall be nominated by the nominating and governance committee of the Board. When nominating at-large directors, the nominating and governance committee shall consider such factors as the geographic and functional representation of the Board. The nominating and governance committee shall seek out for nomination independent directors from diverse backgrounds, who will contribute to the effective functioning of the Board and the Corporation by bringing a broad range of industry expertise, viewpoints, experiences, skill sets and knowledge. If an incumbent independent director is not re-nominated, the nominating and governance committee will use reasonable efforts to ensure that diverse candidates are in the pool of potential nominees for the open independent director position and may retain an independent consultant to identify individuals qualified and willing to serve as an independent director.

(h) Any director which the full Board has determined has a conflict of interest on any compliance or enforcement matter brought before the Board shall not vote on such matter and shall recuse himself or herself from all Board deliberations concerning such matter.

(i) There will be no alternates or proxies for directors.

Section 7.5. Terms of Directors. The directors will be divided into three classes. The number of directors in each class shall be as nearly equal as possible. The term of office of the first class will expire at the second annual meeting of Members; the term of office of the second class will expire one year thereafter; and the term of office of the third class two years thereafter. At each annual meeting of Members, directors shall be chosen for a three year term to succeed those whose term expires. No two at-large directors and no two directors of the same Industry Sector shall be in the same class. At least one (1) independent director shall be in each class. Each director shall hold office until (a) the expiration of the term for which he or she was elected and until his or her successor is elected and qualified, or (b) his or her earlier death, resignation or removal. Any director may be removed at any time by the affirmative vote of two-thirds of the Industry Sector or Industry Sectors, as applicable, electing such director. A director may be removed by the Board for non-attendance at three consecutive Board meetings.

Section 7.6. Reimbursement. Independent directors shall have the right to reimbursement by the Corporation of their actual reasonable travel expenses to Board meetings or when specifically selected to represent the Corporation at a business meeting. The directors elected by the Industry Sectors and the at-large directors shall not be reimbursed by the Corporation for any expenses, unless specifically approved in advance by resolution of the Board.

Section 7.7. Resignations; Vacancies.

(a) Resignations. A director may resign from the Board upon notice given in writing or by electronic transmission to the Corporation. Such

resignation shall take effect at the time identified in the notice as the effective date of resignation.

(b) Vacancies. If a notice of resignation provides that the effective date of resignation will occur on a future date within an unexpired term, the Industry Sector or Industry Sectors, as applicable, may elect a successor director to fill the impending vacancy prior to the effective date of the resignation, in accordance with the procedures and requirements set forth above. The successor director elected by the Industry Sector or Industry Sectors, as applicable, shall commence on the effective date of the resigning director's resignation and hold office for the unexpired term of the vacated directorship replaced.

If a successor Industry Sector or at-large director is not elected prior to the resignation effective date, or if an Industry Sector or at-large director resigns, dies or otherwise becomes incapacitated or is removed during the term of office for which elected, the directorship shall thereupon be vacant and shall be filled by the Industry Sector or Industry Sectors, as applicable, by written or electronic ballot in accordance with the procedures and requirements set forth above. The successor director elected by the Industry Sector or Industry Sectors, as applicable, shall hold office for the unexpired term of the vacated directorship replaced.

If a successor independent director is not elected prior to the resignation effective date, or if an independent director resigns, dies or otherwise becomes incapacitated or is removed during the term of office for which elected or ceases to be independent, as determined by the Board, his or her directorship shall thereupon be vacant and may be filled by resolution of the Board and any independent director so chosen shall hold office until the next annual meeting of Members, at which time a permanent successor shall be elected by the Industry Sectors for the remainder of the unexpired term. Upon an increase in the number of directors on the Board in accordance with Section 7.4(a) of these Bylaws, the independent directorship created thereby may be filled by resolution of the Board and any independent director so chosen shall hold office until the next annual meeting of Members, at which time a permanent successor shall be elected by the Industry Sectors for the remainder of such director's unexpired term.

Section 7.8. Meetings; Notice; Waiver.

(a) Meetings. An annual meeting of the Board shall be held without notice immediately following the annual meeting of the Members. The Board shall elect the Chair and Vice-Chair for the next year at the annual meeting. In addition, regular meetings may be held at such time or times as fixed by the Board. Special meetings of the Board may be called by the Board's Chair, the President or by any three directors and shall be held at the principal office of the Corporation, or such other place within the Region as determined by the Chair or the President after consultation with the Board.

(b) Notice. Notice of the dates, times, and places of all regular and special meetings of the Board shall be published by the Secretary and provided to all directors and Members not less than three (3) days prior to the date of the meeting. Notice shall be deemed given by the Corporation to directors and the Members when (a) posted on the Corporation's public website in a reasonably prominent location, and (b) sent by mail, facsimile or reputable overnight delivery service or by electronic transmission to each director and each Member's representative authorized pursuant to Section 6.10.1.

(c) Waiver. Any person entitled to notice of a regular or special meeting of the Board may waive notice thereof. A waiver of notice by a person entitled to notice is effective whether given before, at, or after the meeting, and whether given in writing or by attendance. Attendance by a director at a meeting of the Board is a waiver of notice of that meeting, unless the director objects at the beginning of the meeting to the transaction of business because the meeting is not lawfully called or convened, or objects before a vote on an item of business because the item may not lawfully be considered at that meeting and does not participate in the consideration of the item at that meeting.

Section 7.9. Quorum. For the Board to take action at a meeting, a quorum of directors must be present. A quorum is a majority of the directors then in office, provided that: (a) if there are three or four independent directors holding office, two independent directors must be present to constitute a quorum, or (b) if there are two independent directors holding office, one independent director must be present to constitute a quorum. If there is only one independent director or no independent directors holding office, there is no requirement that an independent director be present in order for the Board to have a quorum. In the absence of a quorum, a majority of the directors present may adjourn a meeting, without notice, except as may be given at such meeting, until a quorum is present.

Section 7.10. Board Action. The act of a majority of the directors present at a meeting at which a quorum is present shall be the act of the Board, unless the act of a greater number is required by law or these Bylaws.

Section 7.11. Action Without a Meeting. Any action required or permitted to be taken at any meeting of the Board or any committee thereof may be taken without a meeting if all members of the Board or committee, as the case may be, consent thereto in writing or by electronic transmission, and the writing or writings or electronic transmission or transmissions are filed with the minutes of proceeding of the Board or the committee. Any nonconfidential material provided to the Board or a committee in connection with such action shall be posted on the Corporation's website at approximately the same time that it is given to the Board or the committee. The results of all actions taken by the Board or any committee thereof without a meeting shall be promptly posted on the Corporation's website.

Section 7.12. Action by Electronic Communication. A conference among directors by a means of communication through which the directors may simultaneously

hear each other during the conference is a Board meeting if the same notice is given of the conference as would be required for a meeting and if the number of directors participating in the conference is a quorum. Participation in a meeting by this means constitutes personal presence at the meeting. A director may participate in a Board meeting by any means of communication through which the director, other directors participating, and all directors physically present at the meeting may simultaneously communicate with each other during the meeting.

Section 7.13. Board Committees. The Board shall have an audit committee, compensation committee, nominating and governance committee and compliance committee, and such other committees the Board deems necessary and appropriate. Each committee shall be comprised of not less than three directors. The compliance committee shall be comprised of a minimum of five directors, a majority of whom are independent directors. All independent directors shall serve on the compliance committee. The Board may require that a minimum number of independent directors serve on any or all other Board committees. The Board shall have the power to appoint, and to delegate authority to, such other committees of the Board as it determines to be appropriate from time to time. The Board may require any committee to adopt a charter, subject to approval by the Board, governing the activities and authority of the committee and the composition of its members.

Section 7.14. Hearing Body. The Hearing Body shall consist of the Board compliance committee.

7.14.1 Quorum. For the Hearing Body to take action at a hearing, a quorum of members must be present. A quorum is a majority of members of the Hearing Body, provided that two independent directors are present. If a quorum of the Hearing Body does not remain after any recusals and rulings on motions for disqualification, the compliance committee shall appoint a new member to the Hearing Body from among other directors to create a quorum, provided that the requirement that at least two independent directors are present for a quorum shall at all times continue to be met. Such new member shall serve on the Hearing Body for purposes of the subject hearing through the conclusion of the hearing but not thereafter.

7.14.2 Voting. Each Hearing Body member shall have one vote with respect to matters presented at a hearing. Action may be taken at a hearing at which a quorum is present upon the vote of the majority of members present.

Section 7.15. Public Notice of Board Meetings. Notice to the public of the dates, times and places of Board meetings, including committees thereof, and all nonconfidential material provided to the Board or the committees, shall be posted on the Corporation's website, and notice of Board and committee meetings shall be sent by electronic transmission to Members, at approximately the same time that notice is given to the Board or the committee, as the case may be. Board and committee Meetings shall be open to all Members and the public, subject to reasonable limitations due to the availability and size of meeting facilities; provided, that any meeting may be held in or adjourn to closed session to discuss matters of a confidential nature, including, but not

limited to, personnel matters, compliance and enforcement matters, litigation or commercially sensitive or critical infrastructure information of a Member or other Person.

Section 7.16. Posting of Minutes. Minutes of Board and committee meetings shall be posted on the Corporation's website when available.

Section 7.17. Compensation of Directors. The directors elected by the Industry Sectors and the at-large directors shall not receive compensation for their service to the Corporation as directors on the Board. The independent directors shall be entitled to such compensation as the Board may from time to time determine. Nothing contained in these Bylaws shall preclude any director from receiving compensation for services to the Corporation in any other capacity.

ARTICLE VIII. ORGANIZATIONAL GROUPS

Section 8.1. Establishment of Organizational Groups. The Board shall establish such organizational groups, consisting of committees, sub-committees, task forces and working groups of Members, as are necessary and appropriate to accomplish the purposes of the Corporation in an efficient and cost-effective manner. All organizational groups shall be subject to the direction and control of the Board. The membership of organizational groups shall be determined based upon experience, expertise and geographic diversity and to the extent practicable shall include balanced representation of the Industry Sectors. The Board shall establish policies and procedures governing the creation of organizational groups, how they are populated, how voting and related matters are conducted, how they may be reorganized and the direction and termination of such groups. The Board shall conduct a review of all organizational groups of the Corporation on an annual basis to ensure that the business of the Corporation is conducted in an efficient, cost-effective manner.

Section 8.2. Reimbursement. The Board may authorize reimbursement for persons acting on behalf of the Corporation, as necessary in the interests of the Corporation.

ARTICLE IX. OFFICERS

Section 9.1. Officers. The officers of the Corporation shall include a President, one or more Vice Presidents, a Secretary, a Treasurer and any other officers as may be elected or appointed in accordance with the provisions of this Article. The Board may elect or appoint any additional officers that it deems desirable, such other officers to have the authority and perform the duties prescribed by the Board. The same individual may hold any number of offices, except that of President.

Section 9.2. Election and Term of Office. The officers of the Corporation shall be elected annually by the Board at the annual meeting of the Board. Each officer shall

hold office at the pleasure of the Board. If the election of officers is not held at such meeting, such election shall be held as soon thereafter as is convenient. New officers may be created and the positions filled at any meeting of the Board. Each elected officer shall hold office until his or her successor has been duly elected and qualified or upon his or her earlier resignation or removal.

Section 9.3. Removal. Any officer elected by the Board may be removed by the affirmative vote of two-thirds (2/3) of the Board whenever in its judgment the best interests of the Corporation would be served thereby, but such removal shall be without prejudice to the contract rights, if any, of the officer so removed. Election or appointment of an officer or agent shall not of itself create contract rights.

Section 9.4. Vacancies. A vacancy in any office because of death, incapacity, resignation, removal, disqualification, or otherwise, may be filled by the Board for the unexpired portion of the term.

Section 9.5. President. The President shall:

- (a) be the principal executive and operating officer of the Corporation;
- (b) sign certificates of membership, and may sign any deeds, mortgages, deeds of trust, notes, bonds, contracts or other instruments authorized by the Board to be executed, except in cases in which the signing and execution thereof shall be expressly delegated by the Board or by these Bylaws to some other officer or agent of the Corporation; and
- (c) perform all duties incident to the office of President, including hiring and directing staff, and such other duties as may be prescribed by the Board from time to time.

Section 9.6. Vice Presidents. The Vice President(s) shall perform such duties and have such powers as the Board or President may from time to time prescribe. At the request of the Board, the Vice President (or in the event there be more than one Vice President, the Vice Presidents in the order designated, or in the absence of any designation, then in the order of their election) shall perform the duties of the President, and when so acting, shall have all the powers of and be subject to all the restrictions upon the President.

Section 9.7. Secretary. The Secretary shall ensure that the following duties are carried out:

- (a) the minutes of the meetings of the Members and of the Board, and each committee thereof, are recorded;
- (b) all required notices are duly given in accordance with these Bylaws and as required by law;

(c) a register of the current names and addresses of all Members is maintained and posted on the Corporation's website;

(d) a complete copy of the Certificate of Incorporation and Bylaws of the Corporation containing all amendments thereto are kept on file at all times and posted on the Corporation's website, which copies shall always be open to the inspection of any Member; and

(e) generally perform all duties incident to the office of Secretary and such other duties as may be prescribed by the Board from time to time.

Section 9.8. Treasurer. The Treasurer shall be responsible for the following activities:

(a) maintain custody of all funds and securities of the Corporation;

(b) receipt of and the issuance of receipts for all monies due and payable to the Corporation and for deposit of all such monies in the name of the Corporation in such bank or banks or financial institutions as shall be selected by the Board; and

(c) generally perform all duties incident to the office of Treasurer and such other duties as may be prescribed by the Board from time to time.

ARTICLE X. CERTIFICATES OF MEMBERSHIP

Section 10.1. Certificates of Membership. The Board may, but need not, provide for the issuance of certificates evidencing membership in the Corporation, which certificates shall be in such form as may be determined by the Board.

ARTICLE XI. BOOKS AND RECORDS

Section 11.1. Books and Records; Financial Statements. The Corporation shall keep at such office selected by the Board correct and complete copies of its Certificate of Incorporation and Bylaws, accounting records, and minutes of meetings of Members, Board, and committees having any of the authority of the Board. A Member, or the agent or attorney of a Member, may inspect all books and records for any proper purpose at any reasonable time. Upon request, the Corporation shall give the Member a statement showing the financial result of all operations and transactions affecting income and expenses during its last annual accounting period and a balance sheet containing a summary of its assets and liabilities as of the closing date of the accounting period.

ARTICLE XII.
FISCAL YEAR

Section 12.1. Fiscal Year. The fiscal year of the Corporation shall be the calendar year.

ARTICLE XIII.
TRANSFER OF ASSETS

Section 13.1. Member Approval Not Required. Subject to restrictions set forth in the Certificate of Incorporation, the Corporation, by affirmative vote of the Board, may sell, lease, transfer, or dispose of its property and assets in the usual and regular course of its activities and grant a security interest in all or substantially all of its property and assets in the usual and regular course of its activities, upon those terms and conditions and for those considerations, which may be money, securities, or other instruments for the payment of money or other property, as the Board considers expedient, in which case no Member approval is required.

Section 13.2. Member Approval Required. Subject to restrictions set forth in the Certificate of Incorporation, the Corporation may sell, lease, transfer, or dispose of all or substantially all of its property and assets, including its good will, not in the usual and regular course of its activities, upon those terms and conditions and for those considerations, which may be money, securities, or other instruments for the payment of money or other property, as the Board considers expedient only when approved at a regular or special meeting of the Members by the affirmative vote of two-thirds (2/3) of all the Members. Notice of the meeting must be given to the Members. The notice must state that a purpose of the meeting is to consider the sale, lease, transfer, or other disposition of all or substantially all of the property and assets of the Corporation.

ARTICLE XIV.
CONTRACTS, CHECKS, DEPOSITS, AND GIFTS

Section 14.1. Contracts. The Board may authorize any officer or officers or agent or agents of the Corporation, in addition to the officers so authorized by these Bylaws, to enter into any contract or execute and deliver any instrument in the name of and on behalf of the Corporation, and such authority may be general or may be confined to specific instances.

Section 14.2. Checks, Drafts, or Orders. All checks, drafts, or orders for the payment of money, notes, or other evidences of indebtedness issued in the name of the Corporation, may be signed by such officer or officers or agent or agents of the Corporation, and in such manner, as shall from time to time be determined by resolution of the Board.

Section 14.3. Deposits. All funds of the Corporation shall be deposited to the credit of the Corporation in such banks, trust companies, or other depositories as the Board may select.

Section 14.4. Gifts. The Board may accept on behalf of the Corporation any contribution, gift, bequest, or devise for any purpose of the Corporation.

ARTICLE XV. INSURANCE, LIMITATION ON LIABILITY AND INDEMNIFICATION

Section 15.1. Insurance. The President is authorized to procure insurance to protect the Corporation against damages arising out of or related to any directive, order, procedure, action or requirement of the Corporation.

Section 15.2. Limitations on Liability. As provided in Article Fourteenth of the Certificate of Incorporation, a director of the Corporation shall not be personally liable to the Corporation or its Members for monetary damages for breach of fiduciary duty as a director, except for liability (i) for any breach of the director's duty of loyalty to the Corporation or its Members, (ii) for acts or omissions not in good faith or which involve intentional misconduct or a knowing violation of law, (iii) under Section 174 of the Delaware General Corporation Law or (iv) for any transaction from which the director derived any improper personal benefit. If the Delaware General Corporation Law is amended to authorize corporate action further eliminating or limiting the personal liability of directors, then the liability of a director of the Corporation shall be eliminated or limited to the fullest extent permitted by the Delaware General Corporation Law, as so amended. Any repeal or modification of Article Fifteenth of these Bylaws by the Members of the Corporation shall not adversely affect any right or protection of a director of the Corporation existing at the time of such repeal or modification.

Section 15.3. Right to Indemnification.

15.3.1 Indemnified Persons. Each person who was or is made a party or is threatened to be made a party to or is involved in or called as a witness in any Proceeding because he or she is an Indemnified Person shall be indemnified and held harmless by the Corporation to the fullest extent permitted under the Delaware General Corporation Law (the "DGCL"), as the same now exists or may hereafter be amended (but, in the case of any such amendment, only to the extent that such amendment permits the Corporation to provide broader indemnification rights than the DGCL permitted the Corporation to provide prior to such amendment). Such indemnification shall cover all expenses incurred by an Indemnified Person (including, but not limited to, attorneys' fees and other expenses of litigation) and all liabilities and losses (including, but not limited to, judgments, fines, ERISA or other excise taxes or penalties and amounts paid or to be paid in settlement) incurred by such person in connection therewith.

15.3.2 Denial of Authorization for Certain Proceedings. Notwithstanding anything to the contrary in this Section 15.3, except with respect to indemnification of Indemnified

Persons specified in paragraph 15.3.3 of this Section 15.3, the Corporation shall indemnify an Indemnified Person in connection with a Proceeding (or part thereof) initiated by such person only if authorization for such Proceeding (or part thereof) was not denied by the Board of the Corporation prior to the earlier of 60 days after receipt of notice thereof from such Indemnified Person.

15.3.3 Certain Defined Terms. For purposes of this Section 15.3, the following terms shall have the following meanings (such meanings to be equally applicable to both the singular and plural forms of the terms defined):

(1) a “Proceeding” is any investigation, action, suit or proceeding, whether civil, criminal, administrative or investigative, and any appeal therefrom.

(2) an “Indemnified Person” is a person who is, was, or had agreed to become a Director of the Corporation (including, in the case of such person seeking indemnification while serving as a Director who is or was an officer of the Corporation, such person in his capacity as an officer.)

15.3.4 Expenses. Expenses, including attorneys’ fees, incurred by a person indemnified pursuant to paragraph 15.3.1 in defending or otherwise being involved in a Proceeding shall be paid by the Corporation in advance of the final disposition of such Proceeding, including any appeal therefrom, upon receipt of an undertaking (the “Undertaking”) by or on behalf of such person to repay such amount if it shall ultimately be determined that he or she is not entitled to be indemnified by the Corporation; provided that in connection with a Proceeding (or part thereof) initiated by such person, except a Proceeding authorized by paragraph 15.3.5, the Corporation shall pay said expenses in advance of final disposition only if authorization for such Proceeding (or part thereof) was not denied by the Board of the Corporation prior to the earlier of 60 days after receipt of a request for such advancement accompanied by the Undertaking. A person to whom expenses are advanced pursuant hereto shall not be obligated to repay such expenses until the final determination of any pending Proceeding in a court of competent jurisdiction concerning the right of such person to be indemnified or the obligation of such person to repay such expenses.

15.3.5 Protection of Rights. If a claim by an Indemnified Person under paragraph 15.3.1 is not promptly paid in full by the Corporation after a written claim has been received by the Corporation or if expenses pursuant to paragraph 15.3.4 have not been promptly advanced after a written request for such advancement by an Indemnified Person (accompanied by the Undertaking required by paragraph 15.3.4) has been received by the Corporation, the claimant may at any time thereafter bring suit against the Corporation to recover the unpaid amount of the claim or the advancement of expenses. If successful, in whole or in part, in such suit, such claimant shall also be entitled to be paid the reasonable expense thereof. It shall be a defense to any such action (other than an action brought to enforce a claim for expenses incurred in defending any Proceeding in advance of its final disposition where the Undertaking has been tendered to the Corporation that indemnification of the claimant is prohibited by law, but the burden of proving such defense shall be on the Corporation. Neither the

failure of the Corporation (including the Board, independent legal counsel, or the Members) to have made a determination, if required, prior to the commencement of such action that indemnification of the claimant is proper in the circumstances, nor an actual determination by the Corporation (including the Board, independent legal counsel, or the Members) that indemnification of the claimant is prohibited, shall be a defense to the action or create a presumption that indemnification of the claimant is prohibited.

15.3.6 Miscellaneous.

(a) Non-Exclusivity of Rights. The rights conferred on any person by this Section 15.3 shall not be exclusive of any other rights which such person may have or hereafter acquire under any statute, provision of the Certificate of Incorporation, Bylaw, agreement, vote of Members or disinterested directors or otherwise. The Board shall have the authority, by resolution, to provide for such other indemnification of directors, and such indemnification of officers, delegates, employees, agents, or others of the Corporation as it shall deem appropriate.

(b) Insurance, contracts, and funding. The Corporation may maintain insurance, at its expense, to protect itself and any director, officer, employee, delegate or agent of the Corporation against any expenses, liabilities or losses, whether or not the Corporation would have the power to indemnify such person against such expenses, liabilities or losses under the DGCL. The Corporation may enter into contracts with any director, officer, or employee of the Corporation in furtherance of the provisions of this Section 15.3 and may create a trust fund, grant a security interest or use other means (including, without limitation, a letter of credit) to ensure the payment of such amounts as may be necessary to effect the advancing of expenses and indemnification as provided in such contracts or as otherwise provided in this Section 15.3.

(c) Contractual nature. The provisions of this Section 15.3 shall continue as to a person who has ceased to be a director and shall inure to the benefit of the heirs, executors and administrators of such person. This Section 15.3 shall be deemed to be a contract between the Corporation and each person who, at any time that this Section 15.3 is in effect, serves or agrees to serve in any capacity which entitles him to indemnification and advancement of expenses hereunder and any repeal or other modification of this Section 15.3 or any repeal or modification of the DGCL or any other applicable law shall not limit any rights of indemnification for Proceedings then existing or arising out of events, acts or omissions occurring prior to such repeal or modification, including, without limitation, the right to indemnification and advancement of expenses for Proceedings commenced after such repeal or modification to enforce this Section 15.3 with regard to Proceedings arising out of acts, omissions or events arising prior to such repeal or modification.

(d) Cooperation. Each Indemnified Person shall cooperate with the person, persons or entity making the determination with respect to such

Indemnified Person's entitlement to indemnification under this Section 15.3, including providing to such person, persons or entity upon reasonable advance request any documentation or information which is not privileged or otherwise protected from disclosure and which is reasonably available to such Indemnified Person and reasonably necessary to such determination. Any costs or expenses (including attorneys' fees and disbursements) incurred by such Indemnified Person in so cooperating with the person, persons or entity making such determination shall be borne by the Corporation (irrespective of the determination as to such Indemnified Person's entitlement to indemnification) and the Corporation hereby indemnifies and agrees to hold such Indemnified Person harmless therefrom.

(e) Subrogation. In the event of any payment under this Section 15.3 to an Indemnified Person, the Corporation shall be subrogated to the extent of such payment to all of the rights of recovery of such Indemnified Person, who shall execute all papers required and take all action necessary to secure such rights, including execution of such documents as are necessary to enable the Corporation to bring suit to enforce such rights.

(f) Severability. If this Section 15.3 or any portion hereof shall be invalidated or held to be unenforceable on any ground by any court of competent jurisdiction, the decision of which shall not have been reversed on appeal, this Section 15.3 shall be deemed to be modified to the minimum extent necessary to avoid a violation of law and, as so modified, this Section 15.3 and the remaining provisions hereof shall remain valid and enforceable in accordance with their terms to the fullest extent permitted by law.

ARTICLE XVI. TRANSITION

Section 16.1. Transition Standards. The Corporation will use the existing standards, criteria, rules or guides from each existing reliability council region for those Members that join the Corporation as in effect immediately prior to formation of the Corporation until such standards, criteria, rules or guides are adopted, superseded, or rejected by the Corporation. The Corporation will establish any necessary transition committees, subcommittees, working groups or task forces to administer the existing regional reliability standards, criteria, rules and guides until they are adopted, superseded, or rejected by the Corporation. The Corporation will employ its best efforts, within two (2) years of its formation, to work toward a uniform set of Reliability Standards for the entire Region. The Board will develop and implement a standards process and a plan for transition to new Reliability Standards. This process will include a requirement that two-thirds of the directors present at a meeting must vote to adopt new Reliability Standards.

ARTICLE XVII.
PARTICIPATION BY REGULATORY PARTICIPANTS

Section 17.1. Regulatory Participants. All Regulatory Participants shall be entitled to and be provided with the same rights to notice of and participation in meetings or other activities of the Corporation as are provided to Members, but shall not have the right to vote.

ARTICLE XVIII.
BUDGET AND BUSINESS PLAN

Section 18.1. Budget and Business Plan. Each annual budget and business plan of the Corporation shall be approved by the Board in sufficient time in each fiscal year to allow for timely submittal of the approved annual budget and business plan to NERC in accordance with the NERC Rules. The Corporation shall post a draft of each budget and business plan on the Corporation's website for purposes of review and comment by the Members at least ten (10) days prior to the Board meeting at which the budget and business plan are to be approved.

ARTICLE XIX.
AMENDMENT OF BYLAWS

Section 19.1. Amendment Of Bylaws. The power to adopt, amend or repeal these Bylaws is vested in the Members as set forth in Section 6.6.3 of these Bylaws; provided, however, that upon the passage of any federal electric reliability legislation, and/or the adoption of any rules or regulations of the Commission, NERC or other governmental entity with jurisdiction, the Board shall have authority to amend these Bylaws as necessary and appropriate to comply with such law, legislation, rules and regulations.



AMENDED AND RESTATED BYLAWS

OF

ReliabilityFirst Corporation

a Delaware nonprofit corporation

Adopted December 19, 2006

Amended September 21, 2007¹

Amended December 6, 2007²

Amended May 22, 2008³

Amended December 4, 2008⁴

[Amended December 1, 2011⁵](#)

¹ Section 5.9.2

² Sections 1.2, 1.26, 16.1

³ Sections 1.12, 7.13, 7.14

⁴ Sections 5.8, 6.8, 6.9, 6.10.2, 6.10.4, 7.4, 7.5, 7.7, 7.9, 7.11, 7.13

⁵ [Sections 1.24, 2.2, 6.8, 7.4, 7.7](#)

TABLE OF CONTENTS

ARTICLE I. DEFINITIONS	5
Section 1.1. Act.....	5
Section 1.2. Adjunct Member	5
Section 1.3. Affiliate	5
Section 1.4. Associate Member	5
Section 1.5. Board.....	5
Section 1.6. Bulk Power System.....	5
Section 1.7. Certificate of Incorporation.....	5
Section 1.8. Commission.....	6
Section 1.9. Delegation Agreement.....	6
Section 1.10. Electronic Transmission	6
Section 1.11. ERO	6
Section 1.12. Hearing Body..	6
Section 1.13. Industry Sector.....	6
Section 1.14. Large LSEs.....	6
Section 1.15. Medium LSEs.....	6
Section 1.16. Members.....	6
Section 1.17. NERC	6
Section 1.18. NERC Rules.....	7
Section 1.19. Net Energy for Load.....	7
Section 1.20. Person.....	7
Section 1.21. Region.....	7
Section 1.22. Regional Entity.....	7
Section 1.23. Regional Variance	7
Section 1.24. Regional Reliability Standard	7
Section 1.25. Regular Member	7
Section 1.26. Regulatory Participant	8
Section 1.27. Related Party	8
Section 1.28. Reliability Coordinator	8
Section 1.29. Reliability Standard	8
Section 1.30. Reliable Operation	8
Section 1.31. RTOs	8
Section 1.32. Small LSEs.....	8
Section 1.33. Suppliers.....	9
Section 1.34. Transmission Companies	9
ARTICLE II. PURPOSE AND ACTIVITIES	9
Section 2.1. Purpose.....	9
Section 2.2. Activities.....	9
Section 2.3. Not-for-Profit Corporation.....	10
ARTICLE III. POWERS	10
Section 3.1. Powers	10
ARTICLE IV. OFFICES	11
Section 4.1. Principal Office.....	11
ARTICLE V. MEMBERS	11

Section 5.1.	General	11
Section 5.2.	Classes of Members	11
5.2.1	Regular Members.....	11
5.2.2	Associate Members	11
5.2.3	Adjunct Members	11
Section 5.3.	Qualifications of Members	11
Section 5.4.	Admission of Members.....	11
Section 5.5.	Voting Rights.....	12
Section 5.6.	Transfer of Membership	12
Section 5.7.	Obligations of Members	12
Section 5.8.	Withdrawal.....	12
Section 5.9.	Funding and Dues.....	12
5.9.1	NERC Funding.....	12
5.9.2	Application Fee, User-Fees and Other Charges.....	13
Section 5.10.	Penalties	13
ARTICLE VI.	MEETING OF MEMBERS	13
Section 6.1.	Annual Meeting of Members	13
Section 6.2.	Special Meetings of Members.....	13
Section 6.3.	Location of Meetings of Members	14
Section 6.4.	Notice of Meetings	14
6.4.1	Notice Requirements	14
6.4.2	Waiver of Notice; Objections	14
Section 6.5.	Record Date	14
Section 6.6.	Right to Vote; Act of Members	15
6.6.1	Industry Sector Voting	15
6.6.2	Act of Members.....	15
6.6.3	Special Voting Requirements.....	15
Section 6.7.	Quorum	15
Section 6.8.	Action by Written Ballot	15
Section 6.9.	Action by Electronic Communication	16
Section 6.10.	Member Representatives; Proxies	16
6.10.1	Designation of Representative	16
6.10.2	Authorization	16
6.10.3	Effective Period.....	16
6.10.4	Revocation.....	16
Section 6.11.	Public Notice of Member Meetings.....	17
Section 6.12.	Posting of Minutes.....	17
Section 6.13.	Reimbursement of Member Expenses	17
ARTICLE VII.	BOARD OF DIRECTORS.....	17
Section 7.1.	General	17
Section 7.2.	Management of Corporation.....	17
Section 7.3.	Voting	18
Section 7.4.	Composition of the Board	18
Section 7.5.	Terms of Directors.....	19
Section 7.6.	Reimbursement	20
Section 7.7.	Resignations; Vacancies.....	20

Section 7.8.	Meetings; Notice; Waiver	21
Section 7.9.	Quorum	21
Section 7.10.	Board Action.....	21
Section 7.11.	Action Without a Meeting	21
Section 7.12.	Action by Electronic Communication	22
Section 7.13.	Board Committees	22
Section 7.14.	Hearing Body	22
7.14.1	Quorum	22
7.14.2	Voting	23
Section 7.15.	Public Notice of Board Meetings.....	23
Section 7.16.	Posting of Minutes ²³	
Section 7.17.	Compensation of Directors	23
ARTICLE VIII.	ORGANIZATIONAL GROUPS.....	23
Section 8.1.	Establishment of Organizational Groups.....	23
Section 8.2.	Reimbursement	24
ARTICLE IX.	OFFICERS	24
Section 9.1.	Officers.....	24
Section 9.2.	Election and Term of Office	24
Section 9.3.	Removal.....	24
Section 9.4.	Vacancies	24
Section 9.5.	President.....	24
Section 9.6.	Vice Presidents.....	24
Section 9.7.	Secretary	25
Section 9.8.	Treasurer	25
ARTICLE X.	CERTIFICATES OF MEMBERSHIP	25
Section 10.1.	Certificates of Membership.....	25
ARTICLE XI.	BOOKS AND RECORDS.....	26
Section 11.1.	Books and Records; Financial Statements	26
ARTICLE XII.	FISCAL YEAR	26
Section 12.1.	Fiscal Year.....	26
ARTICLE XIII.	TRANSFER OF ASSETS	26
Section 13.1.	Member Approval Not Required	26
Section 13.2.	Member Approval Required.....	26
ARTICLE XIV.	CONTRACTS, CHECKS, DEPOSITS, AND GIFTS	27
Section 14.1.	Contracts	27
Section 14.2.	Checks, Drafts, or Orders	27
Section 14.3.	Deposits.....	27
Section 14.4.	Gifts	27
ARTICLE XV.	INSURANCE, LIMITATION ON LIABILITY AND INDEMNIFICATION	27
Section 15.1.	Insurance	27
Section 15.2.	Limitations on Liability	27
Section 15.3.	Right to Indemnification.....	27
15.3.1	Indemnified Persons	27

15.3.2	Denial of Authorization for Certain Proceedings	28
15.3.3	Certain Defined Terms	28
15.3.4	Expenses	28
15.3.5	Protection of Rights.....	29
15.3.6	Miscellaneous	29
ARTICLE XVI. TRANSITION.....		30
Section 16.1.	Transition Standards.....	30
ARTICLE XVII. PARTICIPATION BY REGULATORY PARTICIPANTS.....		31
Section 17.1.	Regulatory Participants	31
ARTICLE XVIII. BUDGET AND BUSINESS PLAN		31
Section 18.1.	Budget and Business Plan.....	31
ARTICLE XIX. AMENDMENT OF BYLAWS.....		31
Section 19.1.	Amendment Of Bylaws.....	31

**AMENDED AND RESTATED
BYLAWS OF
ReliabilityFirst Corporation
a Delaware nonprofit corporation
(the “Corporation”)**

[As adopted by the Members on December 19, 2006,
amended by the Board of Directors on September 21, 2007,
amended by the Members on December 6, 2007,
amended by the Board of Directors on May 22, 2008,
~~and~~ amended by the Members on December 4, 2008,
and amended by the Members on December 1, 2011]

**ARTICLE I.
DEFINITIONS**

Section 1.1. Act. “Act” shall mean Section 215 of the Federal Power Act (16 U.S.C. §824n).

Section 1.2. Adjunct Member. “Adjunct Member” shall mean any entity that does not qualify to join an Industry Sector but has been approved for membership. Adjunct Members may include Regulatory Participants.

Section 1.3. Affiliate. “Affiliate” shall mean, with respect to any entity, any other entity that, directly or indirectly, through one or more intermediaries, controls, or is controlled by, or is under common control with, such entity, as determined in the sole discretion of the Board of the Corporation. For this purpose, “control” may be presumed by the direct or indirect ownership of ten percent (10%) or more of the outstanding voting capital stock or other equity interests having ordinary voting power.

Section 1.4. Associate Member. “Associate Member” shall mean any entity that has joined an Industry Sector and is an Affiliate or Related Party of a Regular Member.

Section 1.5. Board. “Board” shall mean the Board of Directors of the Corporation.

Section 1.6. Bulk Power System. “Bulk Power System” shall mean facilities and control systems necessary for operating an interconnected electric energy transmission network (or any portion thereof) and electric energy from generation facilities needed to maintain transmission system reliability, but does not include facilities used in the local distribution of electricity.

Section 1.7. Certificate of Incorporation. “Certificate of Incorporation” shall mean the Certificate of Incorporation of the Corporation filed with the Delaware Secretary of State, as from time to time amended.

Section 1.8. Commission. “Commission” shall mean the Federal Energy Regulatory Commission.

Section 1.9. Delegation Agreement. “Delegation Agreement” shall mean the delegation agreement, as supplemented or amended from time to time, between NERC and the Corporation pursuant to which NERC has delegated its authority to the Corporation to propose and enforce Reliability Standards within the Region.

Section 1.10. Electronic Transmission. “Electronic transmission” shall mean any form of communication, not directly involving the physical transmission of paper, that creates a record that may be retained, retrieved and reviewed by a recipient thereof, and that may be directly reproduced in paper form by such a recipient through an automated process.

Section 1.11. ERO. “ERO” shall mean the electric reliability organization established under the Act to enforce Reliability Standards applicable to all owners, operators and users of the Bulk Power System in North America.

Section 1.12. Hearing Body. “Hearing Body” shall mean a group established with authority to conduct and render decisions in a formal compliance hearing of an entity registered in the NERC compliance registry who is the subject of a notice of alleged violation, proposed penalty or sanction, contested mitigation plan or contested remedial action directive.

Section 1.13. Industry Sector. “Industry Sector” shall mean a group of Bulk Power System owners, operators or users in the Region with substantially similar interests as pertinent to the purposes and operations of the Corporation of the Bulk Power System. The Industry Sectors shall consist of the following: (1) Suppliers, (2) Transmission Companies, (3) RTOs, (4) Small LSEs, (5) Medium LSEs, and (6) Large LSEs.

Section 1.14. Large LSEs. “Large LSEs” shall mean entities that serve, or whose Related Parties serve, end use load with annual energy delivery to such load in the Region of 50,000 GWh or greater.

Section 1.15. Medium LSEs. “Medium LSEs” shall mean entities that serve, or whose Related Parties serve, end use load with annual energy delivery to such load in the Region between 10,000 GWh and 50,000 GWh.

Section 1.16. Members. “Members” shall mean Regular Members, Associate Members and Adjunct Members.

Section 1.17. NERC. “NERC” shall mean the North American Electric Reliability Corporation, or any successor entity, which has been certified by the Commission as the ERO pursuant to the Act to establish and enforce Reliability Standards for the Bulk Power System.

Section 1.18. NERC Rules. “NERC Rules” shall mean the NERC Rules of Procedure as approved by the Commission.

Section 1.19. Net Energy for Load. “Net Energy for Load” shall mean net generation of an electric system plus energy received from others less energy delivered to others through interchange. It includes system losses, but excludes energy required for storage of energy at energy storage facilities. Calculations of net energy for load for all purposes under these Bylaws shall be based on the most recent calendar year for which data on net energy for load of the Region is available.

Section 1.20. Person. “Person” shall mean a natural person, corporation, cooperative, partnership, association, or other private or public entity.

Section 1.21. Region. “Region” shall mean the geographic boundaries of the Corporation described in the Delegation Agreement.

Section 1.22. Regional Entity. “Regional Entity” shall mean any entity with which NERC has entered into a delegation agreement to delegate, or which the Commission or a governmental authority in Canada or Mexico has directly assigned, enforcement authority for reliability standards for the Bulk Power System in a defined geographic area of North America.

Section 1.23. Regional Variance. “Regional Variance” shall mean an aspect of a Reliability Standard that applies only within a particular Regional Entity or group of Regional Entities. A Regional Variance may be used to qualify how a particular Regional Entity or Regional Entities achieves the objectives of a Reliability Standard or may establish different measures or performance criteria as necessary to achieve reliability within the particular Regional Entity or group of Regional Entities. A Regional Variance may not be inconsistent with any Reliability Standard as it would otherwise exist without the Regional Variance. Such a Regional Variance may be proposed by a Regional Entity and, if adopted by NERC and approved by the Commission, shall be enforced within the applicable Regional Entity or Regional Entities pursuant to delegated authority.

Section 1.24. Regional Reliability Standard. “Regional Reliability Standard” shall mean a type of Reliability Standard that is applicable only within a particular Regional Entity or group of Regional Entities. A Regional Reliability Standard may augment, add detail to, or implement another Reliability Standard or cover matters not addressed by other Reliability Standards. A Regional Reliability Standard is not binding upon any Member or Registered Entity, nor is it effective or enforceable, until the Regional Reliability Standard has been s, upon adoption adopted by NERC and approval approved by the Commission; ~~shall be as a Reliability Standard~~ ~~s and shall be enforced~~ within the applicable Regional Entity or Regional Entities pursuant to delegated authorities.

Section 1.25. Regular Member. “Regular Member” shall mean any entity that has joined an Industry Sector that either (i) has no Affiliates or Related Parties that are

Members or (ii) is the entity designated to be the Regular Member by any related group of Associate Members.

Section 1.26. Regulatory Participant. “Regulatory Participant” shall mean any state, District of Columbia or any provincial regulatory agency in the Region exercising authority over the rates, terms or conditions of electric service of an entity other than itself within the Region, or the planning, siting, construction or operation of electric facilities of an entity other than itself within the Region, as well as the Commission, regional advisory bodies that may be established by the Commission, or any federal regulator or agency or any entity authorized by any state, the District of Columbia or any province to represent utility consumers.

Section 1.27. Related Party. “Related Party” shall mean, solely for purposes of the governance provisions of these Bylaws, any entity that is registered as part of another entity or is registered for other entities in the NERC Compliance Registry. For purposes of these Bylaws, a representative of a state or federal government agency shall not be deemed a Related Party with respect to each other, and a public body’s regulatory authority, if any, over a Member shall not be deemed to make it a Related Party with respect to that Member.

Section 1.28. Reliability Coordinator. “Reliability Coordinator” shall mean any entity that is recognized as a reliability coordinator by NERC in the Region that does not otherwise qualify as a Transmission Company or RTO.

Section 1.29. Reliability Standard. “Reliability Standard” shall mean a requirement to provide for Reliable Operation of the Bulk Power System, including, without limitation, the foregoing requirements for the operation of existing Bulk Power System facilities, including cyber security protection, and the design of planned additions or modifications to such facilities to the extent necessary for reliable operation of the Bulk Power System, but shall not include any requirement to enlarge Bulk Power System facilities or to construct new transmission capacity or generation capacity.

Section 1.30. Reliable Operation. “Reliable Operation” shall mean operating the elements of the Bulk Power System within equipment and electric system thermal, voltage and stability limits so that instability, uncontrolled separation, or cascading failure of the Bulk Power System will not occur as a result of a sudden disturbance, including a cyber security incident, or unanticipated failure of system elements.

Section 1.31. RTOs. “RTOs” shall mean PJM Interconnection L.L.C. and Midwest Independent Transmission System Operator, Inc., or such other entity that has been recognized by the Commission as a regional transmission operator or recognized functional equivalent in the Region.

Section 1.32. Small LSEs. “Small LSEs” shall mean (i) owners or operators of entities (or their representatives) that serve, or whose Related Parties serve, end use load with annual energy delivery to such load in the Region of 10,000 GWh or less, and

(ii) end-use customers interconnected with the Bulk Power System with load of at least 100 MW at one location in the Region.

Section 1.33. Suppliers. “Suppliers” shall mean owners or operators of electric generation connected to the transmission system and wholesale power marketers in the Region.

Section 1.34. Transmission Companies. “Transmission companies” shall mean (i) owners (or those with ownership entitlement), planners and operators of transmission facilities included in the Bulk Power System in the Region and (ii) Reliability Coordinators.

ARTICLE II. PURPOSE AND ACTIVITIES

Section 2.1. Purpose. The business or purposes to be conducted or promoted by the Corporation are:

- (a) to be a Regional Entity and exercise enforcement authority for Reliability Standards for the Bulk Power System in the Region pursuant to the Delegation Agreement;
- (b) to carry out certain of NERC’s activities that are in furtherance of NERC’s responsibilities as the ERO under the Act or in support of delegated functions, as specified in the NERC Rules or the Delegation Agreement; and
- (c) to engage in any other lawful act or activity for which not for profit corporations may be organized under the Delaware General Corporation Law.

The Corporation shall be exempt from federal income taxation pursuant to Section 501(c) of the Internal Revenue Code of 1986, as amended (hereinafter the “Code”) as an organization described in Section 501(c)(6) of the Code. The Corporation shall not engage directly or indirectly in any activity which would invalidate its status as an organization exempt from taxation under Section 501(a) of the Code as an organization described in Section 501(c)(6) of the Code. No part of the net income to the Corporation shall inure to the benefit of or be distributed to its directors, officers, members or other private persons, except that the Corporation shall be authorized and empowered to pay reasonable compensation for services actually rendered.

Section 2.2. Activities. In support and furtherance of its purpose, and in accordance with and at all times subject to the NERC Rules and the Delegation Agreement, the Corporation’s responsibilities shall include, but not be limited to, the following:

- (a) Reliability Standards. The Corporation shall:

(1) propose Reliability Standards, Regional Variances or modifications thereof to NERC; and

(2) develop Regional Reliability Standards through the Corporation's standards development procedure.

(b) Enforcement. The Corporation shall enforce Reliability Standards (including ~~Regional Reliability Standards and~~ Regional Variances) within the Region through the Corporation's compliance enforcement program.

(c) Delegation-Related Services. The Corporation, on behalf of NERC, shall carry out certain of NERC's activities that are in furtherance of NERC's responsibilities as the ERO under the Act or in support of delegated functions, including:

- (1) Organization registration and certification.
- (2) Reliability readiness audit and improvement.
- (3) Reliability assessment and performance analysis.
- (4) Training and education.
- (5) Situational awareness and infrastructure security.

(d) Budget. The Corporation shall prepare and submit a budget to NERC for the amount of costs the Corporation will incur in support of delegated functions that are in furtherance of NERC's responsibilities as the ERO under the Act.

(e) Non-delegated Functions. The Corporation may conduct such other activities for or on behalf of the Members that are not delegated to the Corporation by NERC under the Delegation Agreement if authorized by the Board and not inconsistent with the Act, NERC Rules, the Delegation Agreement or these Bylaws.

Section 2.3. Not-for-Profit Corporation. The Corporation is operated as a Delaware non-stock nonprofit corporation and is organized pursuant to the general corporation law of the State of Delaware.

ARTICLE III. POWERS

Section 3.1. Powers. The Corporation shall have the power to engage in any lawful act or activity for which corporations may be organized under the general corporation law of the State of Delaware, subject to any limitations provided in applicable federal, provincial or state law or in the Certificate of Incorporation or these Bylaws.

ARTICLE IV. OFFICES

Section 4.1. Principal Office. The principal office of the Corporation shall be located initially within the Region, at such location as the Board may from time to time determine, giving consideration to the total cost to the Corporation and convenience of travel for staff, Members and Regulatory Participants. Once established, the principal office may remain in its location, even if outside the Region.

ARTICLE V. MEMBERS

Section 5.1. General. The terms and conditions of membership in the Corporation shall be as provided in the Certificate of Incorporation and these Bylaws if not inconsistent therewith. All Regular Members and Associate Members shall be required to join a single Industry Sector.

Section 5.2. Classes of Members. The Corporation shall have three (3) classes of Members: Regular Members, Associate Members and Adjunct Members.

5.2.1 Regular Members. Except as set forth in Sections 5.5 and 6.5 of these Bylaws, Regular Members shall have the right to vote on all matters within their Industry Sector. Regular Members shall have all the rights and obligations of being a Member in the Corporation.

5.2.2 Associate Members. Associate Members shall not be entitled to vote within their Industry Sector or for any other purpose as a Member. Associate Members shall otherwise have all the rights and obligations of being a Member in the Corporation.

5.2.3 Adjunct Members. Adjunct Members shall not be entitled to vote for any purpose as a Member. Adjunct Members shall otherwise have all the rights of being a Member in the Corporation.

Section 5.3. Qualifications of Members. Any entity eligible to join an Industry Sector may be a Regular Member or Associate Member of the Corporation. Any entity not eligible to join an Industry Sector may be an Adjunct Member of the Corporation.

Section 5.4. Admission of Members. New Members may join the Corporation upon submittal of an application, in a form approved by the Board, and upon payment of such fees or charges, if any, as may be established by the Board or required by NERC. Each Regular Member and Associate Member shall designate the Industry Sector it wishes to join. A Regular Member and Associate Member may change its Industry Sector designation once each calendar year upon notice to the Corporation. Such notice must be provided to the Secretary of the Corporation at least sixty (60) days before an annual or other meeting of Members if the change is to be effective for such meeting. The President shall review a membership application and may request demonstration by the applicant that it qualifies for membership in a particular Industry Sector. Any dispute with respect to a Regular Member's or Associate Member's

qualifications for a particular Industry Sector shall be resolved by the Board. The President shall have authority to approve an application for membership, subject to review by the Board.

Section 5.5. Voting Rights. Each Regular Member in good standing shall be entitled to one vote in the Industry Sector in which it belongs on all matters submitted to a vote of Members. The Board may suspend voting rights for a Regular Member delinquent by more than 60 days in payment of any penalties or because of the Regular Member's failure to meet other obligations to the Corporation. Except with respect to the election of Industry Sector directors as described elsewhere in the Certificate of Incorporation and these Bylaws, matters properly brought before the Members at an annual or special meeting shall be acted upon by the Industry Sectors voting together as a single class. The vote of each Industry Sector shall be split into an affirmative component based on votes for the matter(s) presented, and a negative component based on votes against the matter(s) presented, in direct proportion to the votes cast within the Industry Sector for and against the matter presented, rounded to two decimal places. If authorized in advance by the Board, voting may be held electronically under such terms and conditions as are approved by the Board.

Section 5.6. Transfer of Membership. A Member of the Corporation may not transfer its membership or a right arising from it except to any Person succeeding to all or substantially all of the assets of the Member. If challenged, the President shall have authority to approve any such transfer, subject to review by the Board.

Section 5.7. Obligations of Members. By applying for and becoming a Regular or Associate Member of the Corporation, each Member agrees to comply with all Reliability Standards, all NERC standards and requirements, and the other obligations of Members of the Corporation set forth in these Bylaws or duly adopted by the Board in order to achieve the purposes of the Corporation. A Regular or Associate Member also agrees to obligate all of its Affiliates that have an impact on reliability in the Region to comply with all Reliability Standards and NERC standards and requirements. These obligations include but are not limited to: (a) obligations to provide data and information needed to perform the functions of the Corporation, (b) payment of any authorized penalties resulting from non-compliance with Reliability Standards, (c) in the case of Regular Members, electing the Board, and (d) providing qualified candidates to serve on organizational working groups. Adjunct Members agree to provide data and information needed to perform the functions of the Corporation.

Section 5.8. Withdrawal. A Member may withdraw from participation in the Corporation upon notice given in writing or by electronic transmission to the Corporation. Such notice shall specify a date, not earlier than thirty (30) days from the date of notice, on which the withdrawal shall become effective.

Section 5.9. Funding and Dues.

5.9.1 NERC Funding. In accordance with and at all times subject to the NERC Rules and the Delegation Agreement, the Corporation shall equitably allocate its dues,

fees and other charges for the delegated functions conducted by the Corporation among all end users. The Corporation shall submit to NERC annually a list of all load-serving entities within the Region. NERC will bill all load-serving entities in the Region for the Corporation's costs for the delegated functions based on Net Energy for Load and be responsible for collection.

5.9.2 Application Fee, User-Fees and Other Charges. The Corporation may charge a nominal fee, which shall be determined by the President, for the submission of applications for membership. The Board of Directors may from time to time fix the amount of user-fees or other charges, if any, for activities that are not delegated to the Corporation by NERC under the Delegation Agreement and determine the methods of collection from entities that choose to participate in such activities.

Section 5.10. Penalties. If the Corporation initiates an investigation that leads to the imposition of a penalty, the Corporation shall receive any penalty monies that results from the investigation. All monies which the Corporation collects from the issuance of penalties shall be applied as a general offset to the Corporation's budget requirements for the subsequent fiscal year. Funds from financial penalties shall not be directly applied to any program maintained by the Corporation.

ARTICLE VI. MEETING OF MEMBERS

Section 6.1. Annual Meeting of Members. The Members shall hold an annual meeting in December of each year, or at such other time specified by the Board. At the annual meeting of Members: (i) each Industry Sector shall elect the successor(s), if any, for any director(s) from their Industry Sector whose term will expire before the next annual meeting of the Members, provided however, that any Industry Sector may elect a successor director representing such Industry Sector prior to such annual meeting, in accordance with the provisions of this Article VI, in which case the election of such succeeding director(s) shall be reported to the Corporation at such annual meeting; (ii) the President and Treasurer shall report on the activities and financial condition of the Corporation; (iii) the Industry Sectors shall elect a slate of at-large and independent directors to fill vacancies or expiring terms; and (iv) the Industry Sectors shall consider and act upon such other matters as are consistent with the notice of the annual meeting. The failure to hold an annual meeting in accordance with these Bylaws shall not affect the validity of a corporate action.

Section 6.2. Special Meetings of Members. Special meetings of the Members may be called by six (6) directors on the Board, by the President, or by Members if at least ten percent (10%) of the Regular Members sign, date, and deliver to the President one or more written demands for a special meeting describing the purpose for which it is to be held. Within fifteen (15) days after receipt of a demand for a special meeting from Regular Members, the President shall cause a special meeting to be called and held on notice in accordance with Section 6.4 of these Bylaws. If the President fails to cause a special meeting to be called and held as required by this Section 6.2, a Regular Member making the demand may call the meeting by giving notice under Section 6.4.

In either event, notice of the meeting and the costs of the meeting shall be at the expense of the Corporation. The business transacted at a special meeting is limited to the purposes stated within the notice of the meeting. Business transacted at a special meeting that is not included in those stated purposes is voidable by or on behalf of the Corporation, unless ninety percent (90%) of the Regular Members entitled to vote were present at such meeting or have waived notice of the meeting under Section 6.4.

Section 6.3. Location of Meetings of Members. Meetings of Members shall be held at a location designated by the President or the Board. If a Regular Member calls a meeting pursuant to Section 6.2, the Regular Members making the demand for the meeting may designate the location, provided the meeting must be held within the Region and in a facility of appropriate size to accommodate the Members.

Section 6.4. Notice of Meetings.

6.4.1 Notice Requirements. Notice of meetings of Members must be given at least five (5) days before the date of a meeting and not more than sixty (60) days before the date of a meeting. The notice must contain the date, time and place of the meeting, instructions for electronic attendance or voting, if applicable, and an agenda of the matters upon which action may be taken at the meeting. A matter may be added to the agenda of a meeting at the meeting upon the affirmative vote of three-quarters (3/4) of the Industry Sector votes cast on a motion to amend the agenda. If the meeting is an adjourned meeting and the date, time and place of the meeting were announced at the time of the adjournment, notice is not required unless a new record date for the adjourned meeting is or must be fixed. Notice shall be deemed given by the Corporation to the Members when (a) posted on the Corporation's public website in a reasonably prominent location, and (b) sent by mail, facsimile or reputable overnight delivery service or by electronic transmission to each Member's representative authorized pursuant to Section 6.10.1

6.4.2 Waiver of Notice; Objections. A Member may waive notice of a meeting of Members. A waiver of notice by a Member entitled to notice is effective whether given before, at, or after the meeting, and whether given in writing, or by attendance. Attendance by a Member at a meeting is a waiver of notice of that meeting, unless the Member objects at the beginning of the meeting to the transaction of business because the meeting is not lawfully called or convened, or objects before a vote on an item of business because the item may not lawfully be considered at that meeting and does not participate in the consideration of the item at that meeting.

Section 6.5. Record Date. The Board may fix a date not more than sixty (60) days before the date of a meeting of Members as the date for the determination of the Members entitled to notice of and entitled to vote at the meeting. When a date is so fixed, only Members on that date are entitled to notice and to vote at the meeting unless the Board fixes a new date for determining the right to notice and to vote, which it must do if the meeting is adjourned to a date more than sixty (60) days after the record date for determining Members entitled to notice of the original meeting.

Section 6.6. Right to Vote; Act of Members.

6.6.1 Industry Sector Voting. Voting of the Members shall be by Industry Sector, with each Industry Sector entitled to cast one vote. Each Member entitled to vote in an Industry Sector shall be entitled to cast one vote in its Industry Sector. The vote of each Industry Sector shall be split into an affirmative component based on votes for the pending motion, and a negative component based on votes against the pending motion, in direct proportion to the votes cast within the Industry Sector for and against the pending motion, rounded to two decimal places. To the extent practicable, all Member votes may be held electronically under such terms and conditions as are approved by the Board.

6.6.2 Act of Members. If a quorum is present, except with respect to any matter described in Section 6.6.3, a majority of the Industry Sector votes cast on the matter shall be the act of the Members.

6.6.3 Special Voting Requirements. Notwithstanding any other provision of these Bylaws, and except as set forth in the Certificate of Incorporation and Section 13.2 of these Bylaws, two-thirds (2/3) of the Industry Sector votes cast shall be required to:

(a) Amend the Bylaws, except as otherwise provided in Section 19.1 of these Bylaws. The substance of the proposed amendment must be contained in the notice of the meeting at which the vote will be taken; however, the Members may modify a proposed Bylaw amendment at the meeting.

(b) Approve any proposal to terminate the Corporation.

Section 6.7. Quorum. A quorum for a meeting of Members is a majority of the Regular Members entitled to vote in each Industry Sector at the meeting. A quorum for a meeting of an Industry Sector is a majority of the Regular Members of that Industry Sector entitled to vote at the meeting. In both cases, electronic participation is acceptable if authorized by the Board. A quorum is necessary for the transaction of business at a meeting of Members or of any Industry Sector. If a quorum is not present, a meeting may be adjourned for that reason by the Industry Sectors or Regular Members then represented or present.

Section 6.8. Action by [Written Ballot](#). All elections of directors shall be by written ballot. ~~Any other action that may be taken at a regular or special meeting of Members or any Industry Sector may be taken without a meeting or during a meeting if the Corporation mails or delivers a written ballot to every Regular Member entitled to vote on the matter. Approval by written ballot is valid only when the number of votes cast by ballot equals or exceeds the quorum required to be present at a meeting authorizing the action, and the number of approvals equals or exceeds the number of votes that would be required to approve the matter at a meeting at which the total number of votes cast was the same as the number of votes cast by ballot. Solicitations for votes by written ballot must: (i) indicate the number of responses needed to meet the~~

~~quorum requirements; (ii) state the percentage of approvals necessary to approve the matter; (iii) specify the time by which a ballot must be received by the Corporation in order to be counted; and (iv) may not be revoked once received. If authorized by the Board, t~~

The requirement of a written ballot shall be satisfied by a ballot submitted by electronic transmission provided that any such electronic transmission must either set forth or be submitted with information from which it can be determined that the electronic transmission was authorized by the Member.

Section 6.9. Action by Electronic Communication. A conference among Members by a means of communication through which the participants may simultaneously hear each other during the conference is a meeting of the Members, if the same notice is given of the conference as would be required for a meeting and if the number of persons participating in the conference is a quorum. Participation in a meeting by this means is personal presence at the meeting. A Member may participate in a meeting of the Members by a means of communication through which the Member, other persons participating, and all persons physically present at the meeting may simultaneously communicate with each other during the meeting. Participation in a meeting by this means constitutes personal presence at the meeting.

Section 6.10. Member Representatives; Proxies.

6.10.1 Designation of Representative. Each year prior to the annual meeting of Members, each Regular Member shall designate the individual authorized to vote on Corporation matters on behalf of the Member, in accordance with procedures approved by the Board. A Regular Member may change such designation at any time by providing at least twenty-four (24) hour written notice to the Secretary of the Corporation. Such notice may be provided by electronic transmission.

6.10.2 Authorization. The individual designated to vote by a Regular Member may appoint a proxy to vote or otherwise act for the Regular Member at any meeting by signing an appointment form either personally or by an attorney so designated by the Regular Member. Such authorization may be in writing or by means of electronic transmission to the person who will be the holder of the proxy, provided that such electronic transmission must either set forth or be submitted with information from which it can be determined that the electronic transmission was authorized by the Member representative.

6.10.3 Effective Period. An appointment of a proxy is effective when received by the Secretary or other officer or agent authorized to tabulate votes. An appointment is valid for the next regular or specially scheduled meeting or ballot by electronic transmission. However, a proxy is not valid for more than sixty (60) days from its date of execution.

6.10.4 Revocation. An appointment of a proxy is revocable by a Regular Member. Appointment of a proxy is revoked by the person appointing the proxy either by open declaration at a meeting or by signing and delivering a revocation in writing or by electronic transmission to the Secretary or other officer or agent authorized to

tabulate proxy votes. This may be done either in a statement that the appointment of the proxy is revoked or by a subsequent appointment that shall serve to cancel all prior proxies.

Section 6.11. Public Notice of Member Meetings. Notice to the public of the dates, times and places of meetings of the Members, and all nonconfidential material provided to the Members, shall be posted on the Corporation's website at approximately the same time that notice is given to the Members. Meetings of the Members shall be open to the public, subject to reasonable limitations due to the availability and size of meeting facilities; provided, that the meeting may be held in or adjourn to closed session to discuss matters of a confidential nature, including, but not limited to, personnel matters, compliance and enforcement matters, litigation or commercially sensitive or critical infrastructure information of a Member or other Person.

Section 6.12. Posting of Minutes. Minutes of meetings of Members shall be posted on the Corporation's website when available.

Section 6.13. Reimbursement of Member Expenses. The Corporation will be under no obligation to reimburse Members for expenses associated with their attendance at regular or special Member meetings.

ARTICLE VII. BOARD OF DIRECTORS

Section 7.1. General. The composition of the Board and the terms of office of the directors, the manner of their nomination, election or appointment, and other terms and conditions of their service, shall be as provided in the Certificate of Incorporation and these Bylaws if not inconsistent therewith.

Section 7.2. Management of Corporation. The business of the Corporation shall be managed under the direction of the Board. Specific functions of the Board shall include, but not be limited to:

- (a) govern the Corporation and oversee all of its activities;
- (b) establish and oversee all organizational groups;
- (c) approve, revise and enforce Reliability Standards utilizing a fair, open, balanced and inclusive process;
- (d) establish compliance monitoring procedures and requirements, and penalties and sanctions for non-compliance consistent with applicable NERC Rules;
- (e) impose penalties and sanctions consistent with the NERC Rules and the procedures approved by the Board;

- (f) establish and approve an annual budget for submission to NERC;
- (g) hire the Corporation's president and approve his or her salary;
- (h) annually at the first regular Board meeting following the annual meeting of Members, elect a Chair ("Chair") and a vice-chair from among the directors on the Board; and
- (i) establish Board committees as appropriate.

Section 7.3. Voting. Each director shall have one vote with respect to decisions of the Board.

Section 7.4. Composition of the Board.

(a) The Board shall consist of fourteen (14) or fifteen (15) directors which number shall be established from time to time by resolution of the Board, which resolution shall in no event have the effect of terminating the term of any incumbent director.

(b) Eight directors shall be elected by the Industry Sectors as follows:

- (i) Suppliers shall elect two (2) directors;
- (ii) Transmission Companies shall elect two (2) directors;
- (iii) RTOs shall select one (1) director;
- (iv) Small LSEs shall elect one (1) director;
- (v) Medium LSEs shall elect one (1) director; and
- (vi) Large LSEs shall elect one (1) director.

(c) Three (3) directors shall be at-large. At-large directors shall be elected by all of the Industry Sectors voting together as a single class.

(d) Three (3) directors, if the Board consists of fourteen (14) directors, and four (4) directors, if the Board consists of fifteen (15) directors, shall be independent from the Corporation and any Member or any Affiliate or Related Party of any Member. Independent directors shall be elected by all of the Industry Sectors voting together as a single class.

(e) Industry Sectors shall elect their respective sector and at-large directors from among individuals holding senior management positions in Member organizations. Any sector-elected or at-large director whose Member organization changes Industry Sectors or who ceases to hold a senior management position in a Member organization shall continue to serve out his or her remaining term, unless such director resigns or is removed. ~~When selecting~~

~~at-large directors, Industry Sectors shall consider such factors as the geographic and functional representation of the Board.~~ No two directors may be employees of a single Member or any Affiliate or Related Party of a Member or any Affiliate.

(f) An independent director is a person (i) who is not an officer or employee of the Corporation, an officer, director, or employee of a Member, or an officer, director or employee of any entity that would reasonably be perceived as having a direct financial interest in the outcome the Board's decisions, or (ii) who does not have a relationship that would interfere with the exercise of independent judgment in carry out the responsibilities of a director. The Board may adopt additional standards for director independence not inconsistent herewith.

(g) At-large and independent directors shall be nominated by the nominating and governance committee of the Board. When nominating at-large directors, the nominating and governance committee shall consider such factors as the geographic and functional representation of the Board. The nominating and governance committee shall seek out for nomination independent directors from diverse backgrounds, who will contribute to the effective functioning of the Board and the Corporation by bringing a broad range of industry expertise, viewpoints, experiences, skill sets and knowledge. If an incumbent independent director is not re-nominated, the nominating and governance committee will use reasonable efforts to ensure that diverse candidates are in the pool of potential nominees for the open independent director position and may retain an independent consultant to identify individuals qualified and willing to serve as an independent director.

(h) Any director which the full Board has determined has a conflict of interest on any compliance or enforcement matter brought before the Board shall not vote on such matter and shall recuse himself or herself from all Board deliberations concerning such matter.

(i) There will be no alternates or proxies for directors.

Section 7.5. Terms of Directors. The directors will be divided into three classes. The number of directors in each class shall be as nearly equal as possible. The term of office of the first class will expire at the second annual meeting of Members; the term of office of the second class will expire one year thereafter; and the term of office of the third class two years thereafter. At each annual meeting of Members, directors shall be chosen for a three year term to succeed those whose term expires. No two at-large directors and no two directors of the same Industry Sector shall be in the same class. At least one (1) independent director shall be in each class. Each director shall hold office until (a) the expiration of the term for which he or she was elected and until his or her successor is elected and qualified, or (b) his or her earlier death, resignation or removal. Any director may be removed at any time by the affirmative vote of two-thirds of the Industry Sector or Industry Sectors, as applicable, electing such director. A director may be removed by the Board for non-attendance at three consecutive Board meetings.

Section 7.6. Reimbursement. Independent directors shall have the right to reimbursement by the Corporation of their actual reasonable travel expenses to Board meetings or when specifically selected to represent the Corporation at a business meeting. The directors elected by the Industry Sectors and the at-large directors shall not be reimbursed by the Corporation for any expenses, unless specifically approved in advance by resolution of the Board.

Section 7.7. Resignations; Vacancies.

(a) Resignations. A director may resign ~~at any time~~ from the Board upon notice given in writing or by electronic transmission to the Corporation. Such resignation shall take effect at the time identified in the notice as the effective date of resignation~~of its receipt by the Corporation~~.

(b) Vacancies. If a notice of resignation provides that the effective date of resignation will occur on a future date within an unexpired term, the Industry Sector or Industry Sectors, as applicable, may elect a successor director to fill the impending vacancy prior to the effective date of the resignation, in accordance with the procedures and requirements set forth above. The successor director elected by the Industry Sector or Industry Sectors, as applicable, shall commence on the effective date of the resigning director's resignation and hold office for the unexpired term of the vacated directorship replaced.

If a successor Industry Sector or at-large director is not elected prior to the resignation effective date, or if~~if~~ an Industry Sector or at-large director resigns, dies or otherwise becomes incapacitated or is removed during the term of office for which elected, the directorship shall thereupon be vacant and shall be filled by the Industry Sector or Industry Sectors, as applicable, by written or electronic ballot in accordance with the procedures and requirements set forth above. The successor director elected by the Industry Sector or Industry Sectors, as applicable, shall hold office for the unexpired term of the vacated directorship replaced.

If a successor independent director is not elected prior to the resignation effective date, or if an independent director resigns, dies or otherwise becomes incapacitated or is removed during the term of office for which elected or ceases to be independent, as determined by the Board, his or her directorship shall thereupon be vacant and may be filled by resolution of the Board and any independent director so chosen shall hold office until the next annual meeting of Members, at which time a permanent successor shall be elected by the Industry Sectors for the remainder of the unexpired term. Upon an increase in the number of directors on the Board in accordance with Section 7.4(a) of these Bylaws, the independent directorship created thereby may be filled by resolution of the Board and any independent director so chosen shall hold office until the next annual meeting of Members, at which time a permanent successor shall be elected by the Industry Sectors for the remainder of such director's unexpired term.

Section 7.8. Meetings; Notice; Waiver.

(a) Meetings. An annual meeting of the Board shall be held without notice immediately following the annual meeting of the Members. The Board shall elect the Chair and Vice-Chair for the next year at the annual meeting. In addition, regular meetings may be held at such time or times as fixed by the Board. Special meetings of the Board may be called by the Board's Chair, the President or by any three directors and shall be held at the principal office of the Corporation, or such other place within the Region as determined by the Chair or the President after consultation with the Board.

(b) Notice. Notice of the dates, times, and places of all regular and special meetings of the Board shall be published by the Secretary and provided to all directors and Members not less than three (3) days prior to the date of the meeting. Notice shall be deemed given by the Corporation to directors and the Members when (a) posted on the Corporation's public website in a reasonably prominent location, and (b) sent by mail, facsimile or reputable overnight delivery service or by electronic transmission to each director and each Member's representative authorized pursuant to Section 6.10.1.

(c) Waiver. Any person entitled to notice of a regular or special meeting of the Board may waive notice thereof. A waiver of notice by a person entitled to notice is effective whether given before, at, or after the meeting, and whether given in writing or by attendance. Attendance by a director at a meeting of the Board is a waiver of notice of that meeting, unless the director objects at the beginning of the meeting to the transaction of business because the meeting is not lawfully called or convened, or objects before a vote on an item of business because the item may not lawfully be considered at that meeting and does not participate in the consideration of the item at that meeting.

Section 7.9. Quorum. For the Board to take action at a meeting, a quorum of directors must be present. A quorum is a majority of the directors then in office, provided that: (a) if there are three or four independent directors holding office, two independent directors must be present to constitute a quorum, or (b) if there are two independent directors holding office, one independent director must be present to constitute a quorum. If there is only one independent director or no independent directors holding office, there is no requirement that an independent director be present in order for the Board to have a quorum. In the absence of a quorum, a majority of the directors present may adjourn a meeting, without notice, except as may be given at such meeting, until a quorum is present.

Section 7.10. Board Action. The act of a majority of the directors present at a meeting at which a quorum is present shall be the act of the Board, unless the act of a greater number is required by law or these Bylaws.

Section 7.11. Action Without a Meeting. Any action required or permitted to be taken at any meeting of the Board or any committee thereof may be taken without a

meeting if all members of the Board or committee, as the case may be, consent thereto in writing or by electronic transmission, and the writing or writings or electronic transmission or transmissions are filed with the minutes of proceeding of the Board or the committee. Any nonconfidential material provided to the Board or a committee in connection with such action shall be posted on the Corporation's website at approximately the same time that it is given to the Board or the committee. The results of all actions taken by the Board or any committee thereof without a meeting shall be promptly posted on the Corporation's website.

Section 7.12. Action by Electronic Communication. A conference among directors by a means of communication through which the directors may simultaneously hear each other during the conference is a Board meeting if the same notice is given of the conference as would be required for a meeting and if the number of directors participating in the conference is a quorum. Participation in a meeting by this means constitutes personal presence at the meeting. A director may participate in a Board meeting by any means of communication through which the director, other directors participating, and all directors physically present at the meeting may simultaneously communicate with each other during the meeting.

Section 7.13. Board Committees. The Board shall have an audit committee, compensation committee, nominating and governance committee and compliance committee, and such other committees the Board deems necessary and appropriate. Each committee shall be comprised of not less than three directors. The compliance committee shall be comprised of a minimum of five directors, a majority of whom are independent directors. All independent directors shall serve on the compliance committee. The Board may require that a minimum number of independent directors serve on any or all other Board committees. The Board shall have the power to appoint, and to delegate authority to, such other committees of the Board as it determines to be appropriate from time to time. The Board may require any committee to adopt a charter, subject to approval by the Board, governing the activities and authority of the committee and the composition of its members.

Section 7.14. Hearing Body. The Hearing Body shall consist of the Board compliance committee.

7.14.1 Quorum. For the Hearing Body to take action at a hearing, a quorum of members must be present. A quorum is a majority of members of the Hearing Body, provided that two independent directors are present. If a quorum of the Hearing Body does not remain after any recusals and rulings on motions for disqualification, the compliance committee shall appoint a new member to the Hearing Body from among other directors to create a quorum, provided that the requirement that at least two independent directors are present for a quorum shall at all times continue to be met. Such new member shall serve on the Hearing Body for purposes of the subject hearing through the conclusion of the hearing but not thereafter.

7.14.2 Voting. Each Hearing Body member shall have one vote with respect to matters presented at a hearing. Action may be taken at a hearing at which a quorum is present upon the vote of the majority of members present.

Section 7.15. Public Notice of Board Meetings. Notice to the public of the dates, times and places of Board meetings, including committees thereof, and all nonconfidential material provided to the Board or the committees, shall be posted on the Corporation's website, and notice of Board and committee meetings shall be sent by electronic transmission to Members, at approximately the same time that notice is given to the Board or the committee, as the case may be. Board and committee Meetings shall be open to all Members and the public, subject to reasonable limitations due to the availability and size of meeting facilities; provided, that any meeting may be held in or adjourn to closed session to discuss matters of a confidential nature, including, but not limited to, personnel matters, compliance and enforcement matters, litigation or commercially sensitive or critical infrastructure information of a Member or other Person.

Section 7.16. Posting of Minutes. Minutes of Board and committee meetings shall be posted on the Corporation's website when available.

Section 7.17. Compensation of Directors. The directors elected by the Industry Sectors and the at-large directors shall not receive compensation for their service to the Corporation as directors on the Board. The independent directors shall be entitled to such compensation as the Board may from time to time determine. Nothing contained in these Bylaws shall preclude any director from receiving compensation for services to the Corporation in any other capacity.

ARTICLE VIII. ORGANIZATIONAL GROUPS

Section 8.1. Establishment of Organizational Groups. The Board shall establish such organizational groups, consisting of committees, sub-committees, task forces and working groups of Members, as are necessary and appropriate to accomplish the purposes of the Corporation in an efficient and cost-effective manner. All organizational groups shall be subject to the direction and control of the Board. The membership of organizational groups shall be determined based upon experience, expertise and geographic diversity and to the extent practicable shall include balanced representation of the Industry Sectors. The Board shall establish policies and procedures governing the creation of organizational groups, how they are populated, how voting and related matters are conducted, how they may be reorganized and the direction and termination of such groups. The Board shall conduct a review of all organizational groups of the Corporation on an annual basis to ensure that the business of the Corporation is conducted in an efficient, cost-effective manner.

Section 8.2. Reimbursement. The Board may authorize reimbursement for persons acting on behalf of the Corporation, as necessary in the interests of the Corporation.

ARTICLE IX. OFFICERS

Section 9.1. Officers. The officers of the Corporation shall include a President, one or more Vice Presidents, a Secretary, a Treasurer and any other officers as may be elected or appointed in accordance with the provisions of this Article. The Board may elect or appoint any additional officers that it deems desirable, such other officers to have the authority and perform the duties prescribed by the Board. The same individual may hold any number of offices, except that of President.

Section 9.2. Election and Term of Office. The officers of the Corporation shall be elected annually by the Board at the annual meeting of the Board. Each officer shall hold office at the pleasure of the Board. If the election of officers is not held at such meeting, such election shall be held as soon thereafter as is convenient. New officers may be created and the positions filled at any meeting of the Board. Each elected officer shall hold office until his or her successor has been duly elected and qualified or upon his or her earlier resignation or removal.

Section 9.3. Removal. Any officer elected by the Board may be removed by the affirmative vote of two-thirds (2/3) of the Board whenever in its judgment the best interests of the Corporation would be served thereby, but such removal shall be without prejudice to the contract rights, if any, of the officer so removed. Election or appointment of an officer or agent shall not of itself create contract rights.

Section 9.4. Vacancies. A vacancy in any office because of death, incapacity, resignation, removal, disqualification, or otherwise, may be filled by the Board for the unexpired portion of the term.

Section 9.5. President. The President shall:

- (a) be the principal executive and operating officer of the Corporation;
- (b) sign certificates of membership, and may sign any deeds, mortgages, deeds of trust, notes, bonds, contracts or other instruments authorized by the Board to be executed, except in cases in which the signing and execution thereof shall be expressly delegated by the Board or by these Bylaws to some other officer or agent of the Corporation; and
- (c) perform all duties incident to the office of President, including hiring and directing staff, and such other duties as may be prescribed by the Board from time to time.

Section 9.6. Vice Presidents. The Vice President(s) shall perform such duties and have such powers as the Board or President may from time to time prescribe. At

the request of the Board, the Vice President (or in the event there be more than one Vice President, the Vice Presidents in the order designated, or in the absence of any designation, then in the order of their election) shall perform the duties of the President, and when so acting, shall have all the powers of and be subject to all the restrictions upon the President.

Section 9.7. Secretary. The Secretary shall ensure that the following duties are carried out:

- (a) the minutes of the meetings of the Members and of the Board, and each committee thereof, are recorded;
- (b) all required notices are duly given in accordance with these Bylaws and as required by law;
- (c) a register of the current names and addresses of all Members is maintained and posted on the Corporation's website;
- (d) a complete copy of the Certificate of Incorporation and Bylaws of the Corporation containing all amendments thereto are kept on file at all times and posted on the Corporation's website, which copies shall always be open to the inspection of any Member; and
- (e) generally perform all duties incident to the office of Secretary and such other duties as may be prescribed by the Board from time to time.

Section 9.8. Treasurer. The Treasurer shall be responsible for the following activities:

- (a) maintain custody of all funds and securities of the Corporation;
- (b) receipt of and the issuance of receipts for all monies due and payable to the Corporation and for deposit of all such monies in the name of the Corporation in such bank or banks or financial institutions as shall be selected by the Board; and
- (c) generally perform all duties incident to the office of Treasurer and such other duties as may be prescribed by the Board from time to time.

ARTICLE X. CERTIFICATES OF MEMBERSHIP

Section 10.1. Certificates of Membership. The Board may, but need not, provide for the issuance of certificates evidencing membership in the Corporation, which certificates shall be in such form as may be determined by the Board.

ARTICLE XI.
BOOKS AND RECORDS

Section 11.1. Books and Records; Financial Statements. The Corporation shall keep at such office selected by the Board correct and complete copies of its Certificate of Incorporation and Bylaws, accounting records, and minutes of meetings of Members, Board, and committees having any of the authority of the Board. A Member, or the agent or attorney of a Member, may inspect all books and records for any proper purpose at any reasonable time. Upon request, the Corporation shall give the Member a statement showing the financial result of all operations and transactions affecting income and expenses during its last annual accounting period and a balance sheet containing a summary of its assets and liabilities as of the closing date of the accounting period.

ARTICLE XII.
FISCAL YEAR

Section 12.1. Fiscal Year. The fiscal year of the Corporation shall be the calendar year.

ARTICLE XIII.
TRANSFER OF ASSETS

Section 13.1. Member Approval Not Required. Subject to restrictions set forth in the Certificate of Incorporation, the Corporation, by affirmative vote of the Board, may sell, lease, transfer, or dispose of its property and assets in the usual and regular course of its activities and grant a security interest in all or substantially all of its property and assets in the usual and regular course of its activities, upon those terms and conditions and for those considerations, which may be money, securities, or other instruments for the payment of money or other property, as the Board considers expedient, in which case no Member approval is required.

Section 13.2. Member Approval Required. Subject to restrictions set forth in the Certificate of Incorporation, the Corporation may sell, lease, transfer, or dispose of all or substantially all of its property and assets, including its good will, not in the usual and regular course of its activities, upon those terms and conditions and for those considerations, which may be money, securities, or other instruments for the payment of money or other property, as the Board considers expedient only when approved at a regular or special meeting of the Members by the affirmative vote of two-thirds (2/3) of all the Members. Notice of the meeting must be given to the Members. The notice must state that a purpose of the meeting is to consider the sale, lease, transfer, or other disposition of all or substantially all of the property and assets of the Corporation.

ARTICLE XIV.
CONTRACTS, CHECKS, DEPOSITS, AND GIFTS

Section 14.1. Contracts. The Board may authorize any officer or officers or agent or agents of the Corporation, in addition to the officers so authorized by these Bylaws, to enter into any contract or execute and deliver any instrument in the name of and on behalf of the Corporation, and such authority may be general or may be confined to specific instances.

Section 14.2. Checks, Drafts, or Orders. All checks, drafts, or orders for the payment of money, notes, or other evidences of indebtedness issued in the name of the Corporation, may be signed by such officer or officers or agent or agents of the Corporation, and in such manner, as shall from time to time be determined by resolution of the Board.

Section 14.3. Deposits. All funds of the Corporation shall be deposited to the credit of the Corporation in such banks, trust companies, or other depositories as the Board may select.

Section 14.4. Gifts. The Board may accept on behalf of the Corporation any contribution, gift, bequest, or devise for any purpose of the Corporation.

ARTICLE XV.
INSURANCE, LIMITATION ON LIABILITY AND INDEMNIFICATION

Section 15.1. Insurance. The President is authorized to procure insurance to protect the Corporation against damages arising out of or related to any directive, order, procedure, action or requirement of the Corporation.

Section 15.2. Limitations on Liability. As provided in Article Fourteenth of the Certificate of Incorporation, a director of the Corporation shall not be personally liable to the Corporation or its Members for monetary damages for breach of fiduciary duty as a director, except for liability (i) for any breach of the director's duty of loyalty to the Corporation or its Members, (ii) for acts or omissions not in good faith or which involve intentional misconduct or a knowing violation of law, (iii) under Section 174 of the Delaware General Corporation Law or (iv) for any transaction from which the director derived any improper personal benefit. If the Delaware General Corporation Law is amended to authorize corporate action further eliminating or limiting the personal liability of directors, then the liability of a director of the Corporation shall be eliminated or limited to the fullest extent permitted by the Delaware General Corporation Law, as so amended. Any repeal or modification of Article Fifteenth of these Bylaws by the Members of the Corporation shall not adversely affect any right or protection of a director of the Corporation existing at the time of such repeal or modification.

Section 15.3. Right to Indemnification.

15.3.1 Indemnified Persons. Each person who was or is made a party or is threatened to be made a party to or is involved in or called as a witness in any

Proceeding because he or she is an Indemnified Person shall be indemnified and held harmless by the Corporation to the fullest extent permitted under the Delaware General Corporation Law (the "DGCL"), as the same now exists or may hereafter be amended (but, in the case of any such amendment, only to the extent that such amendment permits the Corporation to provide broader indemnification rights than the DGCL permitted the Corporation to provide prior to such amendment). Such indemnification shall cover all expenses incurred by an Indemnified Person (including, but not limited to, attorneys' fees and other expenses of litigation) and all liabilities and losses (including, but not limited to, judgments, fines, ERISA or other excise taxes or penalties and amounts paid or to be paid in settlement) incurred by such person in connection therewith.

15.3.2 Denial of Authorization for Certain Proceedings. Notwithstanding anything to the contrary in this Section 15.3, except with respect to indemnification of Indemnified Persons specified in paragraph 15.3.3 of this Section 15.3, the Corporation shall indemnify an Indemnified Person in connection with a Proceeding (or part thereof) initiated by such person only if authorization for such Proceeding (or part thereof) was not denied by the Board of the Corporation prior to the earlier of 60 days after receipt of notice thereof from such Indemnified Person.

15.3.3 Certain Defined Terms. For purposes of this Section 15.3, the following terms shall have the following meanings (such meanings to be equally applicable to both the singular and plural forms of the terms defined):

(1) a "Proceeding" is any investigation, action, suit or proceeding, whether civil, criminal, administrative or investigative, and any appeal therefrom.

(2) an "Indemnified Person" is a person who is, was, or had agreed to become a Director of the Corporation (including, in the case of such person seeking indemnification while serving as a Director who is or was an officer of the Corporation, such person in his capacity as an officer.)

15.3.4 Expenses. Expenses, including attorneys' fees, incurred by a person indemnified pursuant to paragraph 15.3.1 in defending or otherwise being involved in a Proceeding shall be paid by the Corporation in advance of the final disposition of such Proceeding, including any appeal therefrom, upon receipt of an undertaking (the "Undertaking") by or on behalf of such person to repay such amount if it shall ultimately be determined that he or she is not entitled to be indemnified by the Corporation; provided that in connection with a Proceeding (or part thereof) initiated by such person, except a Proceeding authorized by paragraph 15.3.5, the Corporation shall pay said expenses in advance of final disposition only if authorization for such Proceeding (or part thereof) was not denied by the Board of the Corporation prior to the earlier of 60 days after receipt of a request for such advancement accompanied by the Undertaking. A person to whom expenses are advanced pursuant hereto shall not be obligated to repay such expenses until the final determination of any pending Proceeding in a court of competent jurisdiction concerning the right of such person to be indemnified or the obligation of such person to repay such expenses.

15.3.5 Protection of Rights. If a claim by an Indemnified Person under paragraph 15.3.1 is not promptly paid in full by the Corporation after a written claim has been received by the Corporation or if expenses pursuant to paragraph 15.3.4 have not been promptly advanced after a written request for such advancement by an Indemnified Person (accompanied by the Undertaking required by paragraph 15.3.4) has been received by the Corporation, the claimant may at any time thereafter bring suit against the Corporation to recover the unpaid amount of the claim or the advancement of expenses. If successful, in whole or in part, in such suit, such claimant shall also be entitled to be paid the reasonable expense thereof. It shall be a defense to any such action (other than an action brought to enforce a claim for expenses incurred in defending any Proceeding in advance of its final disposition where the Undertaking has been tendered to the Corporation that indemnification of the claimant is prohibited by law, but the burden of proving such defense shall be on the Corporation. Neither the failure of the Corporation (including the Board, independent legal counsel, or the Members) to have made a determination, if required, prior to the commencement of such action that indemnification of the claimant is proper in the circumstances, nor an actual determination by the Corporation (including the Board, independent legal counsel, or the Members) that indemnification of the claimant is prohibited, shall be a defense to the action or create a presumption that indemnification of the claimant is prohibited.

15.3.6 Miscellaneous.

(a) Non-Exclusivity of Rights. The rights conferred on any person by this Section 15.3 shall not be exclusive of any other rights which such person may have or hereafter acquire under any statute, provision of the Certificate of Incorporation, Bylaw, agreement, vote of Members or disinterested directors or otherwise. The Board shall have the authority, by resolution, to provide for such other indemnification of directors, and such indemnification of officers, delegates, employees, agents, or others of the Corporation as it shall deem appropriate.

(b) Insurance, contracts, and funding. The Corporation may maintain insurance, at its expense, to protect itself and any director, officer, employee, delegate or agent of the Corporation against any expenses, liabilities or losses, whether or not the Corporation would have the power to indemnify such person against such expenses, liabilities or losses under the DGCL. The Corporation may enter into contracts with any director, officer, or employee of the Corporation in furtherance of the provisions of this Section 15.3 and may create a trust fund, grant a security interest or use other means (including, without limitation, a letter of credit) to ensure the payment of such amounts as may be necessary to effect the advancing of expenses and indemnification as provided in such contracts or as otherwise provided in this Section 15.3.

(c) Contractual nature. The provisions of this Section 15.3 shall continue as to a person who has ceased to be a director and shall inure to the benefit of the heirs, executors and administrators of such person. This Section 15.3 shall be deemed to be a contract between the Corporation and each person

who, at any time that this Section 15.3 is in effect, serves or agrees to serve in any capacity which entitles him to indemnification and advancement of expenses hereunder and any repeal or other modification of this Section 15.3 or any repeal or modification of the DGCL or any other applicable law shall not limit any rights of indemnification for Proceedings then existing or arising out of events, acts or omissions occurring prior to such repeal or modification, including, without limitation, the right to indemnification and advancement of expenses for Proceedings commenced after such repeal or modification to enforce this Section 15.3 with regard to Proceedings arising out of acts, omissions or events arising prior to such repeal or modification.

(d) Cooperation. Each Indemnified Person shall cooperate with the person, persons or entity making the determination with respect to such Indemnified Person's entitlement to indemnification under this Section 15.3, including providing to such person, persons or entity upon reasonable advance request any documentation or information which is not privileged or otherwise protected from disclosure and which is reasonably available to such Indemnified Person and reasonably necessary to such determination. Any costs or expenses (including attorneys' fees and disbursements) incurred by such Indemnified Person in so cooperating with the person, persons or entity making such determination shall be borne by the Corporation (irrespective of the determination as to such Indemnified Person's entitlement to indemnification) and the Corporation hereby indemnifies and agrees to hold such Indemnified Person harmless therefrom.

(e) Subrogation. In the event of any payment under this Section 15.3 to an Indemnified Person, the Corporation shall be subrogated to the extent of such payment to all of the rights of recovery of such Indemnified Person, who shall execute all papers required and take all action necessary to secure such rights, including execution of such documents as are necessary to enable the Corporation to bring suit to enforce such rights.

(f) Severability. If this Section 15.3 or any portion hereof shall be invalidated or held to be unenforceable on any ground by any court of competent jurisdiction, the decision of which shall not have been reversed on appeal, this Section 15.3 shall be deemed to be modified to the minimum extent necessary to avoid a violation of law and, as so modified, this Section 15.3 and the remaining provisions hereof shall remain valid and enforceable in accordance with their terms to the fullest extent permitted by law.

ARTICLE XVI. TRANSITION

Section 16.1. Transition Standards. The Corporation will use the existing standards, criteria, rules or guides from each existing reliability council region for those Members that join the Corporation as in effect immediately prior to formation of the Corporation until such standards, criteria, rules or guides are adopted, superseded, or

rejected by the Corporation. The Corporation will establish any necessary transition committees, subcommittees, working groups or task forces to administer the existing regional reliability standards, criteria, rules and guides until they are adopted, superseded, or rejected by the Corporation. The Corporation will employ its best efforts, within two (2) years of its formation, to work toward a uniform set of Reliability Standards for the entire Region. The Board will develop and implement a standards process and a plan for transition to new Reliability Standards. This process will include a requirement that two-thirds of the directors present at a meeting must vote to adopt new Reliability Standards.

ARTICLE XVII. PARTICIPATION BY REGULATORY PARTICIPANTS

Section 17.1. Regulatory Participants. All Regulatory Participants shall be entitled to and be provided with the same rights to notice of and participation in meetings or other activities of the Corporation as are provided to Members, but shall not have the right to vote.

ARTICLE XVIII. BUDGET AND BUSINESS PLAN

Section 18.1. Budget and Business Plan. Each annual budget and business plan of the Corporation shall be approved by the Board in sufficient time in each fiscal year to allow for timely submittal of the approved annual budget and business plan to NERC in accordance with the NERC Rules. The Corporation shall post a draft of each budget and business plan on the Corporation's website for purposes of review and comment by the Members at least ten (10) days prior to the Board meeting at which the budget and business plan are to be approved.

ARTICLE XIX. AMENDMENT OF BYLAWS

Section 19.1. Amendment Of Bylaws. The power to adopt, amend or repeal these Bylaws is vested in the Members as set forth in Section 6.6.3 of these Bylaws; provided, however, that upon the passage of any federal electric reliability legislation, and/or the adoption of any rules or regulations of the Commission, NERC or other governmental entity with jurisdiction, the Board shall have authority to amend these Bylaws as necessary and appropriate to comply with such law, legislation, rules and regulations.

Project 2009-26 — Interpretation of CIP-004-1 for WECC

Action

Adopt the interpretation of Requirements R2, R3, and R4 of CIP-004-x¹ (Cyber Security — Personnel and Training) for WECC and direct staff to file with applicable regulatory authorities.

- Interpretation of CIP-004-x. The referenced clean standards below provide the interpretation being approved as an appendix.

[\[CIP-004-3a Clean\]](#) (interpretation applicable to currently effective standard)

[\[CIP-004-4a Clean\]](#) (interpretation prospectively applicable upon future effective date)

Background

On October 15, 2009, WECC requested a formal interpretation of CIP-004-1 Cyber Security — Personnel and Training, Requirements R2, R3, and R4, requesting the following clarification:

Specifically, the WECC RC seeks clarification on the definition of “authorized access” as it applies to temporary support from vendors.

Do the training, risk assessment and access requirements specified in R2, R3, and R4 apply to vendors who are supervised? Assuming that a “supervised” vendor is exempt from CIP-004-1, Requirements R2, R3 and R4, would temporary, indirect and monitored access, such as that provided through remote terminal sessions (WebEx, etc.) or escorted physical access, be considered supervision?

An interpretation was developed and posted for a 30-day public comment period from December 7, 2009 through January 6, 2010, followed by an Initial Ballot from January 6, 2010 through January 19, 2010. There were 80 sets of comments, including comments from approximately 80 different people from approximately 53 companies representing nine of the 10 NERC Industry Segments. However, work on the interpretation was delayed based on reprioritization of the total standards workload and then further delayed until the Standards Committee (SC) developed more formal processes for addressing interpretations in support of the Board of Trustees’ November 2009 guidance.

In April 2011, the SC approved and issued the Guidelines for Interpretation Drafting Teams and directed that work resume on the interpretation. Nominations were solicited for a dedicated Critical Infrastructure Protection (CIP) Interpretation Drafting Team (IDT). A CIP IDT was appointed, and members of the team reviewed the comments received from the 2009 comment period and 2010 ballot. The project team revised the interpretation pursuant to the Guidelines for Interpretation Drafting Teams. In consideration of the Guidelines for Interpretation Drafting Teams, the IDT considered the requirement language in the standard as

¹ The interpretation applies to versions 1, 2, 3, and 4 of the standard.

written in order to provide clarity on the meaning of the standard, and the IDT believes that the meaning of the standard informs the proper reach of the standard.

The modified interpretation was posted for a 45-day public comment period from February 7, 2012 through March 23, 2012 with a Successive Ballot occurring on the last 10 days of the comment period. The ballot achieved a 80 percent approval, with a quorum of 89 percent. A Recirculation Ballot was conducted from April 20, 2012 through April 30, 2012, and the interpretation was approved by stakeholders, achieving an 80 percent approval with a quorum of 91 percent.

Summary

The interpretation provides the following answers to the requestor:

While the Glossary of Terms used in NERC Reliability Standards does not have a definition of “authorized access,” CIP-004-1, Requirement R4 requires that an entity “shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.” For purposes of CIP-004-1, an individual has “authorized access” if he or she is on that list, and, as a result, is subject to Requirements R2, R3, and R4.

As written, all cyber access to Critical Cyber Assets must be authorized, and all authorized access must comply with Requirements R2, R3, and R4. Through the use of the qualifier “unescorted” with regard to physical access, CIP-004-1, Requirement R2, implies the concept of supervision for physical access when an individual is not authorized, and CIP-006 R1.6 also allows for escorted unauthorized physical access via a visitor program. There is no similar qualifier or reference in the requirement that mentions “escorted” or otherwise implies supervision for cyber access within CIP-004. Furthermore, there is no mention of any escorted unauthorized cyber access within CIP-007 similar to the visitor program in CIP-006 R1.6. Compared to “physical access,” the concept or any words relating to “escorting” or “supervision” in the requirement language is absent relative to cyber access.

To the extent a vendor is escorted to physically access a Critical Cyber Asset for purposes other than direct cyber access (e.g., replacing parts on the Critical Cyber Asset), supervision is acceptable (within the context of escorted physical access). If the escorted physical access includes bringing a vendor or other individual to the Critical Cyber Asset to direct someone with authorized access in performing cyber access, such supervision is also acceptable within the language of the requirement, since the vendor or other individual is merely present while an authorized individual conducts the actual cyber access. However, the requirement language does not support the notion of physically escorting a vendor or other individual to a Critical Cyber Asset for the vendor or other individual to perform cyber access, even if supervised. Even if it is possible to provide supervised cyber access to Critical Cyber Assets, there is no basis or contemplation of “escorted” cyber access whatsoever in CIP-004, whether remotely or in person.

A link to the project history and files is included here for reference:

http://www.nerc.com/filez/standards/Project2009-26_CIP-004-1_RFI_WECC.html

If trustees have questions or need additional information, they may contact Herb Schrayshuen, vice president and director of standards and training, at herb.schrayshuen@nerc.net.

**Member Representatives Committee Members to the
Board of Trustees Nominating Committee**

Action

Accept Member Representatives Committee (MRC) recommendation.

Background

At the MRC's May 8, 2012 meeting, Chair Scott Helyer invited members to volunteer to serve on the Board of Trustees Nominating Committee.

This year, Jan Schori will chair the Nominating Committee. The other board members are Paul Barber, Janice Case, Fred Gorbet, Ken Peterson, Bruce Scherr, and Roy Thilly.

In response to Scott Helyer's solicitation, several members of the MRC expressed interest in serving with MRC Chair Scott Helyer and Vice Chair Carol Chinn on the Board of Trustees Nominating Committee. The following five MRC representatives are recommended to the Board for inclusion on the Nominating Committee.

- Scott Helyer (MRC Chair)
- Carol Chinn (MRC Vice Chairman)
- Sylvain Clermont – Federal/Provincial Sector
- Terry Boston – ISO/RTO Sector
- John A. Anderson – Large End-Use Electricity Customer Sector

2013 Business Plan and Budget Preparation Schedule

2012 DATES	NERC	Regional Entity
February 3, 11:00 a.m. ET	FAC Conference Call to discuss quarterly business; includes update on BP&B process and schedule which is posted as part of agenda materials	
February 17	Common BP&B Assumptions posted for comment	
March 9	Comments due on Common BP&B Assumptions	
April 4	Meeting with trades to discuss 2013 BP&B (NERC DC office)	
April 16	Submittal to Regional Entities of Preliminary Internal Draft of NERC business plan and budget	Submittal to NERC of Preliminary Internal Draft of Regional Entity business plan and budgets for circulation among NERC program managers for review and feedback
May 2	Draft #1 of 2012 NERC Business Plan and Budget posted and sent to FAC	
May 3, 10:00am ET	FAC conference call and webinar to discuss Draft #1 of NERC business plan and budget	
May 4		Draft 1 of RE Business Plans and Budgets posted on NERC website
May 8	FAC Meeting	
May 8	MRC Meeting-Presentation of Draft 2013 Business Plan and Budget	
May 18	FAC conference webinar to review Regional Entities' Business Plans and Budgets	Regional Entities present draft business plans and budgets to NERC FAC
May 25	Comments due on Draft #1 of NERC 2013 Business Plan and Budget	

May 31	NERC files 2011 NERC and Regional Entity budget to actual true up with FERC	
June 1	Draft #2 of 2012 NERC Business Plan and Budget posted	
		Board Meeting Dates for Review and Approval of Regional Entity 2013 Business Plans and Budgets SPP – June 19 RFC – June 22 NPCC – June 26 TRE – June 26 WECC – June 26 FRCC – June 28 MRO – June 28 SERC – July 11
June 29	Stakeholder Comments due on NERC Draft #2 2013 Business Plan and Budget	
July 9		Final Regional Entity budget submittal due – approved by Regional Entity boards and final list of LSEs and NEL data
July 19, 10:30 a.m. ET	FAC webinar to review Draft #2 of NERC Business Plan and Budget and final Regional Entity budget submittals	Regional Entities present final business plans and budgets to NERC FAC
August 7	Final NERC and Regional Entity business plans, budgets and assessments posted and mailed to FAC, Board of Trustees and Member Representatives Committee	
August 15	Presentation of final Business Plan and Budget to MRC	
August 15	FAC Meeting to review and recommend approval of NERC and Regional Entity final 2013 business plans, budgets and assessments	

August 16	NERC and RE business plans, budgets and assessments presented to Board of Trustees for approval.	
August 24	Submit package to FERC and Canadian provincial authorities for approval. Package to include: (1) the NERC and RE business plans and budgets approved by the Board of Trustees, (2) NERC's annual funding requirement (including regional entity costs for delegated functions) and (3) the mechanism for assessing charges to recover that annual funding requirement.	

May 21, 2012

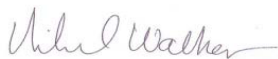
Dear Stakeholders,

NERC is extending the comment period on the first draft of its business plan and budget until this Friday, May 25. The second draft of NERC's Business Plan and Budget will be posted on June 1. The comment period on the second draft of NERC's Business Plan and Budget is extended from June 25 to June 29. All other dates on the 2013 Business Plan and Budget schedule remain the same.

An updated schedule is posted on NERC's website or by clicking [here](#). All comments should be emailed to me at michael.walker@nerc.net.

Thanks and we look forward to your ongoing input.

Sincerely,



Michael Walker
Senior Vice President and Chief Financial and Administrative Officer

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

From: [Kimberly Mielcarek](#)
To: [Kimberly Mielcarek](#)
Subject: NERC Announcements
Date: Wednesday, May 23, 2012 11:23:58 AM

Announcements

Spare Equipment Database Begins Operation

Click for [Database Announcement](#)

ATLANTA – The North American Electric Reliability Corporation’s (NERC) online spare equipment database is now operational. The inventory of spare equipment will be a helpful industry resource should a high-impact, low-frequency event result in damaged equipment. Providing information to the database is voluntary and meant to complement existing transformer sharing and mutual assistance agreements. The database is populated and managed by participating organization bound by a mutual confidentiality agreement. NERC’s initial focus is on high-voltage transmission and generator step-up transformers, which are vital for operation of the integrated bulk power system.

DOE Releases Risk Management Process Guideline

Click for [DOE Announcement](#), [RMP Guideline](#)

WASHINGTON, DC - The Department of Energy’s (DOE) Office of Electricity Delivery and Energy Reliability, in collaboration with the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC), today released guidance to help utilities better understand their cybersecurity risks, assess severity, and allocate resources more efficiently to manage those risks. The Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline, which provides a flexible approach to managing cybersecurity risks across all levels of the organization, was developed by a public-private sector team that was led by the Office of Electricity Delivery and Energy Reliability and included representatives from across the industry.

For more information or assistance, please contact [Kimberly Mielcarek](#).

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

You are currently subscribed to nerc-info as: lpedowicz@npcc.org
To unsubscribe send a blank email to leave-1292704-
325654.1ca6f85fb1574a8515cc07df72d3bfe0@listserv.nerc.com

Announcement

Spare Equipment Database Begins Operation

May 24, 2012

ATLANTA – The North American Electric Reliability Corporation’s (NERC) online spare equipment database is now operational. The inventory of spare equipment will be a helpful industry resource should a high-impact, low-frequency event result in damaged equipment.

Providing information to the database is voluntary and meant to complement existing transformer sharing and mutual assistance agreements. The database is populated and managed by participating organizations bound by a mutual confidentiality agreement. NERC’s initial focus is on high-voltage transmission and generator step-up transformers, which are vital for operation of the integrated bulk power system.

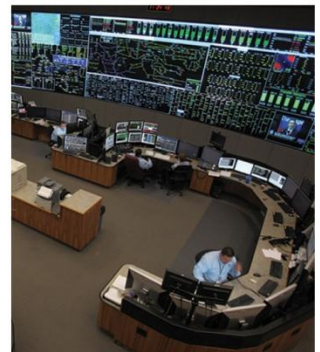
“The spare equipment database builds on industry’s existing extraordinary ability to address high-impact, low-frequency events,” said Mark Lauby, vice president and director of Reliability Assessment and Performance Analysis. “Industry’s participation demonstrates its continued commitment to bulk power system reliability.”

The database was developed based on recommendations from the [Spare Equipment Database](#) report, which was formed in response to direction from NERC’s board upon acceptance of the Electricity Sub-Sector Coordinating Council’s [Critical Infrastructure Strategic Roadmap](#). The joint NERC and Department of Energy report – [High-Impact, Low-Frequency Event Risk to the North American Bulk Power System](#) – released in June 2010 initiated the roadmap development.

Stakeholders must complete the registration process in order to be credentialed and gain access to the database. For more information on the program and database access, contact [Andrew Slone](#).

CONTACT:
Kimberly.Mielcarek@nerc.net

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com



ELECTRICITY SUBSECTOR CYBERSECURITY RISK MANAGEMENT PROCESS

U.S. Department of Energy

May 2012



Acknowledgments

This electricity subsector cybersecurity Risk Management Process (RMP) guideline was developed by the Department of Energy (DOE), in collaboration with the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC). Members of industry and utility-specific trade groups were included in authoring this guidance designed to be meaningful and tailored for the electricity sector. The primary goal of this guideline is to describe an RMP that is tuned to the specific needs of electricity subsector organizations. The NIST Special Publication (SP) 800-39, *Managing Information Security Risk*, provides the foundational methodology for this document. The NIST Interagency Report (NISTIR) 7628, *Guidelines for Smart Grid Cyber Security*, and NERC critical infrastructure cybersecurity standards further refine the definition and application of effective cybersecurity for all organizations in the electricity subsector. The NERC Critical Infrastructure Protection (CIP) cybersecurity standards are developed by a separate industry drafting team and are adopted through an industry balloting process that is not governed by the risk management guideline. While it is anticipated that entities subject to compliance with NERC CIP cybersecurity standards would use this guideline, compliance requirements are not altered in anyway by this guideline. Please consult your NERC CIP compliance authority for any questions on NERC CIP compliance.

DOE wishes to acknowledge and thank the senior leaders from DOE, NIST, NERC, and the members of the core development and subject matter expert teams who participated in the development of this guideline. The senior leaders, core development team, and subject matter expert team, and their organizational affiliations include:

Department of Energy

Patricia Hoffman

Assistant Secretary, Office of Electricity Delivery and Energy Reliability

National Institute of Standards and Technology

Charles H. Romine

Director, Information Technology Laboratory

William C. Barker

Cyber Security Advisor, Information Technology Laboratory

Donna Dodson

Chief, Computer Security Division

George Arnold

National Coordinator for Smart Grid Interoperability

North American Electric Reliability Corporation

Brian M. Harrell

Manager of Security Standards, Training, and Awareness

Risk Management Process Core Development Team

Andy Bochman IBM	Susan Farrand Department of Energy	Scott Saunders Sacramento Municipality Utility District
Bob Caldwell Edgewater	Win Gaulding Northrop Grumman Corporation	Anthony David Scott Accenture
Rocky Campione Planet Technologies	William Huntman Department of Energy	Sean Sherman Arctic Slope Regional Corporation
Paul Crist Lincoln Electric System	Lisa Kaiser Department of Homeland Security	Marianne Swanson National Institute of Standards and Technology
Rick Dakin Coalfire Systems	Matthew Light Department of Energy	Bill Watson Edgewater
Dave Dalva Smart Grid Interoperability Panel Cyber Security Working Group	John Lim Consolidated Edison	Ken Watson Information Technology Sector Coordinating Council
Cameron Doherty Southern California Edison	Samara Moore Department of Energy	Victoria Yan Pillitteri Booz Allen Hamilton
Summer Esquerre NextEra Energy, Inc.	Fowad Muneer ICF International	
	David Norton Federal Energy Regulatory Commission	

Risk Management Process Subject Matter Expert Team

James Brenton Electric Reliability Council of Texas	Felix Kwamena Natural Resources Canada	Reynaldo De Leon Southern California Edison
James Gilsinn National Institute of Standards and Technology	Scott Mix North American Electric Reliability Corporation	James W. Sample Pacific Gas & Electric Company
Neil Greenfield American Electric Power Co., Inc.	Brian Evans-Mongeon Utility Services, Inc.	

CAUTIONARY NOTE

INTENDED SCOPE AND USE OF THIS PUBLICATION

The guidance provided in this publication is intended to address *only* the management of cybersecurity-related risk derived from or associated with the operation and use of information technology and industrial control systems and/or the environments in which they operate. The guidance is *not* intended to replace or subsume other risk-related activities, programs, processes, or approaches that electricity subsector organizations have implemented or intend to implement addressing areas of risk management covered by other legislation, regulation, policies, programmatic initiatives, or mission and business requirements. Additionally, this guidance is not part of any regulatory framework. Rather, the cybersecurity Risk Management Process guidance described herein is complementary to and should be used as part of a more comprehensive enterprise risk management program.

CONTENTS

1. INTRODUCTION.....	1
2. CYBERSECURITY RISK MANAGEMENT OVERVIEW	5
2.1 Risk Management Model	6
2.1.1 Tier 1: Organization.....	7
2.1.2 Tier 2: Mission and Business Processes.....	7
2.1.3 Tier 3: Information Technology and Industrial Control Systems	8
2.2 Risk Management Cycle	8
2.2.1 Risk Framing.....	9
2.2.2 Risk Assessment	10
2.2.3 Risk Response.....	10
2.2.4 Risk Monitoring.....	11
2.3 Risk Management Process	11
3. TIER 1: ELECTRICITY SUBSECTOR ORGANIZATION	15
3.1 Risk Framing at Tier 1	15
3.1.1 Inputs	16
3.1.2 Activities	17
3.1.2.1 Define Risk Assumption	17
3.1.2.2 Identify Risk Management Constraint	20
3.1.2.3 Determine and Implement Risk Tolerance.....	20
3.1.3 Outputs.....	21
3.2 Risk Assessment at Tier 1.....	21
3.2.1 Inputs	22
3.2.2 Activities	23
3.2.2.1 Identify Threats and Vulnerabilities.....	23
3.2.2.2 Determine Risk.....	23
3.2.3 Outputs.....	24



- 3.3 Risk Response at Tier 1 24
 - 3.3.1 Inputs 25
 - 3.3.2 Activities 25
 - 3.3.2.1 Identify Risk Response.....25
 - 3.3.2.2 Evaluate Alternatives 26
 - 3.3.2.3 Determine and Implement Risk Response.....27
 - 3.3.3 Outputs.....28
- 3.4 Risk Monitoring at Tier 1 28
 - 3.4.1 Inputs 30
 - 3.4.2 Activities 30
 - 3.4.2.1 Develop Risk Monitoring Strategy 30
 - 3.4.2.2 Monitor Risk.....32
 - 3.4.3 Outputs.....33
- 3.5 Summary at Tier 1 33
- 4. TIER 2: MISSION AND BUSINESS PROCESSES 35**
 - 4.1 Risk Framing at Tier 2 35
 - 4.1.1 Inputs 36
 - 4.1.2 Activities 36
 - 4.1.2.1 Identify Mission and Business Processes and Applications.....36
 - 4.1.2.2 Establish Risk Tolerance and Risk Methodology 37
 - 4.1.2.3 Identify Cybersecurity Program and Architecture 38
 - 4.1.2.4 Develop or Refine Enterprise Architecture 39
 - 4.1.3 Outputs.....39
 - 4.2 Risk Assessment at Tier 2.....39
 - 4.2.1 Inputs 40
 - 4.2.2 Activities 41
 - 4.2.2.1 Prioritize Mission and Business Processes Based on
Consequence/Impact 41
 - 4.2.2.2 Determine Risk.....41

CONTENTS

4.2.3	Outputs.....	41
4.3	Risk Response at Tier 2.....	41
4.3.1	Inputs	42
4.3.2	Activities	42
4.3.2.1	Determine and Implement Risk Response.....	42
4.3.2.2	Define Cybersecurity Program and Architecture	43
4.3.3	Outputs.....	46
4.4	Risk Monitoring at Tier 2	46
4.4.1	Inputs	47
4.4.2	Activities	47
4.4.2.1	Establish Metrics to Measure Conformance to Cybersecurity Architecture.....	47
4.4.2.2	Measure Effectiveness of Cybersecurity Architecture.....	47
4.4.2.3	Periodically Reassess Cybersecurity Architecture	48
4.4.2.4	Monitor Changes to Environment.....	48
4.4.3	Outputs.....	48
4.5	Summary at Tier 2	48
5.	TIER 3: INFORMATION TECHNOLOGY AND INDUSTRIAL CONTROL SYSTEMS	51
5.1	Risk Framing at Tier 3.....	51
5.1.1	Inputs	52
5.1.2	Activities	52
5.1.2.1	Conduct IT and ICS Inventory	52
5.1.2.2	Define or Refine Cybersecurity Plans.....	52
5.1.3	Outputs.....	53
5.2	Risk Assessment at Tier 3.....	54
5.2.1	Inputs	54

5.2.2	Activities	54
5.2.2.1	Perform Cybersecurity Risk Assessment	54
5.2.2.2	Develop Cybersecurity Risk Assessment Report	54
5.2.3	Outputs.....	55
5.3	Risk Response at Tier 3	55
5.3.1	Inputs	55
5.3.2	Activities	55
5.3.2.1	Determine and Implement Risk Response.....	55
5.3.2.2	Select and Refine Cybersecurity Controls.....	56
5.3.2.3	Accept Cybersecurity Plan	56
5.3.2.4	Develop and Implement Risk Mitigation Plan	56
5.3.3	Outputs.....	57
5.4	Risk Monitoring at Tier 3	57
5.4.1	Inputs	57
5.4.2	Activities	58
5.4.2.1	Manage Technology Acquisition, Configuration, and Changes.....	58
5.4.2.2	Assess Cybersecurity Controls.....	58
5.4.2.3	Monitor New Threats and Vulnerabilities	58
5.4.2.4	Monitor Cybersecurity Mitigation Plan	58
5.4.2.5	Report Cybersecurity Status	59
5.4.2.6	Implement Decommissioning Strategy	59
5.4.3	Outputs.....	59
5.5	Summary at Tier 3	60

CONTENTS

APPENDIX A	REFERENCES	63
APPENDIX B	GLOSSARY	65
APPENDIX C	ACRONYMS	71
APPENDIX D	GOVERNANCE MODELS	73
APPENDIX E	TRUST MODELS	75
APPENDIX F	ROLES AND RESPONSIBILITIES	77
APPENDIX G	RISK RESPONSE STRATEGIES	81
APPENDIX H	COMMON CONTROLS	85

List of Figures

Figure 1:	Risk Management Model	6
Figure 2:	Risk Management Cycle	8
Figure 3:	Risk Management Process	11
Figure 4:	RMP Information Flowchart	12

List of Tables

Table 1:	Risk Management Process Overview	13
Table 2:	Tier 1 RMP Overview	34
Table 3:	Tier 2 RMP Overview	49
Table 4:	Tier 3 RMP Overview	61



1. Introduction

The electricity subsector¹ cybersecurity Risk Management Process (RMP) guideline has been developed by a team of government and industry representatives to provide a consistent and repeatable approach to managing cybersecurity risk across the electricity subsector. It is intended to be used by the electricity subsector, to include organizations responsible for the generation, transmission, distribution, and marketing of electric power, as well as supporting organizations such as vendors. The RMP is written with the goal of enabling organizations—regardless of size or organizational or governance structure—to apply effective and efficient risk management processes and tailor them to meet their organizational requirements. This guideline may be used to implement a new cybersecurity program within an organization or to build upon an organization’s existing internal cybersecurity policies, standard guidelines, and procedures.

The authors recognize that risk management processes in an organization are not executed in a vacuum. Regulatory requirements already exist to include North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, Nuclear Regulatory Commission (NRC) requirements, and a host of other Federal and State requirements. These requirements serve an important role in ensuring reliability, resilience, public safety, individual privacy, and protection of critical infrastructure. Within the RMP, these requirements are treated as inputs to the process and shape the risk management decisions made by an organization. Implementation of the RMP will provide organizations with greater agility in responding to new regulations or changes to existing regulatory requirements, allowing an organization to quickly identify the impact of new requirements and adjust their cybersecurity posture accordingly.

Electricity is widely recognized as a basic necessity for all citizens. It powers economies, consumer conveniences, national security capabilities, and industrial production to deliver competitive advantages in global markets. Whether caused willingly or unknowingly, damage to electricity subsector cyber systems can have a direct effect on the economic and national security interests of all nations.

¹ Homeland Security Presidential Directive 7 (HSPD-7) identifies Energy as one of the 17 critical infrastructure sectors of the Nation. Electricity is one of two subsectors. Oil and Natural Gas are treated as one.

INTRODUCTION

Cybersecurity risk is one of the components of the overall business risk environment and feeds into an organization's enterprise Risk Management Strategy and program. Cybersecurity risk, as with all risks, cannot be completely eliminated, but instead must be managed through informed decision making processes. The RMP is built on the premise that managing cybersecurity risk² is critical to the success of an organization's mission in achieving its business's goals and objectives, specifically the reliable generation and delivery of electric power. Implementation of the RMP will facilitate more informed decision making throughout an organization leading to more effective resource allocation, operational efficiencies, and the ability to mitigate and rapidly respond to cybersecurity risk. The goal is to reduce the likelihood and impact of a cyber event to an organization's operations, assets, and individuals. Implementation of the RMP across the electricity subsector will result in a common approach to managing cybersecurity risk, facilitating improved information exchange among organizations, between other stakeholders to include private sector and State and Federal agencies, and across international boundaries (Canada and Mexico). This will result in an improved dialogue that recognizes the need to manage this risk through an ongoing process to achieve the common goal of generating and delivering electric power.

Over the past few decades, the electricity subsector has become increasingly dependent on digital technology to reduce costs, increase efficiency, and maintain reliable operations. Information technology³ (IT) and industrial control systems⁴ (ICS) are vulnerable to malicious attacks and misuse. ICS are now being integrated with traditional business IT that provides corporate services (e.g., network, email). Data produced in the operation of ICS are increasingly used to support business decisions. Historically, ICS were composed of proprietary technologies with limited connection to an organization's corporate networks or the Internet. In today's world, the efficiencies of commercial off-the-shelf (COTS) hardware platforms and software applications, interconnected public and private networks, and remote support are moving organizations from an isolated environment into a global, interconnected environment. Technologies that drive the emerging smart grid will further integrate IT energy management systems, ICS, and business systems.

The highly publicized Stuxnet worm is an example of how vulnerabilities within IT systems can be used to reach into ICS (in this case, a programmable logic controller). Stuxnet blends social engineering, use of Universal Serial Bus (USB) drives, COTS vulnerabilities, and ICS application vulnerabilities to compromise a physical control device.

² Unless otherwise stated, references to risk in this publication refer to cybersecurity risk derived from the operation and use of organizational systems, including the processes, standards, guidelines, procedures, and structures within organizations that influence or affect the design, development, implementation, and ongoing operation of IT and ICS.

³ IT is a discrete system of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes interconnected or dependent business systems and the environment in which they operate (i.e., people, processes, technologies, and facilities).

⁴ An ICS is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. Operations Technology (OT) is an emerging term within industry used to describe hardware and software systems used to operate industrial control devices. For purposes of this document the term ICS will be used though some organizations may use the term OT.



All IT and ICS have vulnerabilities that are subject to threats and threat actors⁵ who either intentionally or unintentionally (accidentally) disrupt organizational operations, take revenge for perceived wrongdoings, or have means to perpetrate acts of terrorism. The increasing number of vulnerabilities as well as the interconnectedness of systems could serve as a blueprint for attackers who wish to access Intelligent Electronic Devices (IED) (e.g., controllers, relays, reclosers), safety systems, critical decision data, support systems, and physical and cybersecurity systems. This can cause damage to an electricity subsector organization's assets or harm to individuals, and can even compromise the reliable delivery of electricity.

Today's mission and business needs are reducing separation between ICS and business and administrative networks, resulting in increased vulnerabilities. This guideline provides a process that organizations can implement to manage the increased risks that these new technologies are introducing into the electricity subsector.

To successfully execute organizational mission and business functions in the electricity subsector, using IT and ICS processes, an organization's leadership function must be committed to making risk management a fundamental mission and business requirement. Understanding and handling cybersecurity risk is a strategic capability and an enabler of an efficient, effective, and sustained mission for business objectives across all electricity subsector organizations.

⁵ For additional information on threat sources, see US-CERT Cyber Threat Source Descriptions at http://www.us-cert.gov/control_systems/csthreats.html.



2. Cybersecurity Risk Management Overview

Electricity subsector organizations deal with risk every day in meeting their business objectives. They may include financial risk, risk of failure of equipment, and personnel safety risk, to name just a few. These organizations have developed processes to evaluate risks associated with their business and to choose how to deal with those risks based on organizational priorities and both internal and external constraints. This management of risk is conducted as an interactive, ongoing process as part of normal operations. To this end, these organizations may have developed enterprise risk management processes and strategies to define how they will address both inherent and residual risk in accomplishing their missions. While recognizing the larger context of risk management within an organization, this document has been written to provide a consistent and scalable risk management process specific to the risks inherent in operating IT and ICS. For purposes of this document, the term, risk management, refers to the program and supporting processes used to manage cybersecurity risk to an organization's operations, its assets, and individuals.⁶

Everyone in the organization is responsible for cybersecurity, but regardless of the size or type of the organization, executive leadership/governing boards are responsible for how cybersecurity risk impacts the organization's mission and business processes. In developing a governance structure, the organization establishes a risk executive function responsible for the organization-wide strategy to address risks, establishing accountability. The risk executive is a functional role that provides a more comprehensive, organization-wide approach to risk management. This function could exist as a collection of executive managers, board of directors, or committee of a cooperative organization. The function serves as the common enterprise risk management resource for senior leaders or executives, mission and business process owners, chief information officers (CIOs), chief information security officers, information system owners, enterprise architects, cybersecurity architects, and any other stakeholders having a vested interest in the mission and business success of organizations. In implementing the RMP, organizations have flexibility to determine how best to conduct the activities, including the sequence, degree of rigor, formality, and how the results or outputs of each activity are captured and shared across the organization and between organizations.

Electricity subsector organizations have a variety of risk management methodologies, models, and systems that they may already use for addressing areas such as safety and financial risk. The RMP discussed in this document is not meant to supersede these but to incorporate cybersecurity risk management within the existing structure. If an organization already has an established RMP, then much of the information contained in this document may already be known and may be used in conjunction with that process. The RMP described in this document is meant to supplement an organization's existing risk management framework and provide flexible guidelines that may be leveraged as needed. If the organization does not have

⁶ Adapted from National Information Assurance Glossary, Committee on National Security Systems (CNSS) 4009.

CYBERSECURITY RISK MANAGEMENT OVERVIEW

an existing risk management framework, then the RMP described in this document may be used as a standalone framework.

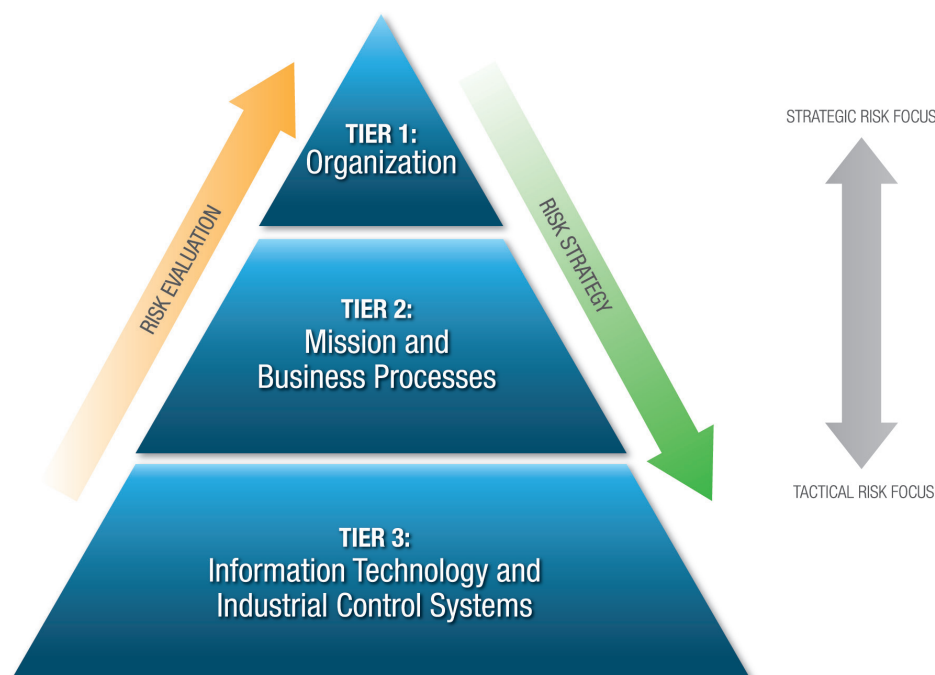
2.1 RISK MANAGEMENT MODEL

The risk management model⁷ presented in this document uses a three-tiered structure to provide a comprehensive view of an electricity subsector organization. This structure can be applied to any organization regardless of size or operations. The three tiers of the risk management model are:

- Tier 1: Organization;
- Tier 2: Mission and Business Processes; and
- Tier 3: Information Technology and Industrial Control Systems.

This model represents an electricity subsector organization's strategic focus in Tier 1, the mission and business processes focus in Tier 2, and tactical focus in Tier 3. Figure 1 illustrates the tiered risk management model.

Figure 1: Risk Management Model



⁷ NIST Special Publication (SP) 800-39, *Managing Information Security Risk*, provides the foundational methodology used in this document.



2.1.1 Tier 1: Organization

Tier 1 addresses risk from an organizational perspective by establishing and implementing a governance structure consistent with the strategic goals and objectives of the electricity subsector organization. Governance⁸ structures provide direction and oversight for risk management activities conducted by an organization. The risk management decisions at Tier 1 are inputs to the activities carried out at Tier 2 and Tier 3. The Tier 1 risk management activities may include:

- Establishing and implementing a structure for risk management and governance;
- Identifying and prioritizing mission and business processes with respect to strategic goals and objectives;
- Establishing the recovery order for critical mission and business processes;
- Establishing the organization's risk tolerance;
- Defining techniques and methodologies for assessing cybersecurity risk;
- Defining risk management constraints and requirements; and
- Establishing the organization's cybersecurity Risk Management Strategy.⁹

2.1.2 Tier 2: Mission and Business Processes

Tier 2 addresses risk from a mission and business process perspective. This tier informs and is informed by the IT and ICS technical architecture. Tier 2 activities are inputs to activities in Tier 3, and provide feedback to Tier 1. Generally, operational management is involved at this tier. However, in some organizations, the executive management may perform some of the tier functions. Cybersecurity risk management at this level focuses on the execution of specific mission and business processes. The risk management activities for Tier 2 may include:

- Identifying and prioritizing assets necessary to support the mission and business processes of an organization defined in Tier 1;
- Identifying cybersecurity processes needed to successfully execute mission and business processes;
- Mapping cybersecurity requirements¹⁰ against mission and business processes;
- Developing a disciplined and structured approach for managing IT and ICS assets that support mission and business processes; and
- Providing a clear and concise roadmap to (1) allow traceability from the highest level strategic goals and objectives of the organization; (2) ensure that mission and business process-driven cybersecurity requirements and protections are defined, implemented, maintained, and monitored; and (3) promote cost-effective, efficient, and resilient IT and ICS.

⁸ Additional information about governance models can be found in Appendix D, Governance Models.

⁹ The cybersecurity Risk Management Strategy is a component within an organization's enterprise Risk Management Strategy. The enterprise Risk Management Strategy may consist of risk strategy components, such as program management risk, investment risk, budgetary risk, legal liability risk, safety risk, inventory risk, or supply chain risk, in addition to a cybersecurity Risk Management Strategy.

¹⁰ Cybersecurity requirements can be obtained from a variety of sources (e.g., legislation, policies, regulations, standards, and organizational mission and business requirements).

CYBERSECURITY RISK MANAGEMENT OVERVIEW

2.1.3 Tier 3: Information Technology and Industrial Control Systems

Tier 3 addresses system risk from an IT and ICS perspective. It is guided and informed by the activities from Tiers 1 and 2. Tier 3 activities lead to the selection, deployment, and monitoring of cybersecurity controls (safeguards and countermeasures) at the system level. The cybersecurity controls are subsequently allocated to the various components of IT and ICS in accordance with the cybersecurity architecture¹¹ developed by the organization. Activities at this level provide feedback to Tier 2 and Tier 1 on the organization's risk posture. Tier 3 risk management activities may include:

- Categorizing IT and ICS into levels by risk and value to mission and business processes;
- Allocating cybersecurity controls to systems and the environments in which they operate;
- Managing the selection, implementation, assessment, and monitoring of cybersecurity controls; and
- Establishing a process to routinely reassess a system's cybersecurity posture based on new threat information, vulnerabilities, or system changes.

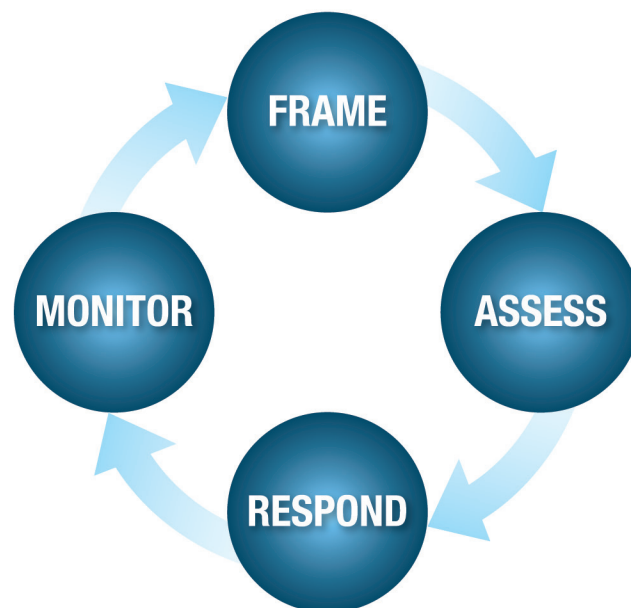
2.2 RISK MANAGEMENT CYCLE

The risk management cycle is an iterative and continuous process, constantly reformed by the changing risk landscape, as well as by organizational priorities and functional changes.

The risk management cycle provides four elements that structure an organization's approach to risk management, as represented in Figure 2:

- Frame;
- Assess;
- Respond; and
- Monitor.

Figure 2: Risk Management Cycle



¹¹ Cybersecurity architecture is a component of the enterprise architecture that describes the structure and behavior for an enterprise's cybersecurity processes, cybersecurity systems, personnel, and organizational units, showing their alignment with the enterprise's mission and strategic plans.



The risk management cycle is a comprehensive process that requires organizations to (1) frame risk (i.e., establish the context for risk-based decisions), (2) assess risk, (3) respond to risk once determined, and (4) monitor risk on an ongoing basis, using effective organizational communications and an iterative feedback loop for continuous improvement in the risk-related activities of organizations. Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization.

The output of the risk management process is a strategy addressing how an electricity subsector organization intends to frame, assess, respond to, and monitor risk. The strategy makes explicit and transparent the risk perceptions that an organization in the electricity subsector routinely uses to make investment and operational decisions. The following sections briefly describe each of the four risk management components.

2.2.1 Risk Framing

The risk framing element describes the environment in which risk-based decisions are made. Establishing a realistic and credible risk frame requires that organizations in the electricity subsector, identify:

- Assumptions about threats, vulnerabilities, impacts, and likelihood of occurrence;
- Constraints imposed by legislation, regulation, resource constraints (time, money, and people) and other factors identified by the organization;
- Risk tolerance, which identifies the level of acceptable risk;
- Priorities within mission and business processes, and trade-offs between different types of risk; and
- Trust relationships, such as physical interconnections, third-party service providers, reciprocity agreements, or device vendors.¹²

Risk framing includes third parties that are provided access to sensitive data and critical systems. For example, vendors may need access to systems to provide updates and support, but the risks they introduce could impact subsequent risk analysis and mitigation strategies.

¹² Each organization must take steps to be aware of the potential for risk from external relationships to ensure that it does not impose undue risks on others. Additional information about ways in which organizations can obtain levels of trust can be found in Appendix E, Trust Models.

CYBERSECURITY RISK MANAGEMENT OVERVIEW

2.2.2 Risk Assessment

The risk assessment element identifies, prioritizes, and estimates risk to an organization's operations, assets, individuals, and other interconnected electricity subsector organizations. The purpose of the risk assessment element is for organizations to identify the following components of risk and evaluate these against mission and business processes:

- Threats;
- Vulnerabilities;
- Impact (consequence or opportunity); and
- Likelihood (probability or frequency an event will occur).

Identifying cyber threats and vulnerabilities is not confined to review of IT and ICSs. Governance structures, mission and business processes, enterprise and cybersecurity architectures, facilities, equipment, supply chain activities, and external service providers, etc. are all considered during the risk assessment. To support the risk assessment element, organizations identify:

- Tools, techniques, and methodologies that are used to assess risk;
- Assumptions related to risk assessments;
- Constraints that may affect risk assessments;
- Roles and responsibilities¹³ related to risk assessment;
- Risk assessment information to be collected, processed, and communicated; and
- Threat information to be obtained.

2.2.3 Risk Response

The risk response element addresses how an electricity subsector organization responds to risk once that risk is assessed. The risk response element provides a consistent, organization-wide response to risk consistent with the organization's risk exposure. In this element, organizations:

- Develop alternative courses of action for responding to risk;
- Evaluate the alternative courses of action;
- Determine appropriate courses of action consistent with the organization's risk tolerance level; and
- Implement the courses of action.

The output of the risk response element informs the Risk Management Strategy and describes the types of risk responses that may be implemented (i.e., accepting, avoiding, mitigating, sharing, or transferring risk); the process to evaluate courses of action; the communication methods used across an organization and to external organizations (e.g., external service providers, supply chain partners) for those risk responses; and the tools, techniques, and methodologies used to develop courses of action for responding to risk.

¹³ Additional information about the responsibilities of organizational officials can be found in Appendix F, Roles and Responsibilities.



It may be determined through a cost-benefit analysis that during the risk response element certain response actions are not feasible to implement, are cost prohibitive, or are not relevant to electricity subsector operations. This may require implementation of compensating controls¹⁴ to manage the risk in an acceptable way and meet the cybersecurity requirements. The risk response element is the point where organizations make choices on how best to deal with that risk.

2.2.4 Risk Monitoring

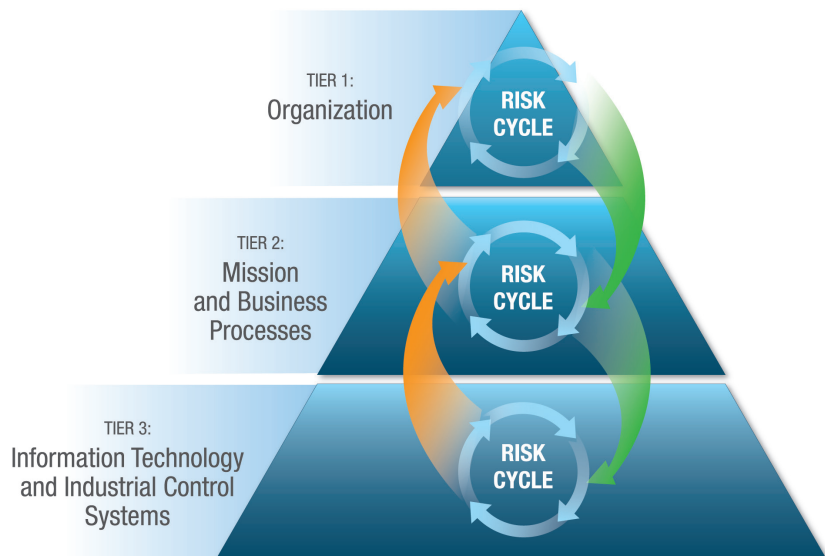
The risk monitoring element addresses how risks are monitored and communicated over time in an electricity subsector organization. During the risk monitoring element, organizations:

- Verify that risk response measures are implemented and that the cybersecurity requirements derived from the Risk Management Strategy are satisfied;
- Evaluate the ongoing effectiveness of risk response measures;
- Identify changes that may impact risk to an organization's IT and ICS and the operational environments;¹⁵ and
- Define the monitoring process to assess how change impacts the effectiveness of risk responses.

2.3 RISK MANAGEMENT PROCESS

The RMP shown in Figure 3 is based on integrating the risk management cycle shown in Figure 2 at each business tier in the risk management model shown in Figure 1. The goals of this process are to improve risk assessment, awareness, and develop a culture of cybersecurity at all levels of an organization. To facilitate these goals, further sections of this document will elaborate on the activities and outputs recommended to focus leaders, managers, security, and IT and ICS personnel on the practices of a strong risk program. The

Figure 3: Risk Management Process



¹⁴ A compensating control is a cybersecurity control employed in lieu of a recommended control that provides equivalent or comparable control.

¹⁵ Operational environments include but are not limited to threats; vulnerabilities; mission and business processes; enterprise and cybersecurity architectures; ITs; personnel; facilities; supply chain relationships; organizational governance and culture; procurement and acquisition processes; organizational policies and procedures; and organizational assumptions, constraints, risk tolerance, and priorities and trade-offs.

CYBERSECURITY RISK MANAGEMENT OVERVIEW

outputs (often documents) will help to promote communications among stakeholders, maintain focus on cybersecurity risk, and provide a basis for risk analysis and risk mitigation. The process is designed to (1) accommodate any size or type of organization, (2) support a mission and business focus top-down approach, and (3) promote a culture of security and improve risk communications.

The RMP assumes little about the size or type of organization, but it does assume that the functions of leadership (Tier 1), business management (Tier 2), and systems management (Tier 3) exist in all electricity subsector organizations. These functions may be conducted by a single individual, committee, division, or any other organizational structure.

As Figure 4 shows, each tier has within it an execution of the risk management cycle. The cycle elements (frame-assess-respond-monitor) each produce outputs that become inputs to the next element. General descriptions of the risk management cycle outputs at each tier are illustrated in Table 1. The RMP is a flexible process that allows organizations to implement it as appropriate to their organization. What is important is that all three tiers are engaged in the process. The sequencing and timing of the various activities will vary depending on the organization's structure, culture, and other factors.

Figure 4: RMP Information Flowchart

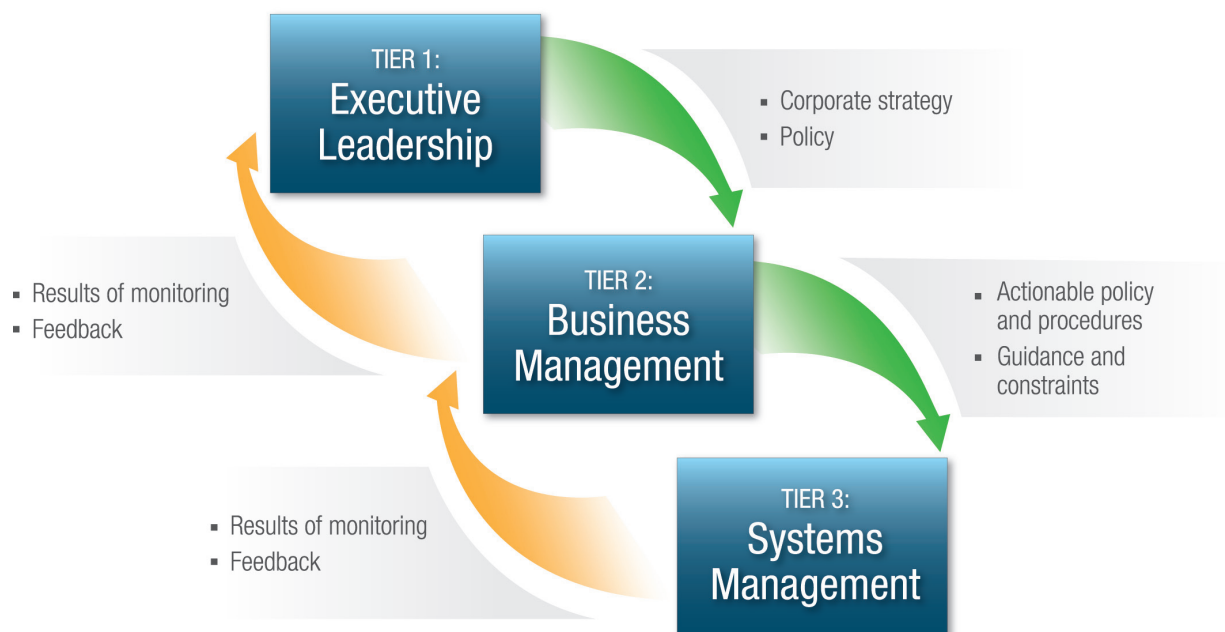




Table 1: Risk Management Process Overview

	TIER 1	TIER 2	TIER 3
RISK FRAMING	Section 3.1 Produce a set of organizational policies, governance structure, and guidance that form the basis for the Risk Management Strategy	Section 4.1 Establish risk assessment methodology and define the cybersecurity components of the enterprise architecture	Section 5.1 Develop the cybersecurity plan that identifies the components, systems, hardware, and software of the IT and ICS
RISK ASSESSMENT	Section 3.2 Determine risk to an organization's operations	Section 4.2 Develop prioritized list of mission and business processes	Section 5.2 Conduct risk assessment and develop cybersecurity risk assessment report
RISK RESPONSE	Section 3.3 Decide on the appropriate courses of action to accept, avoid, mitigate, share, or transfer risk.	Section 4.3 Using the prioritized list of processes, establish cybersecurity program and architecture	Section 5.3 Develop and implement risk mitigation plan
RISK MONITORING	Section 3.4 Determine the ongoing effectiveness of risk response measures	Section 4.4 Measure the effectiveness of and level of conformance with the cybersecurity architecture	Section 5.4 Monitor changes and measure effectiveness of cybersecurity controls

Table 1 above provides an overview of the entire risk management process and can be used as a resource for organizations implementing the RMP. Each cell summarizes the significant activities of the risk cycle across each tier.

The RMP defines and promotes a common understanding of risk tolerance and policy and communicates it across the organization. Because the process starts or includes the highest management levels of a business, it supports a top-down approach that incorporates business goals and objectives. It also facilitates a bottom-up communication of resource needs and implementation challenges.



3. Tier 1: Electricity Subsector Organization

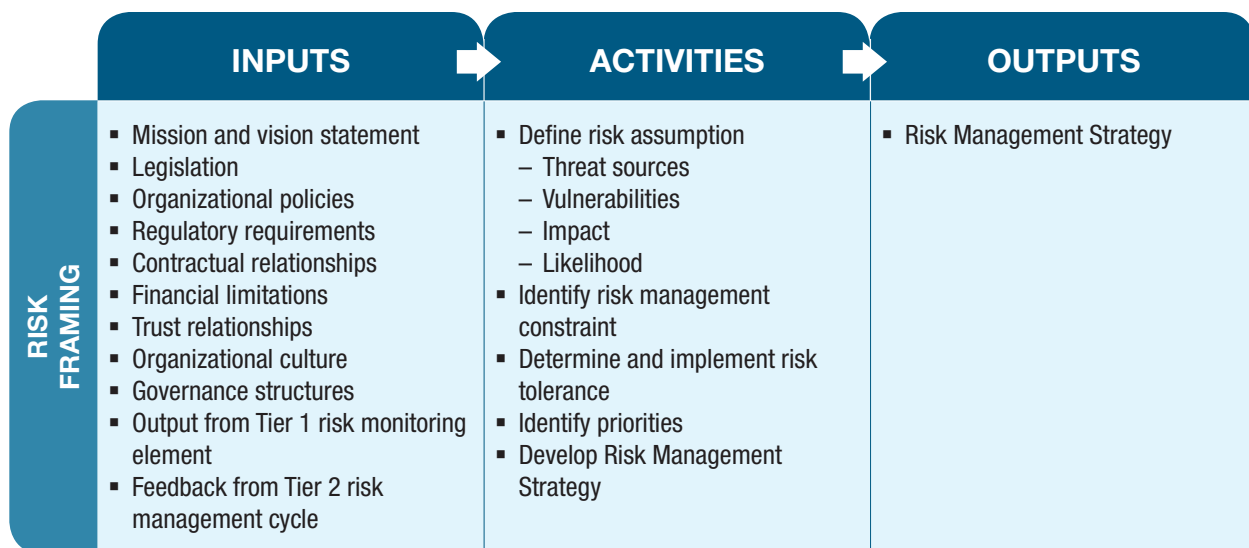
The RMP at Tier 1 produces an initial cybersecurity risk management strategy (if one does not already exist) that includes a risk assessment methodology, a risk monitoring strategy, and a cybersecurity governance program. This strategy is iteratively informed and revised based on outputs from Tiers 2 and 3. The cybersecurity Risk Management Strategy is the high-level document that changes over time to direct the organization on how to analyze and prioritize cybersecurity risk, risk tolerance, priorities, and goals of addressing cybersecurity risks. Generally, at Tier 1, organizations identify and prioritize mission and business processes. The mission and business processes owners and IT and ICS managers use the Cybersecurity Risk Management Strategy to allocate resources in a prioritized manner and also provide feedback to senior management on the effectiveness of the risk management program. The executive leadership uses institution of a governance program to provide focused and structured oversight and systematic review of the RMP.

3.1 RISK FRAMING AT TIER 1

Risk framing establishes the context and provides a common perspective for how an electricity subsector organization manages risk. The risk content and perspective will vary across organizations on the basis of their type and size. For instance, a small rural cooperative may have a fairly well-defined but limited scope of business that includes a few hundred distribution end points, a couple of generation assets, small field operations, and administration functions. This is dramatically different from a larger investor-owned utility that has millions of customers, interstate transmission assets, investments in large-scale generation facilities, and wholesale marketing activities. Risk framing for both of these organizations will reflect the realities of each organization, from the unique functions they perform to the specific assets they manage.

Once the operational environment is adequately framed, an organization will be able to appropriately assess, respond to, and monitor risk. The risk framing element makes explicit the specific risk assumptions, risk management constraints, tolerances, priorities, and trade-offs used within organizations for making investment and operational decisions.

TIER 1: THE ELECTRICITY SECTOR ORGANIZATION



3.1.1 Inputs

Source inputs to the Tier 1 risk framing element may include:

- Mission and vision statements;
- Legislation (international, Federal, regional, State, local, and Tribal);
- Organizational policies;
- Regulatory requirements (e.g., NERC registration and functional model);
- Contractual relationships (e.g., third-party agreements, service-level agreements, memoranda of understanding, and memoranda of agreement);
- Financial limitations;
- Trust relationships, both internal and external to the organization;¹⁶
- Organizational culture, both internal and external to the organization;
- Governance structures;
- Outputs from the Tier 1 risk monitoring elements;¹⁷ and
- Feedback from the Tier 2 risk management cycle.

¹⁶ Additional information about trust relationships and trust models can be found in Appendix E, Trust Models.

¹⁷ These outputs will not exist if this is the first time an organization is implementing the risk management lifecycle at Tier 1. These outputs will only exist once an organization has completed the risk management lifecycle at Tier 1 and Tier 2.



3.1.2 Activities

3.1.2.1 Define Risk Assumption

Risk assumption activities identify how risk is assessed, responded to, and monitored. As part of the framing element, the organization identifies and describes threat sources, vulnerabilities, impacts, and likelihood. This provides a common terminology and frame of reference throughout the organization for comparing and addressing risks across the disparate environment mission and business process areas. Additionally, at Tier 1, an organization may leverage threat scenarios, identified by industry associations and task forces, to enhance its approach to a complete risk analysis.

Threats

Threats can introduce undesirable events with adverse impacts on organizational operations, assets, individuals, and other organizations in the electricity subsector. During the framing element, the organization broadly identifies types of threats to their organization.

Threats may include:

- People (e.g., current/former employees, third-party personnel, the public);
- Processes (e.g., missing, deficient, or poorly implemented procedures);
- Technology (e.g., component failure through design, implementation, and/or maintenance);
- External disasters (e.g., natural or man-made); and
- Systemic, recurring cybersecurity incidents.

For all threats determined through the identification of threat sources, electricity subsector organizations should develop a concise description of:

- Types of tactics, techniques, and procedures employed by adversaries;¹⁸
- Threats mitigated by countermeasures (e.g., controls, safeguards);
- Threats not being addressed by countermeasures (e.g., controls, safeguards);
- Assumptions about threat targeting, intentions, and capabilities; and
- Credible and useful sources of threat information (e.g., electricity subsector Information Sharing and Analysis Center [ES-ISAC] and United States Computer Emergency Readiness Team [US-CERT]).

By identifying and describing threats at Tier 1, organizations provide a basis for aggregating and consolidating the results of risk assessments at Tier 2 into an overall assessment of risk throughout the organization.

¹⁸ Adversaries can be characterized in terms of threat levels (based on capabilities, intentions, and targeting) or with additional detail.

TIER 1: THE ELECTRICITY SECTOR ORGANIZATION

Vulnerabilities

Vulnerabilities are vectors that a threat may exploit to cause adverse impacts to IT and ICS in electricity subsector organizations. At Tier 1, vulnerabilities can be associated with deficiencies or weaknesses in organizational governance structures or processes. The vulnerabilities can also be associated with the susceptibility of organizations to adverse issues from external sources (e.g., technology owned or managed by third parties). As part of the risk framing element at Tier 1, the organization may:

- Provide guidance on how to consider dependencies on external organizations as vulnerabilities;
- Identify the degree of specificity with which vulnerabilities are described (e.g., identification of weak or deficient cybersecurity controls);
- Determine how vulnerability information is shared across the organization, through its governance structure and communication processes;
- Identify sources of credible and useful vulnerability information; and
- Make explicit any assumptions about the degree of organizational, IT, and ICS vulnerability to specific threats.

Impact

Electricity subsector organizations provide guidance on how to assess impacts to operations (i.e., mission disruption, financial loss, image, and reputation), assets, and individuals. At Tier 1, the organization's senior executive leadership identifies which business impacts related to cybersecurity are considered at Tier 2. Additional impacts may be identified by Tiers 2 and 3, iteratively informing the process. A cybersecurity event can have varying impacts on an organization at different levels and in different time frames. For instance, a cybersecurity compromise of communications equipment used for transmission line management could lead to cascading failures across portions of the grid. The resulting downstream outages could result in dissatisfied customers, legal and regulatory actions, or impact on reputation brand and corporate value.



Likelihood

An electricity subsector organization can employ a variety of approaches for determining the likelihood of cybersecurity threat events. It may prefer quantitative¹⁹ risk assessments or qualitative²⁰ risk assessments, as is the case when the risk assessment involves a high degree of uncertainty. Likelihood determinations can be based on either threat assumptions or actual threat data (e.g., historical data on cyber attacks or specific information on adversary capabilities, intentions, and targeting). When specific and credible threat data is available (e.g., types of cyber attacks, attack trends, and frequencies of attacks), an organization may use empirical data and statistical analysis to determine specific probabilities of threat events occurring. It then selects a method consistent with its organizational culture and risk tolerance. To determine the likelihood of threats exploiting vulnerabilities, electricity subsector organizations can employ a variety of approaches, such as:

- Threat assumptions (e.g., historical data on cyber attacks, earthquakes);
- Threat modeling, such as comparison or perspective methods;
- Actual threat information (e.g., specific information on threat capabilities, intentions, and targeting);
- Empirical data and statistical analyses used to determine more specific probabilities of threats occurring; and
- Vulnerabilities identified at the individual weakness or deficiency level or at the root-cause level.

¹⁹ Quantitative risk is the use of measurable, objective data to determine asset value, probability of loss, and associated risks.

²⁰ Qualitative risk is the measure of risk or asset value based on rank or separation into categories such as low, moderate, high.

TIER 1: THE ELECTRICITY SECTOR ORGANIZATION

3.1.2.2 Identify Risk Management Constraint

Identification of constraints assists in providing requirements, determining priorities, and in making cost-effective decisions. Some organizations may be compelled to meet strict regulatory requirements (e.g., NERC CIP cybersecurity standards) that limit risk response options, while other organizations may be constrained by resource availability, contractual obligation, culture, or timing. Many IT and ICS assets in the electricity subsector must operate for long periods (possibly decades) without disruption. A lack of flexibility in changing legacy systems may drive the need to integrate more stringent cybersecurity controls into the systems upon initial deployment. Constraints to be considered by the organization include:

- Direct financial limitations (e.g., rate case agreements);
- Indirect financial limitations (e.g., financial obligations, debt financing);
- Legal, regulatory, and/or contractual requirements (e.g., divestiture obligations, union contracts);
- Organizational policies (e.g., restrictions on outsourcing);
- Organizational culture, which can impose indirect constraints on governance changes (e.g., precluding a shift from decentralized to hybrid governance structures); and
- Cultural constraints that limit the visibility into and between operational technology support and IT support organizations.

3.1.2.3 Determine and Implement Risk Tolerance

In the electricity subsector, organizations identify and communicate the level of risk tolerance acceptable in meeting their mission and business process objectives. At Tier 1, organizations will define their risk tolerance on the basis of the information developed in the risk framing element. There is no correct level of organizational risk tolerance. Rather, the degree of risk tolerance is (1) generally indicative of organizational culture, (2) potentially different for different types of losses/compromises, and (3) subject to the risk tolerance of executive leadership. The ramifications of risk management decisions that are based on risk tolerance are significant. They can vary between low risk tolerant organizations sacrificing critical business objectives in order to avoid an unacceptable risk and high risk tolerant organizations focusing on near-term business efficiencies at the expense of possible equipment failure.

It is important that the organization exercise due diligence in determining risk tolerance—recognizing how fundamental this decision is to the effectiveness of the risk management program. There are a variety of techniques for identifying risk tolerance. Additionally, risk tolerance is not determined solely by assessment of internal risks. Several external requirements (including regulation) may dictate that some risks cannot be accepted at all or that levels of risk mitigation may be predetermined. The organizations may define risk tolerance for other types of organizational and operational risks (e.g., financial, safety, compliance, or reputation) that will have an impact on cybersecurity risk.



3.1.3 Outputs

Outputs from the Tier 1 risk framing element produce a set of organizational policies, governance structure, and guidance that form the basis for the Risk Management Strategy and include:

- Scope of the organization's cybersecurity RMP (e.g., organizations covered, mission and business processes affected, how risk management activities are applied at Tier 1);
- Risk assessment guidance, including the description of threat, sources of threat information, example threat events (in particular, adversary tactics, techniques, and procedures), when to consider and how to evaluate threats, sources of vulnerability information, risk assessment methodologies to be used, and risk assumptions;
- Cybersecurity risk management constraints on executing risk management activities; and
- Organizational priorities relating to cybersecurity risk.

Many of the outputs of the risk framing element serve as inputs to the risk assessment element of the RMP.

3.2 RISK ASSESSMENT AT TIER 1

At the Tier 1 organization level, the risk assessment element includes:

- Prioritizing investment strategies for business units or functions; and
- Establishing a standard risk assessment methodology or provide guidance for consistent implementation of risk assessment across the enterprise.

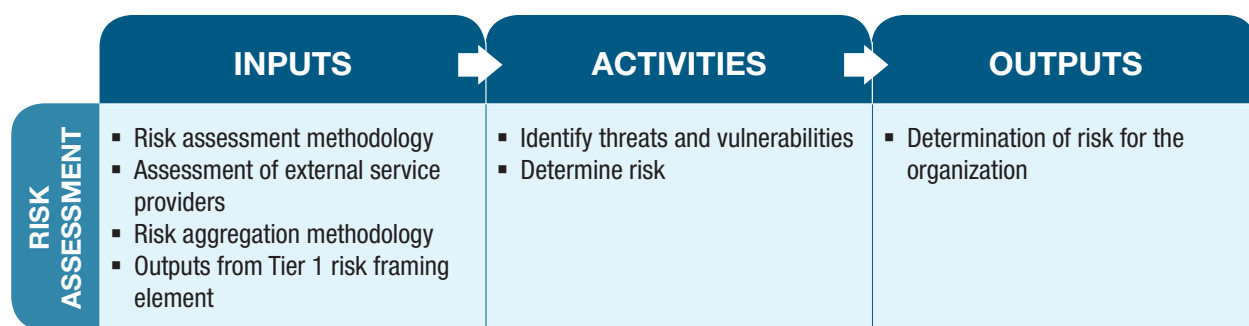
Risk assessments conducted at Tier 1 are used to refine threat, vulnerability, likelihood, and impact information in assessments conducted in Tier 2. Organization-wide risk assessments in the electricity subsector provide some initial prioritization of risks for the organization's leadership to consider when moving to the risk response element.

Risk assessments should be treated as a regularly repeated process and not a one-time activity. Keeping risk assessments up-to-date provides many potential benefits, such as timely and relevant information that enable senior executive leadership to perform continuous risk management. The frequency of risk assessments is determined by the organization based on a number of variables such as criticality of functions, technological changes, and resource constraints.

A Tier 1 organization could be seen as the investment holding company of a number of related businesses involved in the generation, transmission, and distribution of electricity. The business goal is for maximum communication, consistency, and enhanced value. To achieve this, an organization sets standards for risk assessment by reviewing assessments already performed in the organization's operations environment and sets the standards for all of the related businesses to follow.

TIER 1: THE ELECTRICITY SECTOR ORGANIZATION

Organizations may determine that conducting comprehensive risk assessments does not provide sufficient value or is too overwhelming. In such situations, electricity subsector organizations may consider conducting incremental and/or differential risk assessments. An incremental risk assessment considers only new information (e.g., the effects of using a new piece of technology on mission and business processes), whereas a differential risk assessment considers how changes affect the overall risk determination. Incremental or differential risk assessments are useful if organizations require a more targeted review of risk, seek an expanded understanding of risk, or desire an expanded understanding of the risk in relation to its mission and business processes.



3.2.1 Inputs

Inputs to the Tier 1 risk assessment element may include:

- Determining organizationally consistent risk assessment methodologies;²¹
- Determining breadth and depth of analysis employed during risk assessments;
- Defining the level of granularity required for assessing threats and vulnerabilities;
- Deciding whether and/or how to assess external service providers;
- Deciding whether and/or how to aggregate risk assessment results from different organizational entities or mission and business processes organization-wide; and
- Outputs from the risk-framing element in Tier 1.

Organizational expectations on Tier 1 risk assessment methodologies, techniques, and/or procedures are shaped heavily by governance structures, risk tolerance, risk management constraints, priorities, culture, and trust.

²¹ Examples of risk assessment methodologies include NIST SP800-30, OCTAVE/SQUARE, RAM-E, ISO-27005, ISO-31000, probabilistic risk assessment (PRA), and Failure Mode Effects and Analysis (FMEA).



3.2.2 Activities

3.2.2.1 Identify Threats and Vulnerabilities

A Tier 1 risk assessment focuses on the identification of threats to and vulnerabilities of an organization. Threat analysis requires an examination of threats, data, and events to estimate capabilities, intentions, and targeting information from many sources. Threat information generated at Tier 1 can be used to inform or refine the risk-related activities in Tier 2 and Tier 3. Vulnerabilities related to organizational governance and external dependencies are most effectively identified at Tier 1.

In many organizations, risk scenarios are developed where decision tree style risk determinations are used. Vendors and various supporting government organizations develop threat scenarios that are helpful in identifying and analyzing threats and vulnerabilities. These risk scenarios are constantly changing and will require routine review of threat assumptions used in organizational risk determination.

3.2.2.2 Determine Risk

At Tier 1, the organization determines that risk exists to its operations, assets, and individuals in the event that threats were to exploit identified vulnerabilities. Organizations determine risk by considering the likelihood that threats may exploit vulnerabilities, resulting in adverse impacts if such exploitations occur. Organizations use threat and vulnerability information, along with likelihood and impact information, to determine risk. This risk determination may be accomplished qualitatively or quantitatively.

Risk Determination and Uncertainty

The Tier 1 guidance for determining risk uncertainty indicates how combinations of likelihood and impact are combined to determine the risk level. During the risk framing element, organizations may have provided guidance on how to analyze risk and how to determine risk when a high degree of uncertainty exists. Uncertainty is a particular concern when a risk assessment considers advanced persistent threats (APTs)²² for which analysis of interacting vulnerabilities may be needed, knowledge of the APT is sparse, and past behavior may not be predictive.

Even with the establishment of explicit criteria, risk assessments are influenced by organizational culture and the personal experiences and accumulated knowledge of the individuals conducting the risk assessments. As a result, risk assessors may reach different

²² An APT is an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing/extending footholds within the IT and ICS infrastructure of the targeted organizations for the purposes of exfiltrating information; undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The APT (1) pursues its objectives repeatedly over an extended period of time, (2) adapts to defenders' efforts to resist it, and (3) is determined to maintain the level of interaction needed to execute its objectives.

TIER 1: THE ELECTRICITY SECTOR ORGANIZATION

conclusions from the same information. It is the responsibility of the organization's senior risk executive function to harmonize a consistent risk determination across the organization, while driving the organization to adopt justified risk response actions. The defined and applied processes of an organization provide the means to identify inconsistent practices and include processes to identify and resolve such inconsistencies.

3.2.3 Outputs

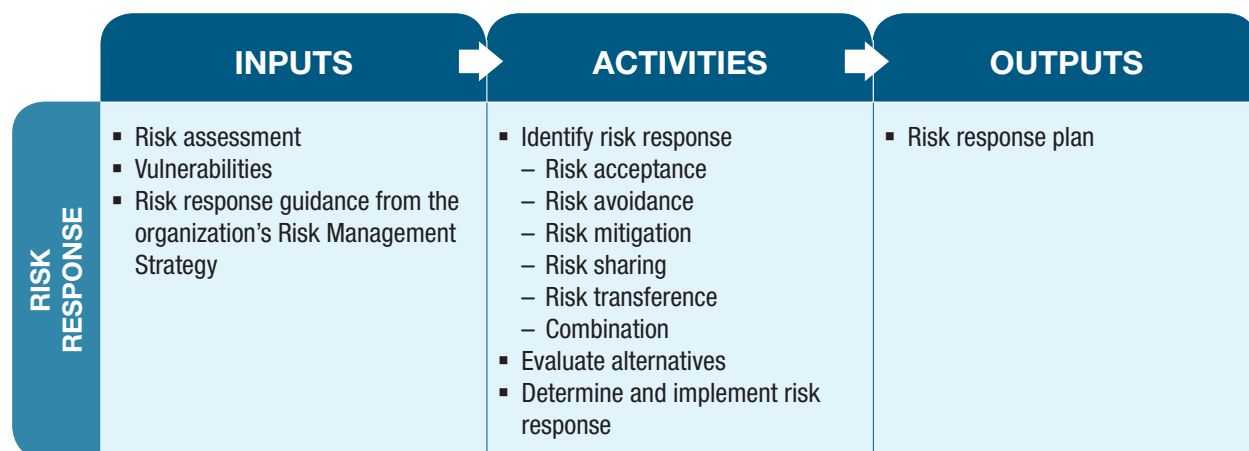
The output of the risk assessment element is a determination of risk to the organization's operations, assets, and individuals. Risk determination is the primary input for selecting appropriate risk responses in subsequent tiers and elements. The information collected in assessment activities is used to iteratively inform the risk determination on a regular basis. There are a variety of risk assessment methodologies that an organization may choose to employ. Each methodology has its own strengths and weaknesses that must be considered in determining which methodology to apply.

3.3 RISK RESPONSE AT TIER 1

For the risk response element at Tier 1, the organization evaluates, decides upon, and implements appropriate courses of action to the organization's operations, assets, individuals, and other organizations. Decisions on how to employ risk response measures across an organization may be made at Tier 1, although the decisions are informed by risk-related information from the lower tiers.

A utility that is responsible for electricity delivery recognizes the risk of earthquake or natural disaster to the generation and transmission functions conducted by contracted organizations. The utility finds its options to mitigate this risk to be highly limited and costly and, therefore, decides to take limited measures to address this risk. This would be an example of partial acceptance of risk by an electricity subsector organization at Tier 1.

Conversely, the same utility may have recently replaced all consumer meters with new meters that transmit data wirelessly. The risk is considered relatively low after the risk assessment is performed; however, consumer fears about privacy lead the small utility to invest in expensive data protection measures as a means to promote trust and alleviate any perceived risk. In this case, the acceptance of risk at Tier 1 will affect the operations and risk constraints at Tier 2 and Tier 3.





3.3.1 Inputs

Inputs to the Tier 1 risk response element may include:

- Risk assessment; and
- Risk response guidance from the organization's Risk Management Strategy.

3.3.2 Activities

3.3.2.1 Identify Risk Response

At Tier 1, risk response requires identifying alternative courses of action to respond to risk as determined during the risk assessment. A course of action is a time-phased or situation-dependent combination of risk response measures. Organizations can respond to risk in a variety of ways.²³

These include:

- Risk acceptance;
- Risk avoidance;
- Risk mitigation;
- Risk sharing;
- Risk transference; or
- Combinations of the above.

If an electric utility operation relied on new IT for telemetry of line and device information, the risk of failure of these devices could affect reliability, cybersecurity, and the safety of assets. A risk response the utility could incorporate is backup communications channels for fail over.

Risk Acceptance

Risk acceptance is the appropriate risk response when the identified risk is within the risk tolerance of the electricity subsector organization. In some instances, organizations may accept risk deemed to be low or moderate, depending on particular situations or conditions. Conversely, organizations that are subject to regulatory authorities will have a lower risk tolerance and may be restricted from accepting risk for specific business functions.²⁴

Organizations may make determinations on the general level of acceptable risk and the types of acceptable risk, while considering organizational priorities and trade-offs between:

- Near-term mission and business needs and the potential for long-term mission and business impacts;
- Organizational interests and the potential impacts on individuals and other organizations; and
- Regulatory requirements.

²³ Additional information about how an organization responds to risks can be found in Appendix G, Risk Response Strategies.

²⁴ For example, per NERC Reliability Standards, organizations in the electricity subsector with components deemed part of the critical infrastructure may not accept certain risks for said components.

TIER 1: THE ELECTRICITY SECTOR ORGANIZATION

Risk Avoidance

Risk avoidance involves taking specific actions to eliminate the activities or technologies that are the basis for the risk. Organizations revise or reposition activities or technologies to their mission and business processes to avoid the potential for unacceptable risk.

Risk Mitigation

Risk mitigation, also known as risk reduction, is the appropriate risk response for that portion of risk that cannot be accepted, avoided, shared, or transferred. The alternatives to mitigate risk depend on:

- The scope of risk response decisions assigned or delegated to the senior risk official, as defined by the organization's governance structure; and
- The organization's Risk Management Strategy and associated risk response strategies.

The means used by organizations in the electricity subsector to mitigate risk can involve a combination of risk response measures across all tiers.

Risk Sharing

Risk sharing is the appropriate risk response when an organization desires and has the resources to shift some risk liability and responsibility to other organizations. Risk sharing does not always reduce the impact of regulatory compliance enforcement or financial liability, unless the agreement(s) between the risk sharing organizations acknowledge transfer of both responsibility and liability. Risk sharing often occurs when organizations determine that addressing risk requires expertise or resources that are better provided by other organizations.

Risk Transference

Risk transference is the appropriate risk response when an organization desires and has the resources to shift risk liability and responsibility to other organizations. Risk transference shifts the entire risk responsibility or liability from one organization to another organization. It is important to note that risk transference reduces neither the likelihood of harmful events occurring nor the impact to an organization's operations, assets, individuals, or other organizations. Risk transference often occurs when organizations determine that addressing risk requires expertise or resources that are better provided by other organizations.

3.3.2.2 Evaluate Alternatives

In the risk response element, electricity subsector organizations evaluate alternative courses of action for responding to risk. The evaluation of alternative courses of action can include:

- How effectiveness is measured and monitored in achieving the desired risk response; and
- The feasibility of implementation throughout the expected period of time, during which the course of action is followed.



During the evaluation of alternative courses of action, trade-offs can be made explicit between near-term gains in mission and business effectiveness and/or efficiency and long-term risk to mission and business processes. A risk prioritization evaluation is conducted for each course of action to provide the information necessary for:

- Selecting between the courses of action; and
- Evaluating the courses of action in terms of response effectiveness, costs, mission and business impact, and any other factors deemed relevant to an electricity subsector organization.

Risk prioritization evaluation also considers the issue of competing resources. The organization should consider whether the cost for implementing a given course of action has the potential to adversely impact other missions or business functions, and, if so, to what extent.

3.3.2.3 Determine and Implement Risk Response

Decisions on appropriate courses of action include some form of prioritization. Some risks may be of greater concern than other risks. In such cases, more resources may be directed at addressing higher priority risks than lower priority risks. This does not mean that the lower priority risks would not be addressed. Rather, it could mean that fewer resources might be directed at the lower priority risks or that they may be addressed at a later time. A key part of the risk decision process is the recognition that, regardless of the decision, there still remains a degree of residual risk²⁵ that must be addressed. Organizations determine acceptable degrees of residual risk on the basis of their risk tolerance and the specific risk tolerances of particular decisionmakers. The specific beliefs and approaches that organizations embrace with respect to these risk-related concepts affect the courses of action selected by decisionmakers. Once a course of action is selected, it is incorporated into the Risk Management Strategy that is communicated throughout the organization and implemented.

When developing a Risk Management Strategy, each organization should consider options to effectively mitigate known risks while allocating justified resources. The balance between controlling costs and achieving risk management objectives requires analysis of all costs. Consequence costs resulting from a system breach are much harder to determine. Depending on the scope of systems and data involved in the Risk Management Strategy, organizations may consider the following elements to determine the cost of compromise:

- Impact from service disruption on both the organization and the clients it serves;
- Value of data lost;
- Brand damage;
- Shareholder value;
- Cost of incident response and recovery; and
- Fines, penalties, and potential litigation for damages.

²⁵ Residual risk is the risk that remains after a risk response has been applied.

TIER 1: THE ELECTRICITY SECTOR ORGANIZATION

Organizations have differing roles in the electricity subsector. Risk mitigation within the organization will vary depending upon the likelihood and severity of the consequences resulting from a security breach and the investment required.

3.3.3 Outputs

The output from the Tier 1 risk response element is a risk response plan that guides the implementation of the selected courses of action with consideration for:

- Individuals or organizational elements responsible for the selected risk response measures and specifications of effectiveness criteria (i.e., articulation of key risk and performance indicators and thresholds);
- Dependencies of each selected risk response measure on other risk response measures;
- Dependencies of selected risk response measures on other factors (e.g., the implementation of other planned IT measures);
- Timelines for implementation of risk response measures;
- Plans for monitoring the effectiveness of risk response measures;
- Triggers for risk monitoring;
- Results of response activities added to the Risk Management Strategy; and
- Interim risk response measures selected for implementation, if appropriate.

3.4 RISK MONITORING AT TIER 1

The risk monitoring element provides the organization with the means to determine the ongoing effectiveness of risk response measures and to identify risk impacting changes to the organization's IT and ICS and the operational environments. Analyzing the risk monitoring results provides the capability to maintain awareness of the risk being incurred, highlight the need to revisit the RMP, and initiate process improvement activities, as needed.²⁶

Organizations employ risk monitoring tools, techniques, and procedures to increase risk awareness. This enables senior leadership to develop a better understanding of the ongoing risk to organizational operations, assets, individuals, and other organizations. Risk monitoring is fundamental to strategic cybersecurity risk management because it improves threat awareness while providing the foundation to correlate controls in a way that moves beyond a singular defense strategy.

²⁶ Draft NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, provides guidance on monitoring organizational information systems and environments of operation.

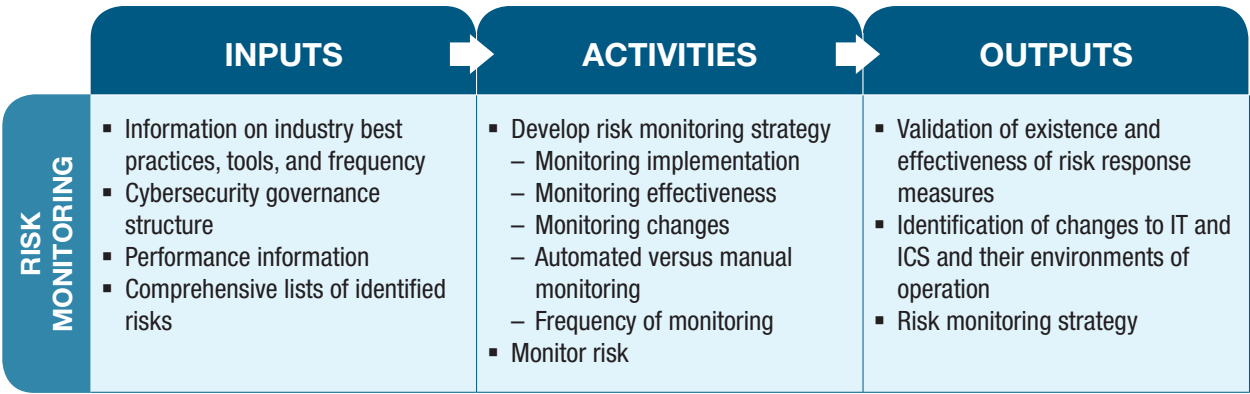


Senior leadership in the organization determines and verifies the metrics for evaluating the mission and business processes and procedures to ensure that the activities involving cybersecurity risk are being performed in an effective manner. Risk monitoring provides electricity subsector organizations with the means to:

- Verify risk response implementation;²⁷
- Determine the effectiveness of risk response measures; and
- Identify risk impacting changes to IT and ICS and the operational environments of operation.

Each organization may employ risk monitoring tools, techniques, and procedures to increase risk awareness. At Tier 1, monitoring activities might include ongoing threat assessments and how changes in the threat environment may affect Tier 2 and Tier 3 activities. This includes the organization’s enterprise and cybersecurity architectures, as well as its IT and ICS. Organization-level monitoring is another key part of the governance structure that establishes accountability for deploying and maintaining controls. The metrics used to monitor program effectiveness and reporting frequency are determined by the level of risk being managed in each business process within the organization.

At Tier 1, strategic criteria for continuous monitoring of cybersecurity are defined by the organization’s risk tolerance, how the organization plans to monitor risk given the inevitable changes to organizational IT and ICS and their environments of operation, and the degree and type of oversight the organization plans to use to ensure that the Risk Management Strategy is being effectively carried out. Metrics defined and monitored by officials at this level are designed to deliver information necessary to make risk management decisions in support of the organization’s governance structure.



²⁷ Implementation verification ensures that organizations have implemented required risk response measures and that cybersecurity requirements derived from, and traceable to, organizational mission and business processes, directives, regulations, policies, and standards and guidelines are satisfied.

TIER 1: THE ELECTRICITY SECTOR ORGANIZATION

3.4.1 Inputs

Inputs to the Tier 1 risk monitoring element include the strategy and implementation courses of action determined during the risk response element. Inputs to Tier 1 risk monitoring may also include:

- Information on industry best practices, tools, and frequency;
- Cybersecurity governance structure;
- Performance information; and
- Comprehensive lists of identified risks.

3.4.2 Activities

3.4.2.1 Develop Risk Monitoring Strategy

The organization develops a risk monitoring strategy that includes the purpose, type, and frequency of monitoring activities. The objective of a risk monitoring program is to:

- Verify that required risk response measures are implemented;
- Verify that cybersecurity requirements are derived from, and traceable to, the organization's mission and business processes;
- Determine the ongoing effectiveness of risk response measures after implementation;
- Identify changes to the organization's IT and ICS and the operational environments in which they operate;
- Monitor changes in the feasibility of the ongoing implementation of risk response measures;
- Determine how the risk monitoring programs directly impact the means used by the organization to conduct monitoring activities and where monitoring occurs;
- Determine the monitoring type to be employed, including approaches that rely on automation, procedural, or manual activities; and
- Determine how often monitoring activities are conducted, while balancing the value gained from frequent monitoring with potential for operational disruptions.

Monitoring Implementation

Implementation monitoring is employed to ensure that business process owners are implementing needed risk response measures. Failure to implement the risk response measures selected by the organization may result in the organization continuing to be subject to identified risks and may introduce the potential for failing to comply with regulatory requirements (e.g., legislation, regulations, standards) or organizational mandates (e.g., policies, procedures, mission and business requirements). Typically, the organization's senior risk executive will obtain feedback and reports as part of the governance structure from business process owners or function owners to determine whether implementation of the risk response strategy has been achieved.



Monitoring Effectiveness

Monitoring effectiveness is employed by the organization to determine if implemented risk response strategies have been successful in mitigating identified risks to the acceptable risk tolerance level. Although determining effectiveness is more complex than implementation monitoring, failure to achieve desired levels of effectiveness are indications that risk response measures are implemented incorrectly or not operating as intended. Additionally, risk response measures implemented and operating correctly do not guarantee an effective reduction of risk. This is primarily due to:

- The complexity of operating environments that may generate unintended consequences;
- Subsequent changes in levels of risk or associated risk;
- Inappropriate or incomplete criteria established as an output of the risk response element; and
- Changes in IT and ICS and the operational environments after implementation of risk response measures.

Monitoring Changes

In addition to implementation and effectiveness monitoring, the organization monitors changes to the IT and ICS and the operational environments in which they operate. Monitoring changes is not linked directly to previous risk response measures, but is important to detect changes that may affect the risk to an organization's operations, assets, individuals, and other organizations. Generally, such monitoring detects changes in conditions that may alter risk assumptions articulated in the risk framing element.

A utility determines that it has a good handle on its risk assessment and mitigation strategy. The organization wants to start a continuous monitoring program with automation tools to progress toward a systematic and higher level of cybersecurity for its organization. The utility begins with an inventory of all cybersecurity monitoring functions already in place by:

- Taking existing tools and collecting samples of the data and reporting it;
- Considering tools to help automate identification and status of all IT and ICS assets;
- Assessing and categorizing technology by asset type, system boundary, and risk level or importance; and
- Considering cybersecurity and compliance tool features that best match the needs for staff experience.

Organizations then focus on the regulatory reporting and requirements they have to meet. In the above example, the organization must already report specific compliance adherence with NERC CIP cybersecurity standards. This reporting offers a chance to reevaluate the tools and methods employed to achieve compliance with the NERC CIP cybersecurity standards.

TIER 1: THE ELECTRICITY SECTOR ORGANIZATION

Automated Versus Manual Monitoring

In Tier 1, monitoring typically involves reporting, analysis, and policy or strategy change recommendations. The governance structure within the organization assigns key metrics to track and evaluate on a routine basis. The organization may employ a semi-automated risk management application or dashboard to track and monitor key metrics. While the risks and controls may be technical, Tier 1 focuses on organization-level responsibilities that meet the expectations, mission, and other defined key business metrics of the organization's executive leadership/governing boards and shareholders.

Frequency of Monitoring

The frequency of risk monitoring (whether automated or manual) is driven by the mission and business processes of the organization, as well as the cost and ability to use the monitoring results to facilitate greater situational awareness. An increased level of awareness in the cybersecurity state of IT and ICS helps the organization develop a better understanding and management of risk. Risk monitoring frequency is also driven by other factors, such as:

- The anticipated frequency of changes in IT and ICS and the operational environments;
- The potential impact of risk if not properly addressed through appropriate response measures; and
- The degree to which the threat environment is changing.

The frequency of monitoring can also be affected by the type of monitoring conducted (i.e., automated versus manual approaches). Continuous monitoring²⁸ can provide significant benefits, especially in situations in which monitoring limits the opportunities of adversaries to gain access within an organization.

3.4.2.2 Monitor Risk

In the risk monitoring element in Tier 1, the organization monitors IT and ICS and the operational environments on an organization-defined metric to verify compliance, determine the effectiveness of risk response measures, and identify any changes. Once an organization completes development of their monitoring strategies and risk response methods, the strategies are implemented throughout the organization. Because the size and complexity of monitoring programs can be large, monitoring may be phased in or performed at different frequencies, based on the risk level or complexity of the risk response mechanism. The particular aspects of monitoring that are performed are dictated largely by the assumptions, constraints, risk tolerance, and priorities established during the risk framing element.

²⁸ Continuous monitoring is the process and technology used to detect risk issues associated with an electricity subsector organization's operational environment maintaining ongoing awareness to support organizational risk decisions.



Coordination of monitoring activities facilitates the sharing of risk-related information to provide early warning or trending for allocating risk response measures in a timely and efficient manner. If monitoring is not coordinated, then its benefit may be reduced and could undermine the overall effort to identify and address risk.

3.4.3 Outputs

The output from the Tier 1 risk monitoring element is a risk monitoring strategy that addresses the following:

- Verifying that required risk response measures are implemented;
- Verifying that cybersecurity requirements are derived from, and traceable to, the organizational mission and business processes;
- Determining the ongoing effectiveness of risk response measures; and
- Identifying changes to IT and ICS and the operational environments.

As part of the RMP, outputs from the risk monitoring element can be useful feedback to the risk framing element within each tier.

3.5 SUMMARY AT TIER 1

The risk management cycle for Tier 1 has been described as one of the risk executive functions, serving as the common risk management resource for senior leadership without prescribing a specific governance model. This could exist as a collection of executive managers, board of directors, or a committee of a cooperative organization. The Tier 1 function provides direction that management (at Tier 2 and Tier 3) uses to guide the operations of the organization. Providing a cybersecurity governance framework in most organizations includes a process to define expectations, provide policy and guidance, verify performance, and set constraints for organizational behavior. The RMP model assumes that governance functions for organizations exist at Tier 1 and can be enhanced to address cybersecurity risk issues.

The cybersecurity risk management program developed at Tier 1 is the high-level strategy that changes over time to direct the organization on how to analyze and prioritize cybersecurity risk, risk tolerance, organizational priorities, and the goals of addressing cybersecurity risks.

Table 2 provides an overview of the inputs, activities, and outputs from the risk framing, assessment, response, and monitoring elements in Tier 1 of the RMP. This table focuses on the typical inputs and outputs, but the list is not exhaustive.

TIER 1: THE ELECTRICITY SECTOR ORGANIZATION

Table 2: Tier 1 RMP Overview

	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Mission and vision statement ▪ Legislation ▪ Organizational policies ▪ Regulatory requirements ▪ Contractual relationships ▪ Financial limitations ▪ Trust relationships ▪ Organizational culture ▪ Governance structures ▪ Output from Tier 1 risk monitoring element ▪ Feedback from Tier 2 risk management cycle	▪ Define risk assumption – Threat sources – Vulnerabilities – Impact – Likelihood ▪ Identify risk constraint ▪ Determine and implement risk tolerance ▪ Identify priorities ▪ Develop Risk Management Strategy	▪ Risk Management Strategy
RISK ASSESSMENT	▪ Risk assessment methodology ▪ Assessment of external service providers ▪ Risk aggregation methodology ▪ Outputs from Tier 1 risk framing element	▪ Identify threat and vulnerability ▪ Determine risk	▪ Determination of risk for the organization
RISK RESPONSE	▪ Risk assessment ▪ Vulnerabilities ▪ Risk response guidance from the organization's Risk Management Strategy	▪ Identify risk response – Risk acceptance – Risk avoidance – Risk mitigation – Risk sharing – Risk transference – Combination ▪ Evaluate alternatives ▪ Develop and implement risk response	▪ Risk response plan
RISK MONITORING	▪ Information on industry best practices, tools, and frequency ▪ Cybersecurity governance structure ▪ Performance information ▪ Comprehensive lists of identified risks	▪ Develop risk monitoring strategy – Monitoring implementation – Monitoring effectiveness – Monitoring changes – Automated versus manual monitoring – Frequency of monitoring ▪ Monitor risk	▪ Validation of existence and effectiveness of risk response measures ▪ Identification of changes to IT and ICS and their environments of operation ▪ Risk monitoring strategy



4. Tier 2: Mission and Business Processes

At Tier 2, mission and business process owners consider cybersecurity risks from an operations perspective. They explicitly take into account any adverse impact a process may have on the mission objectives of the organization's operations. Within electricity subsector organizations, individual business units (i.e., lines of business) may be grouped into the domains of generation, transmission, distribution, markets, and field operations. The identification of the mission, along with corresponding business processes, assists in defining both the criticality and sensitivity of operational processes and associated information.

An enterprise cybersecurity architecture is an integral part of an organization's enterprise architecture. The enterprise cybersecurity architecture represents the portion of the enterprise architecture that specifically addresses IT and ICS resilience and security and provides information for the implementation of cybersecurity risk mitigation. The enterprise cybersecurity architecture is part of an organization's overall enterprise cybersecurity program, which relates to an organization's enterprise risk management program, overall IT/ICS governance, the enterprise architecture, and physical security activities. Cybersecurity program governance provides for the principles for security guidance, as well as development of policies, standards, guidelines, procedures, and audit enforcement processes. This governance structure ensures that cybersecurity requirements are consistently applied.

The primary output from Tier 2 of the RMP is the cybersecurity program and architecture that will be used in Tier 3.

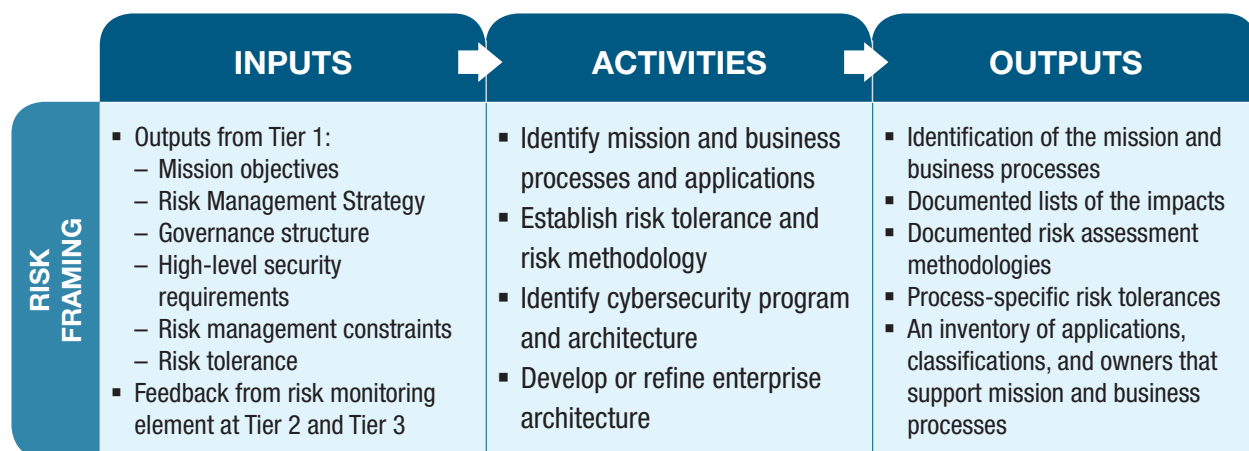
4.1 RISK FRAMING AT TIER 2

The risk framing element at Tier 2 identifies and documents the cybersecurity environment. Risk framing establishes a framework to guide the development of a cybersecurity program across the organization's mission and business processes. An essential input to this risk-framing element at Tier 2 is the Risk Management Strategy established in Tier 1. The organization and its business units identify the mission and business processes supporting the organization's objectives. Within Tier 2, the business units identify and map threats, vulnerabilities, consequences, and impacts to each of the mission and business processes identified.

Methodologies identified at Tier 1 are used to evaluate the impacts associated with the loss of confidentiality, integrity, and availability of IT and ICS resources, including information and data. The methodologies may be integrated into a risk measurement framework where risk assessment results from the evaluation of business processes can be harmonized. The resulting risks identified are rank-ordered as an input to the cybersecurity program. The resulting information from the risk assessments is used to determine management, technical, and operational controls and may be helpful in determining the appropriate mitigation of risk.

TIER 2: MISSION AND BUSINESS PROCESSES

The organization may assess this information to determine appropriate resources and funding needed for development and implementation of the cybersecurity program.



4.1.1 Inputs

Inputs to the risk framing element for Tier 2 may include the following outputs from Tier 1:

- Mission objectives;
- Risk Management Strategy;
- Governance structure;
- High-level security requirements;
- Constraints;
- Risk tolerance; and
- Feedback from the risk monitoring element at Tier 2 and Tier 3.

4.1.2 Activities

4.1.2.1 Identify Mission and Business Processes and Applications

In Tier 2, the organization inventories and documents its mission and business processes, as well as the applications²⁹ that support the mission objectives identified in Tier 1.

The mission and business processes derived from an analysis of the mission objectives may be shared across other business processes. These processes can be characterized as horizontal or vertical. Horizontal processes are those associated with cross-functional business processes, such as payroll, regulatory services, or IT services. Vertical processes are more specific to a business function, such as field or customer operations, transmission operations, or distribution engineering. A large organization, for example, may include a

²⁹ Application refers to a technology-enabled solution that supports the mission and corresponding business processes. The application is only defined at a level sufficient to identify the criticality to the mission and business processes.



number of vertical processes related to energy generation, transmission, distribution, trading, and customer relationship management. A specialized organization performing a limited set of reliability functions, such as reliability coordination and/or load and generation balancing authority, may have fewer such vertical processes. The relationship between these processes and applications, whether they are insourced or outsourced, is an important input for the risk assessment element later in this section.

The determination of how granular an organization needs to be in defining its business processes is a function of how the organization determines the highest level at which these business processes support a specific mission objective. These business processes are reviewed to identify their cybersecurity objectives (e.g., confidentiality, integrity, availability). From the cybersecurity risk management perspective, the commonality of cybersecurity objectives derived from the security requirements is an important input in the determination of common requirements across mission and business processes. Electricity subsector organizations may find useful guidance for identifying process in the functions as defined in the NERC Functional Model.³⁰

4.1.2.2 Establish Risk Tolerance and Risk Methodology

Once mission and corresponding business processes have been identified, each process is analyzed to establish process-specific cybersecurity risk assumptions and constraints. The impacts to the organization for the loss of confidentiality, integrity, and availability are established for each identified IT and ICS business process. Electricity subsector organizations may consider how regulatory and contractual constraints may influence the impact to the identified business processes. Some examples of such constraints are:

- Occupational Safety and Health Administration (OSHA) regulations;
- Health Insurance Portability and Accountability Act (HIPAA) for those organizations that process such information for internal health and medical-related processes;
- NERC reliability standards (CIP and others) for those organizations that are registered as NERC functional entities;
- NRC cybersecurity regulations;
- Payment Card Industry Data Security Standards (PCI-DSS) for organizations processing credit card payments from customers;
- Sarbanes-Oxley Act (SOX) requirements for qualified publicly listed companies;
- Federal Information Security Management Act (FISMA) requirements for U.S. Federal electricity subsector organizations; and
- Corporate contracts and/or agreements (including outsourcing and third parties).

³⁰ For additional information, see NERC Functional Model at <http://www.nerc.com>.

TIER 2: MISSION AND BUSINESS PROCESSES

Along with the impact assessment, process-specific risk tolerance needs to be established. Organizations consider the risk tolerance policies from the Tier 1 analysis and apply this guidance to each mission and business process. Risk tolerance may vary based on the impact to the mission or business process. Feedback from the risk assessment phase from Tier 2 and Tier 3, especially the impact, may provide essential input to this aspect of the framing process. Additional inputs to process-specific risk tolerance include sources of information for cybersecurity threats. Vulnerability assumptions (such as vendors, the ES-ISAC, Financial Services Information Sharing and Analysis Center [FS-ISAC], IT Information Sharing and Analysis Center [IT-ISAC], NERC Alert, ICS Cyber Emergency Response Team [ICS-CERT], and the US-CERT) may also be considered.

Risk assessment methodologies provide a standard way to measure impact across the organization (often expressed as financial impacts in dollar amounts or in a variable scale of high, medium, and low). However, any risk assessment methodology may define impact in different ways for groups of processes using qualitative analysis techniques. Generally, risk is calculated as a function of the threat, vulnerability, likelihood, and consequence/impact:

A customer relationship management process is relatively more tolerant of risks associated with loss of availability and integrity, but much less tolerant of risks associated with loss of confidentiality: unauthorized disclosure of personal identifiable information (PII) can have a high financial and reputation impact. On the other hand, processes associated with the reliable transmission and distribution of electric power are relatively more tolerant of risks associated with loss of confidentiality and less tolerant of risks associated with availability and integrity: inability to complete an operation in real time may result in loss of life or substantial damage to the electric infrastructure.

$$\text{Risk} = f(\text{threat, vulnerability, likelihood, consequence/impact})$$

Adoption of standard risk assessment methodologies for determining the impacts associated with the loss of confidentiality, integrity, and availability of IT and ICS are essential in providing input to the risk assessment element. When information on threats and their likelihood is not well defined, an option for determining relative risk level may be to focus on consequence/impact.

4.1.2.3 Identify Cybersecurity Program and Architecture

For organizations that currently maintain a cybersecurity program and architecture, it is during the risk assessment and risk response elements that an inventory of existing policies, architecture, and guidance are identified for validation. For organizations without a cybersecurity program and/or architecture, implementing the complete risk cycle in Tier 2 will assist in the development of these areas for your organization.



4.1.2.4 Develop or Refine Enterprise Architecture

Enterprise architecture is a management practice employed by organizations to maximize the effectiveness of their IT and ICS resources in supporting achievement of mission and business objectives. By developing the enterprise architecture or refining the existing enterprise architecture, organizations gain:

- A disciplined and structured approach for managing IT and ICS resources;
- Greater clarity and understanding of the infrastructure;
- Design and development of the associated IT and ICS for maximizing resilience;
- An opportunity to standardize, consolidate, and optimize resources;
- A common language for discussing risk management issues related to mission, business processes, and performance goals;
- Efficient, cost-effective, consistent, and interoperable cybersecurity capabilities to help the organization better protect mission and business functions; and
- The ability to segment, build redundancy, and eliminate single points of failure.

4.1.3 Outputs

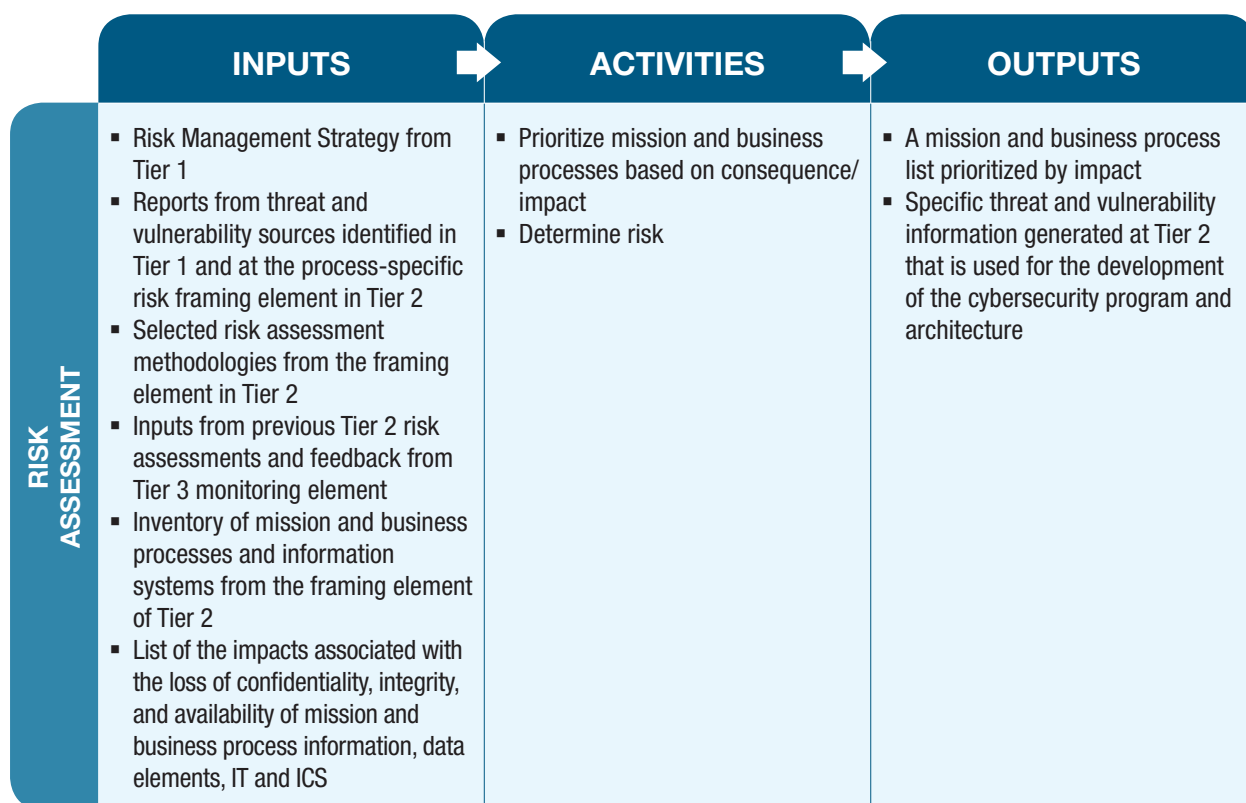
Outputs from the Tier 2 risk framing activities may include:

- Identification of mission and business processes that support the organization's Risk Management Strategy from Tier 1;
- Documented lists of impacts associated with loss of confidentiality, integrity, and availability of business process information, including data elements, and IT and ICS resources for both business administrative services and operations of electricity subsector resources;
- Documented risk assessment methodologies to be applied across all mission and business processes;
- Process-specific risk tolerances; and
- An inventory of information systems, data and/or information classifications, and business process owners supporting mission and business processes identified during the Tier 2 framing element.

4.2 RISK ASSESSMENT AT TIER 2

In the risk assessment element at Tier 2, mission and business processes and associated cybersecurity risks are identified using the selected risk assessment methodologies defined in the risk framing element in Tier 2. These risks are mapped to each of the mission functions, business processes, and the information systems supporting the organization. The assessment element includes the development of a prioritized list of processes based on the consequence/impact to the organization.

TIER 2: MISSION AND BUSINESS PROCESSES



4.2.1 Inputs

Inputs to the Tier 2 risk assessment element may include:

- The Risk Management Strategy from Tier 1;
- Reports from threats and vulnerability sources³¹ identified in Tier 1 and at the process-specific risk framing element in Tier 2;
- Selected risk assessment methodologies from the framing element in Tier 2;
- Inputs from previous Tier 2 risk assessments and feedback from Tier 3 monitoring element;
- Inventory of mission functions, business processes, and information systems developed from the framing element of Tier 2 that support the organization's mission objectives developed in Tier 1; and
- A documented list of impacts associated with loss of confidentiality, integrity, and availability of mission and business process information, data elements, and IT and ICS.

³¹ When reviewing the process-specific cybersecurity threat and vulnerability reports, organizations should make a determination on whether threat reports have provided enough information to determine a probability of threat.



4.2.2 Activities

4.2.2.1 Prioritize Mission and Business Processes Based on Consequence/Impact

In the assessment element of Tier 2, the organization first determines the consequence/impact for each mission and business process and application. In prioritizing mission and business processes, the organization considers the consequence/impact to the organization and the reliability of the electricity subsector.

4.2.2.2 Determine Risk

In determining risk at Tier 2, the organization focuses on organizational operations and vulnerabilities associated with enterprise architecture and mission and business processes. In some cases, these processes may have greater impact on the ability of the organization to successfully carry out its mission and business processes due to the potential impact across multiple IT and ICS mission environments. The organization reviews process-specific cybersecurity threat and vulnerability reports to decide whether these reports have provided enough information to determine threat likelihood.

In addition, an organization will prioritize each mission and business process to make risk response and monitoring decisions. The organization prioritizes the mission and business processes according to the determined risks and uses this prioritized list in the development of the cybersecurity program and architecture within the enterprise architecture.

4.2.3 Outputs

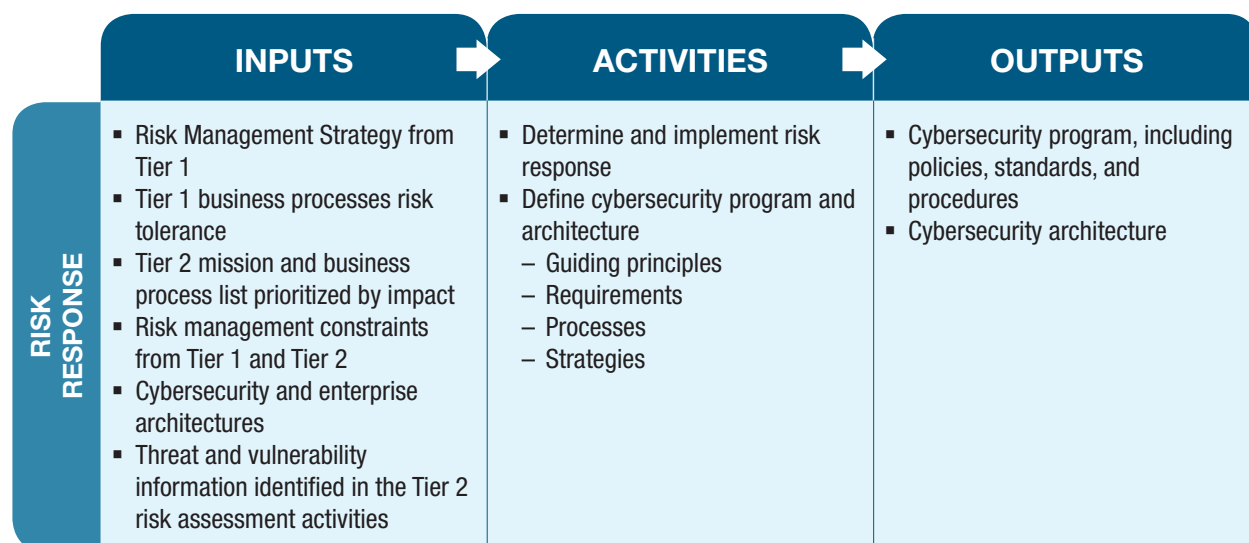
Outputs from the Tier 2 risk assessment element may include:

- A mission and business process list prioritized by impact and;
- Specific threat and vulnerability information generated at Tier 2 that is used for the creation of the cybersecurity program and architecture.

4.3 RISK RESPONSE AT TIER 2

In the Tier 2 risk response element, electricity subsector organizations use the list of mission and business processes prioritized by impact from the risk assessment element to determine the most appropriate risk response. In most cases, input from the risk assessment element also influences the design of the IT and ICS architecture itself due to considerations for meeting the requirements of the cybersecurity program.

TIER 2: MISSION AND BUSINESS PROCESSES



4.3.1 Inputs

Inputs to the Tier 2 risk response element may include:

- The Risk Management Strategy from Tier 1;
- The Tier 1 business processes risk tolerance;
- A Tier 2 mission and business process list, prioritized by impact;
- The risk management constraints from Tier 1 and Tier 2;
- The cybersecurity and enterprise architectures; and
- Threat and vulnerability information, identified in the Tier 2 risk assessment activities.

4.3.2 Activities

4.3.2.1 Determine and Implement Risk Response

Tier 2 risk response activities allow the organization to identify, evaluate, approve, and implement appropriate risk responses to accept, avoid, mitigate, share, or transfer risk to their operations, resources, and other organizations that may result from the operation and use of IT and ICS. As such, organizations develop risk mitigation strategies based on strategic goals and objectives, mission and business requirements, and organizational priorities.³²

³² Additional information on how an organization responds to risk can be found in Appendix G, Risk Response Strategies.



4.3.2.2 Define Cybersecurity Program and Architecture

During the response element of Tier 2, organizations develop and/or refine their cybersecurity program and architecture. The organization considers how they can inject cybersecurity architecture-planning activities into the definition of the enterprise architecture. Organizations may find it appropriate to define different cybersecurity architectural principles and ensure that connections or inheritance of cybersecurity controls between IT and ICS are clearly recognized.

A cybersecurity program may include:

- High-level policies and standards that define the objectives of the organization's cybersecurity program;
- Roles and responsibilities for the activities in the cybersecurity program;
- Establishment of minimum operating standards with common cybersecurity controls³³ that provide defense in depth and defense in breadth;
- Requirements and design principles for implementing controls, with consideration for various process-specific requirements;
- Procedures for implementing controls and enforcing policies;
- Transfer of operational high-impact risks to other mission and business processes; and
- Requirements and design principles for monitoring and measuring the effectiveness of the cybersecurity programs.

The cybersecurity architecture for organizations in the electricity subsector may include the following items.

Guiding principles for the protection of enclave boundaries (e.g., network perimeter controls, access controls, monitoring)

Some cyber systems may need to establish, identify, and authorize access as part of the cybersecurity architecture. This includes defining ingress and egress filtering and documenting data flows. To facilitate this process, system logs need to be maintained and correlated to identify anomalous communication. Robust access controls should also provide for authentication, authorization, and accounting of people, process, and technology.

³³ A common cybersecurity control is one that is utilized and/or inherited throughout an organization. Additional information about common controls can be found in Appendix H, Common Controls.

TIER 2: MISSION AND BUSINESS PROCESSES

Segmentation strategies for the various network enclaves and process types

Segmentation strategies for the various network types defined by cybersecurity requirements may include strategies for Internet connections, public carrier networks, virtual private networks (VPNs), corporate intranet networks, and high-value networks, such as ICS networks. These strategies provide guidance for the use of such controls as network firewalls (e.g., the use of various types of firewalls for controlling the ingress or egress of data from public networks or guidelines for network perimeter access to high value resources, and secured enclaves that are adjacent to business networks). Segmentation strategies for business processes (e.g., production, development, and test) that are determined by risk assessment to be high risk to mission and business processes may include increased intrusion detection and prevention monitoring.

Special requirements for generation plants, transmission, and distribution field assets

Many field assets have requirements for providing operational and nonoperational³⁴ data to engineering or business users for short- and long-term planning and analysis purposes. Organizations may provide standardized architectures to do this in a secure and controlled manner.

Data center and server farm environments

Organizations may provide standardized network architectures for providing secure services from network environments with a high concentration of systems providing common services such as Web application services, database services, or file services. The architecture will clearly stipulate those elements necessary to provide an adequate level of network access control and monitoring.

Separate remote access requirements for business and operations networks

The ability to remotely access systems for the purpose of maintenance and support is an important function. Organizations may provide a standardized architecture that would provide the level of cybersecurity controls commensurate with their risk profiles. Organizations should consider the threat environment

In the area of interactive remote access, a sample electric subsector organization implements a standardized architecture that uses a terminal service approach with printing and file-sharing restrictions for general interactive remote access to business services. This approach mitigates vulnerabilities associated with shared file services and data exfiltration. For access to its operations networks, the organization has implemented a standardized multitiered bastion host (jump-host) architecture and strong multifactor authentication that minimizes vulnerabilities associated with connections of the source to the target system or network.

³⁴ Operational data are data used to operate the system, such as line flows and breaker positions. Nonoperational data are data about the system operations, such as configuration information, asset management information, or event analysis data.



for the business process or class of business processes and provide architectural options for remote access to the business process, as guidance to selecting actual controls at Tier 3.

Guiding principles for end point protection

Organizations may consider an adequate level of standardization to optimize the end point management, taking into consideration differing cybersecurity requirements or priorities. These may include antivirus and malware protection, system integrity, system-level access controls, and cybersecurity event monitoring.

Standardized requirements for supply chain sourcing processes

Organizations in the electricity subsector should consider the standard cybersecurity requirements included in supply chain sourcing business processes. The organization should have a standardized business process for evaluation for cybersecurity requirements, by using standard frameworks for vendor qualification, technical evaluation, commercial evaluation, and selection processes.

Standardized requirements for change management, testing, and production certification processes

Organizations may consider standardized architectural elements necessary to develop a framework for change control, configuration management, testing, and certification and accreditation business processes to ensure that cybersecurity effectiveness is maintained. These elements may include standardized software tools and methodologies for managing system changes and testing across the organization.

Human resource practices relevant to cybersecurity

Organizations should establish repeatable on-boarding and off-boarding business processes to assess the suitability of the workforce. On-boarding business processes should include a personnel risk assessment (also known as a background investigation or check) that performs criminal history verification, identity verification (e.g., Social Security Number and driver's license), credit check, personal and professional reference check, and verification and validation of education and professional credentials. The personnel risk assessment may be updated based on risk classification determined by the organization. The organization may need to establish an off-boarding program as well to ensure that all system and physical access is appropriately removed. For cases in which an employee is terminated, organizations may consider establishing repeatable procedures to forensically maintain workforce systems for investigations.

TIER 2: MISSION AND BUSINESS PROCESSES

Standardized processes for cybersecurity incident response

Organizations may need to establish repeatable business processes that include training their workforce on how to identify, report, and respond to suspected cybersecurity incidents. The processes may need to account for creating the categories of events and incidents (e.g., denial of service, malicious code/software, and inappropriate use), the identification of the computer incident response team, and their roles and responsibilities. The purpose of the incident response plan is to have processes that determine whether an incident has occurred, whether the incident was contained and/or eradicated, and whether the system recovered from the incident. There may be defined processes for the forensic analysis and storage of incident evidence.

Standardized processes for business continuity of the business and disaster recovery for operations

Organizations may need to develop repeatable processes that are based on the classification and recovery point objectives (RPOs) and recovery time objectives (RTOs) to ensure that information systems are available to the organization. The degree to which business continuity and disaster recovery are supported by the organization may be different for each mission function and business process application.

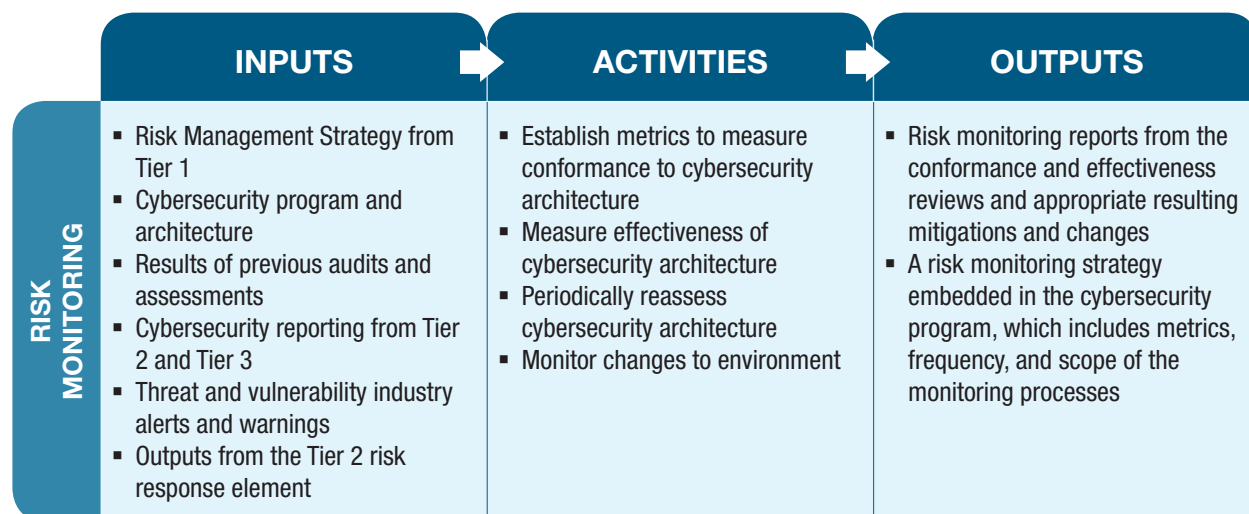
4.3.3 Outputs

Output for the Tier 2 risk response element includes:

- Cybersecurity program, including policies, standards, guidelines and procedures; and
- Cybersecurity architecture.

4.4 RISK MONITORING AT TIER 2

In the risk monitoring element, the organization monitors and measures the effectiveness and level of conformance to their cybersecurity program and architecture. This process helps identify the risk impact of changes to IT and ICS operational environments.





4.4.1 Inputs

Input to the Tier 2 risk monitoring element may include:

- The Risk Management Strategy from Tier 1;
- The cybersecurity program and architecture;
- The results of previous audits, assessments, and cybersecurity reporting from Tier 2 and Tier 3;
- Threat and vulnerability industry alerts and warnings; and
- The outputs from the Tier 2 risk response element.

4.4.2 Activities

To monitor the effectiveness of and measure the level of conformance to the cybersecurity program and architecture, the electricity subsector organizations may take the following actions.³⁵

4.4.2.1 Establish Metrics to Measure Conformance to Cybersecurity Architecture

A good measure of the appropriateness of cybersecurity architecture is the level at which the actual implementation of cybersecurity controls conform to that architecture. By periodically assessing the number of deviations from standard architecture and the rationales for these deviations, organizations can fine tune the architecture in an iterative process.

4.4.2.2 Measure Effectiveness of Cybersecurity Architecture

Measuring the effectiveness of cybersecurity architecture ensures that the defined architecture is implemented and still providing a valid framework for the selection of controls for Tier 3. This is usually conducted in conjunction with an assessment of the implemented controls through testing and analysis. The results of this assessment can then be used as input for the risk response element to help develop new or modified architectural elements for the cybersecurity architecture. For example, performance requirements may dictate a change from a proxy-based network access control architecture to an inspection-based network access control architecture. In turn, inspection-based access control may have limitations on behavioral analysis or the use of heuristics in malware prevention.

³⁵ Draft NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, provides guidance on monitoring organizational information systems and environments of operation.

TIER 2: MISSION AND BUSINESS PROCESSES

4.4.2.3 Periodically Reassess Cybersecurity Architecture

Organizations should define the frequency of comprehensive, organization-wide monitoring of the cybersecurity architecture to maintain its effectiveness and efficiency. Reassessment frequency should allow for comprehensive reviews and implementation of mitigation changes to the cybersecurity architecture.

The proliferation and use of personal mobile devices, both for personal and corporate application use, necessitates the review of the enterprise architecture and the cybersecurity architecture to incorporate components and policies that will support the secure implementation of processes and applications in IT and ICS environments.

4.4.2.4 Monitor Changes to Environment

Electricity subsector organizations should establish business processes to review changes to the threat and vulnerability landscape for input to the risk response element. For example, the evolution of threats from simple threats based on basic scripts to sophisticated APTs changes the cybersecurity architecture needs for risk response. Deviations from enterprise architectures are evaluated by the defined governance structure.

4.4.3 Outputs

Outputs from the Tier 2 risk monitoring activities may include:

- Risk monitoring reports from effectiveness and efficiency reviews and the appropriate resulting mitigations and changes; and
- A risk monitoring strategy embedded in the cybersecurity program, which includes metrics, frequency, and scope of the monitoring processes.

The output from the Tier 2 risk monitoring element will be the input to the risk framing element in Tier 3 and the feedback to Tier 2 and Tier 1.

4.5 SUMMARY AT TIER 2

At Tier 2, mission and business process owners refine the Risk Management Strategy and identify and prioritize the business processes that are critical to the organization's operations. It is at this tier that the cybersecurity program and architecture are refined as inputs to the activities at Tier 3 and as feedback to activities in Tier 1.

Table 3 provides an overview of the inputs, activities, and outputs from the risk framing, assessment, response, and monitoring elements in Tier 2 of the RMP.



Table 3: Tier 2 RMP Overview

	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	- Outputs from Tier 1: – Mission objectives – Risk Management Strategy – Governance structure – High-level security requirements – Risk management constraints – Risk tolerance - Feedback from risk monitoring element at Tier 2 and Tier 3	- Identify mission and business processes and information systems - Establish risk tolerance and risk methodology - Identify cybersecurity program and architecture - Develop or refine enterprise architecture	- Identification of the mission and business processes - Documented lists of the impacts - Documented risk assessment methodologies - Process-specific risk tolerances - An inventory of applications, classifications, and owners that support mission and business processes
RISK ASSESSMENT	- Risk Management Strategy from Tier 1 - Reports from threat and vulnerability sources identified in Tier 1 and at the process-specific risk framing element in Tier 2 - Selected risk assessment methodologies from the framing element in Tier 2 - Inputs from previous Tier 2 risk assessments and feedback from Tier 3 monitoring element - Inventory of mission and business processes and information systems from the framing element of Tier 2 - List of the impacts associated with the loss of confidentiality, integrity, and availability of mission and business process information, data elements, IT and ICS	- Prioritize mission and business processes based on consequence/impact - Determine risk	- A mission and business process list prioritized by impact - Specific threat and vulnerability information generated at Tier 2 that is used for the development of the cybersecurity program and architecture
RISK RESPONSE	- Risk Management Strategy from Tier 1 - Tier 1 business processes risk tolerance - Tier 2 mission and business process list prioritized by impact - Risk management constraints from Tier 1 and Tier 2 - Cybersecurity and enterprise architectures - Threat and vulnerability information identified in the Tier 2 risk assessment activities	- Determine and implement risk response - Define cybersecurity program and architecture – Guiding principles – Requirements – Processes – Strategies	- Cybersecurity program including policies, standards, guidelines, and procedures - Cybersecurity architecture
RISK MONITORING	- Risk Management Strategy from Tier 1 - Cybersecurity program and architecture - Results of previous audits and assessments - Cybersecurity reporting from Tier 2 and Tier 3 - Threat and vulnerability industry alerts and warnings - Outputs from the Tier 2 risk response element	- Establish metrics to measure the conformance to cybersecurity architecture - Measure the effectiveness of cybersecurity architecture - Periodically reassess cybersecurity architecture - Monitor changes to environment	- Risk monitoring reports from the effectiveness and efficiency reviews and appropriate resulting mitigations and changes - A risk monitoring strategy embedded in the cybersecurity program, which includes metrics, frequency, and scope of the monitoring processes



5. Tier 3: Information Technology and Industrial Control Systems

Tier 3 of the risk management model represents IT and ICS resources. At Tier 3, IT and ICS owners, common control providers, system and security engineers, and information system security officers make risk-based decisions on the implementation, operation, and monitoring of systems. To address risk at Tier 3, the risk management cycles use four elements—frame, assess, respond, and monitor—are applied. The major activities at Tier 3 use the outputs from the Tier 2 cybersecurity program and architecture and the Tier 1 Risk Management Strategy. Using these inputs, the organization inventories the resources, develops cybersecurity plans, evaluates the cybersecurity posture, selects appropriate controls, and evaluates the impact and effectiveness of those controls at the system level. The following sections provide a detailed description of the inputs, activities, and outputs for each of the elements.

It is acknowledged that IT and ICS have different cybersecurity requirements. An ICS is primarily concerned with availability. The ICS communication is time critical, with specific determination requirements for jitter and latency. Conversely, delays within an IT system database or Web page access are not unexpected by IT users. While the use of encryption or packet authentication is more common with an IT system to protect confidentiality and integrity, the same use in an ICS may reduce the level of ICS performance. The activities at Tier 3 will assist in determining the controls and risk responses that apply to the cybersecurity requirements of the IT and ICS.

5.1 RISK FRAMING AT TIER 3

	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Risk Management Strategy from Tier 1 ▪ Threat and vulnerability information from Tier 2 ▪ Prioritized list of mission and business processes, and information systems by impact/consequence from Tier 2 ▪ Catalog of cybersecurity controls ▪ Cybersecurity program and architecture ▪ Enterprise architecture ▪ Results from monitoring element of Tier 3 ▪ Inventory of current information systems and resources created at Tier 3	▪ Conduct IT and ICS inventory ▪ Define or refine cybersecurity plans	▪ Baseline cybersecurity plan, which includes the inventory of IT and ICS and identification of boundaries, and the list of threats and vulnerabilities

TIER 3: INFORMATION TECHNOLOGY AND INDUSTRIAL CONTROL SYSTEMS

5.1.1 Inputs

The inputs to the risk framing element at Tier 3 for IT and ICS may include:

- Risk Management Strategy from Tier 1;
- Threat and vulnerability information from Tier 2;
- Prioritized list of mission and business processes and information systems by impact/consequence from Tier 2;
- Catalog of cybersecurity controls;
- Cybersecurity program and architecture;
- Enterprise architecture;
- Results from monitoring element of Tier 3; and
- Inventory of current information systems and resources from Tier 3.

5.1.2 Activities

5.1.2.1 Conduct IT and ICS Inventory

The IT and ICS inventory process begins by identifying the information systems, resources, and relationships between IT and ICS; mission and business processes; and the information systems they support. The organization that owns, manages, and/or controls the resources is determined from the relationship between the mission and business process, the information and information system owner, and any contractual arrangements with internal or external organizations. This establishes authority and accountability for cybersecurity of the information systems and resources.

5.1.2.2 Define or Refine Cybersecurity Plans³⁶

For each IT and ICS, the organization gathers contextual information about the information system, including inventory, owners, network diagrams, data flows, and interfaces to other information systems. The cybersecurity plan addresses the technical configuration and cybersecurity posture of the information system. In the development of the cybersecurity plan, the organization identifies the common cybersecurity controls applicable to the IT or ICS.

The results of the cybersecurity plan development process influence both the selection and refinement of appropriate cybersecurity controls for IT and ICS, as well as the minimum assurance

The level of detail provided in the cybersecurity plan is determined by the organization, and information may be added to the description as it becomes available. Some organizations may have separate documents that contain different components of the cybersecurity plan. The RMP provides organizations the flexibility to decide whether their plan is one document or a collection of documents.

³⁶ Cybersecurity plan development outlines are provided by organizations such as the National Rural Electric Cooperative Association and NIST SP 800-18.



requirements. The cybersecurity plan process reviews organizational responsibilities for each information system in order to establish clear ownership to assess and respond to risk. The level of detail provided in the cybersecurity plan is determined by the organization, and information may be added to the description as it becomes available.

The cybersecurity plan for the IT and ICS may include:

- Full descriptive name, including associated acronym;
- Owner and risk official, including contact information;
- Parent or governing organization that manages, owns, and/or controls it;
- Location and environment of operations (narrative and diagram views);
- Version or release number of the IT and ICS applications and hardware;
- Purpose, functions, and capabilities of (mission and business processes supported) and sensitivity of each function;
- IT and ICS integration into the enterprise architecture and cybersecurity architecture;
- Threat and vulnerability information;
- Cybersecurity controls;
- Types and sensitivity of information processed, stored, and transmitted;
- Boundary for risk management and cybersecurity authorization purposes;
- Applicable laws, policies, regulations, or standards affecting cybersecurity;
- Architectural description, including network topology;
- Hardware, firmware, operating system and application software, and system interfaces (internal and external);
- Subsystems, components, and mechanisms (static and dynamic);
- Information flows and paths, including inputs and outputs;
- Network connection rules for external communications;
- Encryption techniques used for information processing, transmission, and storage;
- Authentication, authorization, and accounting controls that include shared accounts, administrative account, and user account management;
- Organizational affiliations, access rights, and privileges;
- Business continuity and/or disaster recovery requirements for RPO/RTO;
- Incident response points of contact;
- Cybersecurity assessment procedures; and
- Other information as required by the organization.

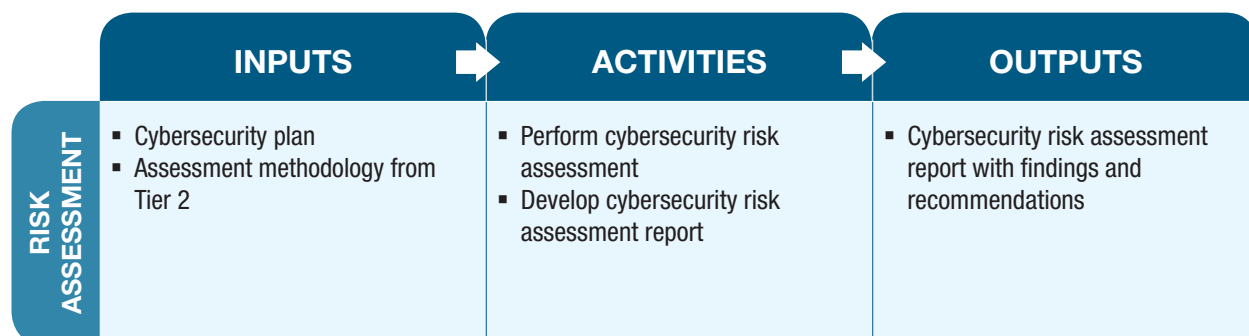
This information will be used during the assessment element to evaluate the system's alignment with the cybersecurity program and architecture.

5.1.3 Outputs

The outputs from the Tier 3 risk framing element include a baseline cybersecurity plan that includes an inventory of the IT and ICS, with identification of boundaries, and a list of threats and vulnerabilities.

TIER 3: INFORMATION TECHNOLOGY AND INDUSTRIAL CONTROL SYSTEMS

5.2 RISK ASSESSMENT AT TIER 3



5.2.1 Inputs

The inputs to the risk assessment element at Tier 3 are:

- Cybersecurity plan; and
- Assessment methodology from Tier 2.

5.2.2 Activities

5.2.2.1 Perform Cybersecurity Risk Assessment

This activity assesses the existing cybersecurity risk by using the risk assessment procedures defined in the cybersecurity plan.³⁷ The cybersecurity risk assessment considers new threats and vulnerabilities to guide the adjustment of existing controls and the selection of new controls. This is done by determining the extent with which the controls are implemented correctly, operating as intended, and producing the desired outcome, with respect to meeting the cybersecurity requirements for IT and ICS. Following the cybersecurity risk assessment, the organization determines the consequence/impact of the residual risk and prioritizes the results. The reliability and accuracy of risk determinations are dependent on the currency, accuracy, completeness, and integrity of information collected.

5.2.2.2 Develop Cybersecurity Risk Assessment Report

Organizations should prepare a cybersecurity risk assessment report, documenting issues, findings, and recommendations for correcting weakness identified during the cybersecurity control assessments. This assessment report includes the information necessary to demonstrate the effectiveness and efficiency of the cybersecurity controls employed within or inherited by IT and ICS. Cybersecurity control assessment results are documented with a level of detail appropriate for the assessment and in accordance with the reporting format prescribed by the policies of the organization.

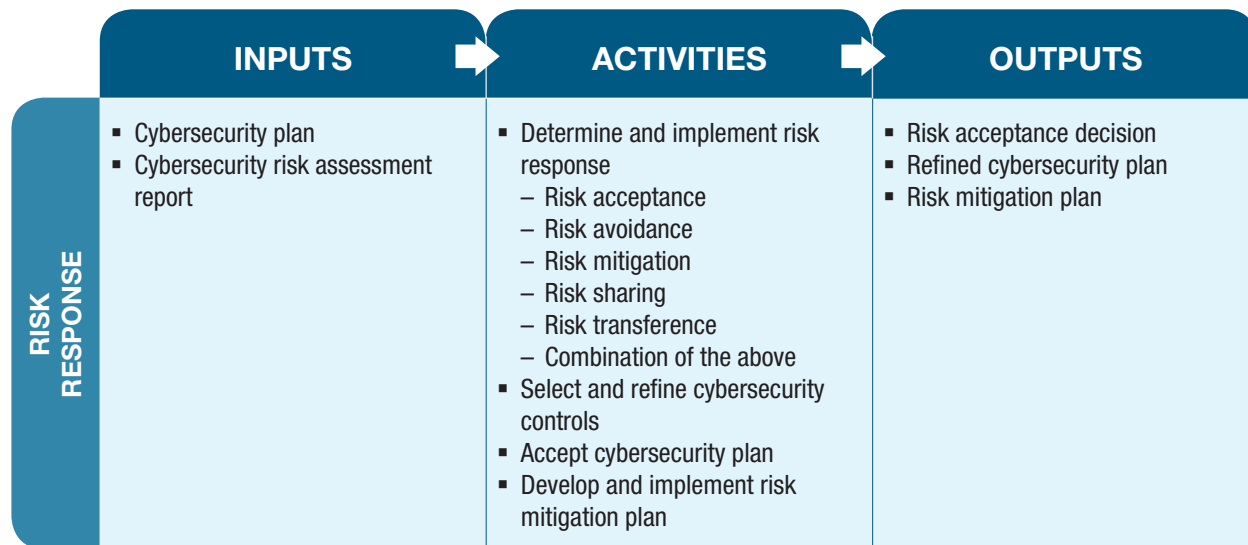
³⁷ The assessment may include penetration testing, vulnerability assessments, code reviews, software code reviews, and other appropriate tests.



5.2.3 Outputs

The output from the Tier 3 risk assessment element is a cybersecurity risk assessment report with findings and recommendations.

5.3 RISK RESPONSE AT TIER 3



5.3.1 Inputs

The inputs to the risk response element at Tier 3 are:

- Cybersecurity plan; and
- Cybersecurity risk assessment report.

5.3.2 Activities

5.3.2.1 Determine and Implement Risk Response

Based on the results of the cybersecurity risk assessment, organizations determine the appropriate risk response action.³⁸ These risk Response Actions may be:

- Risk acceptance;
- Risk avoidance;
- Risk mitigation;
- Risk sharing;
- Risk transference; or
- Combinations of the above.

The choice of available risk responses may be constrained by regulatory compliance regimes or other mandates. For example, the acceptance of risk is not available as part of the NERC CIP cybersecurity standards. Organizations are required to select and deploy the specific controls as defined by the standards.

³⁸ Additional information on how an organization responds to risk can be found in Appendix G, Risk Response Strategies.

TIER 3: INFORMATION TECHNOLOGY AND INDUSTRIAL CONTROL SYSTEMS

5.3.2.2 Select and Refine Cybersecurity Controls

Cybersecurity controls will be selected and refined based on the cybersecurity system categorization of IT and ICS. This is incorporated into the cybersecurity plan. The cybersecurity control selection process includes:

- Listing cybersecurity controls to be implemented;
- Tailoring the baseline cybersecurity controls for the system;
- Supplementing the tailored baseline cybersecurity controls, if necessary, with additional controls and/or control enhancements to address unique needs based on the risk assessment; and
- Describing the intended application of each control.

5.3.2.3 Accept Cybersecurity Plan

Upon completion of the cybersecurity plan, the senior executive (Tier 1) and system owner (Tier 2) review the plan and accept the response actions identified in the plan. This process documents the organizational acceptance of risk.

5.3.2.4 Develop and Implement Risk Mitigation Plan

The organization implements cybersecurity controls based on the findings and recommendations of the cybersecurity risk assessment report. The cybersecurity plan is updated based on the findings of the assessment and any remediation actions taken. The implementation of new controls or the modification of existing controls requires a reassessment to verify alignment with the cybersecurity plan. Once the response element is complete, the cybersecurity plan will contain an accurate list and description of the cybersecurity controls implemented, including compensating controls, and a list of residual vulnerabilities. The organization may also develop a risk mitigation plan reflecting the organization's priorities for addressing the remaining weaknesses and deficiencies in the IT and ICS operational environment. A mitigation plan identifies:

- The tasks to be accomplished, with a recommendation for completion either before or after IT and ICS implementation;
- Compensating controls and measures;
- The resources required to accomplish the tasks;
- Any milestones in meeting the tasks; and
- The scheduled completion dates for the milestones.



5.3.3 Outputs

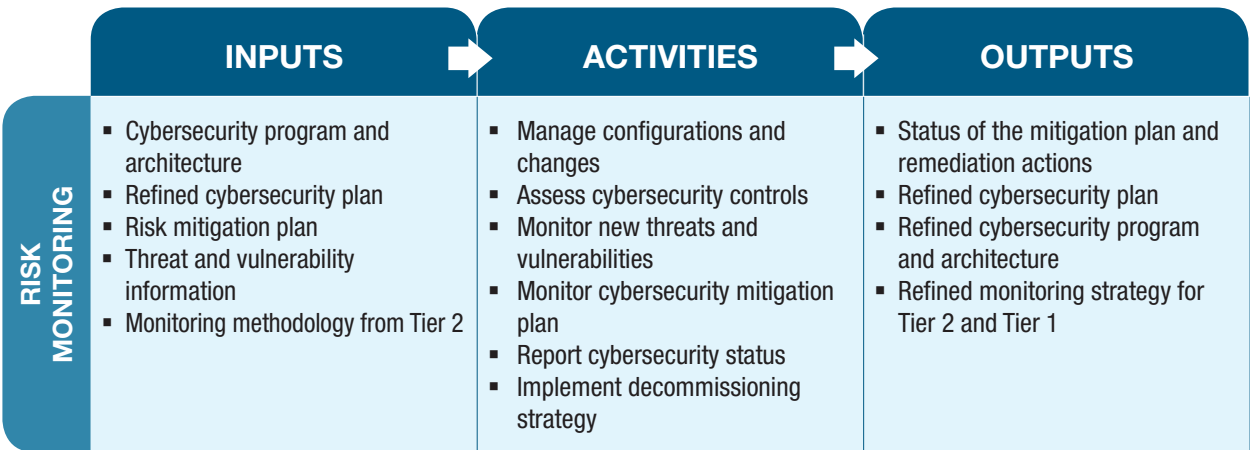
The outputs from the Tier 3 risk response element are:

- Risk acceptance decision;
- Refined cybersecurity plan; and
- Risk mitigation plan.

5.4 RISK MONITORING AT TIER 3

Ongoing monitoring of cybersecurity controls is essential for maintaining an effective cybersecurity plan. Organizations need to develop a strategy for the continuous monitoring of cybersecurity controls, to include review of any proposed or actual changes to IT and ICS. The implementation of a robust, continuous monitoring program allows an organization to understand the cybersecurity state over time and in a highly dynamic environment with changing threats, vulnerabilities, and technologies. An effective monitoring program includes:

- Configuration management and change control processes;
- Cybersecurity impact analyses on proposed or actual changes to IT and ICS;
- Assessment of selected cybersecurity controls employed; and
- Cybersecurity status reporting.



5.4.1 Inputs

The inputs to the risk monitoring element at Tier 3 are:

- Cybersecurity program and architecture;
- Refined cybersecurity plan;
- Risk mitigation plan;
- Threat and vulnerability information; and
- Monitoring methodology from Tier 2.

TIER 3: INFORMATION TECHNOLOGY AND INDUSTRIAL CONTROL SYSTEMS

5.4.2 Activities

5.4.2.1 Manage Technology Acquisition, Configuration, and Changes

Organizations implement processes that ensure technology acquisition and configuration accounts for risks to mission and business processes. A disciplined and structured approach to managing, controlling, and documenting changes to the IT and ICS operational environments is an essential element of an effective governance around the cybersecurity control monitoring program. It is important to record any relevant information about specific changes to hardware, software, or firmware, such as version or release numbers, descriptions of new or modified features/capabilities, and cybersecurity implementation guidance.

5.4.2.2 Assess Cybersecurity Controls

Organizations should assess a selected subset of the technical, management, and operational cybersecurity controls employed within, and inherited by, IT and ICS, in accordance with the Tier 1 monitoring strategy defined by the organization. The selection of cybersecurity controls to be monitored and the frequency of monitoring is based on the monitoring strategy developed by IT and ICS owner(s) and approved by the risk executive. Automation and tools are likely to be used to verify whether a control is working as described and whether it remains an effective mitigation to specific risks.

5.4.2.3 Monitor New Threats and Vulnerabilities

As part of the ongoing monitoring element, an organization needs to evaluate new threats and vulnerabilities identified during the framing element in Tiers 1 and 2 by reviewing and responding to additional vendor or industry warnings or alerts. To maintain an up-to-date awareness of threats and vulnerabilities, the organization should establish and maintain a schedule for checking applicable information sources and identify the personnel responsible for the task.

5.4.2.4 Monitor Cybersecurity Mitigation Plan

During the monitoring element, an organization should periodically evaluate the mitigation plan to correct weaknesses or deficiencies identified during the cybersecurity control assessment. Organizations may use this as a means to report system level cybersecurity status to management. Cybersecurity controls that are modified, enhanced, or added during the monitoring process are reassessed to ensure that appropriate corrective actions are taken to eliminate weaknesses or deficiencies or to mitigate identified risks.



5.4.2.5 Report Cybersecurity Status

Organizations should report IT and ICS cybersecurity status to the appropriate governance structure on an ongoing basis and in accordance with their monitoring strategy. This reporting includes the effectiveness and efficiency of cybersecurity controls employed within or inherited by IT and ICS. Organizations may need to review the reported cybersecurity status of IT and ICS on an ongoing basis and in accordance with the monitoring strategy to determine whether the risk to operations and resources remains acceptable. This reporting can be event driven, time driven or both. The cybersecurity status report provides:

- Organizational leadership with information on the cybersecurity state and the effectiveness and efficiency of deployed cybersecurity controls;
- A description of the ongoing monitoring activities;
- The IT and ICS owners information on how vulnerabilities are being addressed;
- Ongoing communication with executive leadership/governing boards; and
- A summary of changes to cybersecurity plans and cybersecurity assessment reports.

5.4.2.6 Implement Decommissioning Strategy

Organizations should implement a decommissioning strategy when resources are removed from service. When a resource is removed from operation, a number of risk management actions are required. Organizations should ensure that:

- Cybersecurity controls addressing system removal and decommissioning (e.g., media sanitization, configuration management, and control) are implemented; and
- Tracking and management systems (including inventory systems) are updated to indicate the specific components being removed from service.

5.4.3 Outputs

The outputs from Tier 3 risk monitoring element may include:

- Status of the mitigation plan and remediation actions;
- Refined cybersecurity plan;
- Refined cybersecurity program and architecture; and
- Refined monitoring strategy for Tier 2 and Tier 1.

TIER 3: INFORMATION TECHNOLOGY AND INDUSTRIAL CONTROL SYSTEMS

5.5 SUMMARY AT TIER 3

Tier 3 represents the application of the RMP to the IT and ICS resources. In Tier 3, organizations act on the outputs from the Tier 2 cybersecurity program and architecture and the Tier 1 Risk Management Strategy. Applicable cybersecurity controls are selected and applied to resources, based on cybersecurity baselines and risk assessments. Mitigation plans are used to monitor the progress of how and when identified residual risks are addressed during the cybersecurity risk assessment. The outputs of Tier 3 provide feedback to the Tier 2 and Tier 1 framing elements to reinform the risk assessment.

Table 4 provides an overview of the inputs, activities, and outputs from the risk framing, assessment, response, and monitoring elements in Tier 3 of the RMP.



Table 4: Tier 3 RMP Overview

	INPUTS	ACTIVITIES	OUTPUTS
RISK FRAMING	▪ Risk Management Strategy from Tier 1 ▪ Threat and vulnerability information from Tier 2 ▪ Prioritized list of mission and business processes and information systems by impact/consequence from Tier 2 ▪ Catalog of cybersecurity controls ▪ Cybersecurity program and architecture ▪ Enterprise architecture ▪ Results from monitoring element of Tier 3 ▪ Inventory of current information systems and resources from Tier 3	▪ Conduct IT and ICS inventory ▪ Define or refine cybersecurity plans	▪ Baseline cybersecurity plan that includes the inventory of IT and ICS and identification of boundaries, and the list of threats and vulnerabilities
RISK ASSESSMENT	▪ Cybersecurity plan ▪ Assessment methodology from Tier 2	▪ Perform cybersecurity risk assessment ▪ Develop cybersecurity risk assessment report	▪ Cybersecurity risk assessment report with findings and recommendations
RISK RESPONSE	▪ Cybersecurity plan ▪ Cybersecurity risk assessment report	▪ Determine and implement risk response – Risk acceptance – Risk avoidance – Risk mitigation – Risk sharing – Risk transference – Combination of the above ▪ Select and refine cybersecurity controls ▪ Develop and implement risk mitigation plan	▪ Risk acceptance decision ▪ Refined cybersecurity plan ▪ Risk mitigation plan
RISK MONITORING	▪ Cybersecurity program and architecture ▪ Refined cybersecurity plan ▪ Risk mitigation plan ▪ Threat and vulnerability information ▪ Monitoring methodology from Tier 2	▪ Manage technology acquisition, configuration, and changes ▪ Assess cybersecurity controls ▪ Monitor new threats and vulnerabilities ▪ Monitor cybersecurity mitigation plan ▪ Report cybersecurity status ▪ Implement decommissioning strategy	▪ Status of the mitigation plan and remediation actions ▪ Refined cybersecurity plan ▪ Refined cybersecurity program and architecture ▪ Refined monitoring strategy for Tier 2 and Tier 1



Appendix A References

LEGISLATION, POLICIES, DIRECTIVES, STANDARDS, AND GUIDELINES

1. American Recovery and Reinvestment Act (P.L. 111-5), February 2009.
2. Canada's Cyber Security Strategy, 2010.
3. *Canada-United States Action Plan for Critical Infrastructure*, 2010.
4. Canadian: Action Plan for Critical Infrastructure, 2009.
5. Canadian: National Strategy for Critical Infrastructure, 2009.
6. Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance (IA) Glossary*, April 2010.
7. Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, October 2009.
8. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
9. Energy Independence and Security Act of 2007 (P.L. 110-140, Title XIII–Smart Grid), December 2007.
10. Energy Sector Control Systems Working Group, *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, September 2011.
11. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
12. International Electrotechnical Commission 62443, *Security for Industrial Automation and Control Systems Series*.
13. ISO/IEC 15408:2005, *Common Criteria for Information Technology Security Evaluation*, 2005.
14. ISO/IEC 73:2009, *Risk Management—Vocabulary*, 2009.
15. ISO/IEC 31000:2009, *Risk Management—Principles and Guidelines*, 2009.
16. ISO/IEC 27000:2009, *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*, 2009.
17. ISO/IEC 27005:2011, *Information Technology—Security Techniques—Information Security Risk Management*, 2011.
18. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
19. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.
20. National Institute of Standards and Technology Interagency Report 7628, *Guidelines for Smart Grid Cyber Security*, August 2010.
21. National Institute of Standards and Technology Interagency Report 7298, Revision 1, *Glossary of Key Information Security Terms*, February 2011.

APPENDIX A REFERENCES

22. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
23. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.
24. National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.
25. National Institute of Standards and Technology Special Publication 800-70, Revision 1, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, September 2009.
26. National Institute of Standards and Technology Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010.
27. National Institute of Standards and Technology Special Publication 800-53A, Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010.
28. National Institute of Standards and Technology Special Publication 800-137, Initial Public Draft, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, December 2010.
29. National Institute of Standards and Technology Special Publication 1108, Release 1, *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, January 2010.
30. National Institute of Standards and Technology Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, (Projected Publication Spring 2011).
31. National Institute of Standards and Technology Special Publication 800-39, Revision 1, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011.
32. National Institute of Standards and Technology Special Publication 800-82, *Guide to Industrial Control Systems (ICS) Security*, June 2011.
33. North American Electric Reliability Corporation, *Version 4 Critical Infrastructure Protection Reliability Standards*, April 2012.
34. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
35. U.S. Department of Homeland Security (DHS), *DHS Risk Lexicon*, September 2010.



Appendix B Glossary

COMMON TERMS AND DEFINITIONS

This appendix provides definitions for security terminology used in this publication. The terms in this glossary are consistent with the commonly accepted standards, such as Software Engineering Institute (SEI), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), and Committee on National Security Systems (CNSS).

Assurance	Grounds for confidence that the set of intended security controls in an information technology (IT) and industrial control system (ICS) are effective in their application.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an IT and ICS.
Availability	Ensuring timely and reliable access to and use of information.
Common Cybersecurity Control	A common cybersecurity control is a cybersecurity control that is used and/or inherited throughout an organization.
Compensating Control	A compensating control is a cybersecurity control employed in lieu of a recommended control that provides equivalent or comparable control.
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Cyber Attack	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or for destroying the integrity of the data or stealing controlled information.
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber attacks.

APPENDIX B GLOSSARY

Cybersecurity Architecture

An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, cybersecurity systems, personnel, and subordinate organizations, showing their alignment with the organization's mission and strategic plans.

Cybersecurity Control Assessment

The testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the cybersecurity requirements for an IT and ICS or organization.

Cybersecurity Controls

The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an IT and ICS to protect the confidentiality, integrity, and availability of the system and its information.

Cybersecurity Plan

Formal document that provides an overview of the cybersecurity requirements for an IT and ICS and describes the cybersecurity controls in place or planned for meeting those requirements.

Cybersecurity Policy

A set of criteria for the provision of security services.

Cybersecurity Requirements

Requirements levied on an IT and ICS that are derived from applicable legislation, executive orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission and business case needs in order to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Cybersecurity Risk

The risk to organizational operations (including mission, functions, image, reputation), resources, and other organizations due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or IT and ICS.

**Cyberspace**

A global domain within the information environment consisting of the interdependent network of IT and ICS infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Defense-in-Breadth

A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).

Defense-in-Depth

Cybersecurity strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

Enterprise Architecture

The design and description of an enterprise's entire set of IT and ICS: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.

Environment of Operation

The physical surroundings in which an IT and ICS processes, stores, and transmits information.

Industrial Control System

Used to control industrial processes such as manufacturing, product handling, production, and distribution.

Information Technology

A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. In the context of this publication, the definition includes interconnected or dependent business systems and the environment in which they operate.

Integrity

Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.

APPENDIX B GLOSSARY

Management Controls	The security controls for an IT and ICS that focus on the management of risk and security.
Operational Controls	The security controls for an IT and ICS that are primarily implemented and executed by people (as opposed to systems).
Organization	An electricity subsector organization of any size, complexity, or positioning within an organizational structure that is charged with carrying out assigned mission and business processes and that uses IT and ICS in support of those processes.
Resources	Money, materials, staff, and other assets that can be used by an electricity subsector organization in order to meet its mission and business objectives.
Risk	A measure of the extent to which an organization is threatened by a potential circumstance or event, and typically a function of (1) the adverse impacts that would arise if the circumstance or event occurs and (2) the likelihood of occurrence.
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), resources, other organizations, and the Nation, resulting from the operation of an IT and ICS.
Risk Evaluation	A component of the risk assessment element in which observations are made on the significance and acceptability of risk to the organization.
Risk Management	The program and supporting processes to manage cybersecurity risk to organizational operations (including mission, functions, image, reputation), resources, other organizations, and the Nation, and includes (1) establishing the context for risk-related activities, (2) assessing risk, (3) responding to risk once determined, and (4) monitoring risk over time.
Risk Management Strategy	Any strategic-level decisions on how executive leadership/governing boards manage risk to an organization's operations, resources, and other organizations.



Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk reducing controls recommended from the RMP.
Risk Monitoring	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations, resources, and other organizations.
Security Objective	Security objectives are generally categorized as Confidentiality (<i>preventing unauthorized disclosure</i>), Integrity (<i>preventing modification or destruction of information</i>), and Availability (<i>preventing disruption of access to or use of information or an information system</i>).
Technical Controls	Cybersecurity controls for an IT and ICS that are primarily implemented and executed by the IT and ICS through mechanisms contained in the hardware, software, or firmware components of the system.
Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), resources, and other organizations through an IT and ICS via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Assessment	Process of evaluating the severity of threat to an IT and ICS or organization and describing the nature of the threat.
Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.
Vulnerability	Weakness in IT and ICS, system cybersecurity procedures, internal controls, or implementation that could be exploited by a threat source.
Vulnerability Assessment	Systematic examination of an IT and ICS or product to determine the adequacy of cybersecurity measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed cybersecurity measures, and confirm the adequacy of such measures after implementation.



Appendix C **Acronyms**

APT	Advanced Persistent Threat
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CNSS	Committee on National Security Systems
COTS	Commercial Off-the-Shelf
DOE	Department of Energy
ES-ISAC	Electricity Subsector Information Sharing and Analysis Center
FISMA	Federal Information Security Management Act
FS-ISAC	Financial Services Information Sharing and Analysis Center
IA	Information Assurance
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
IT	Information Technology
IT-ISAC	Information Technology Information Sharing and Analysis Center
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
PRA	Probabilistic Risk Assessment
RAM-E	Risk Assessment Methodology for Energy Infrastructures
RMP	Risk Management Process
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SP	Special Publication
SQUARE	Security Quality Requirements Engineering



Appendix D Governance Models

APPROACHES TO CYBERSECURITY GOVERNANCE

Governance in the electricity subsector can take many forms. Three approaches to cybersecurity governance can be used to meet organizational needs: (1) a *centralized* approach, (2) a *decentralized* approach, or (3) a *hybrid* approach. The authority, responsibility, and decision making power related to cybersecurity and risk management differ in each governance approach. The appropriate governance structure for an organization varies based on many factors (e.g., mission and business processes, size of the organization, organizational operations, resources, and risk tolerance).

Centralized Governance Model

In centralized governance structures, the authority, responsibility, and decision making power are vested solely within a central body. The centralized body establishes the policies, standards, guidelines, procedures, and processes for ensuring enterprise-wide involvement in the development and implementation of risk management and cybersecurity strategies, risk and cybersecurity decisions, as well as in the creation of internal and external communication mechanisms. A centralized approach to governance requires strong, well-informed central leadership and provides consistency throughout the organization. Centralized governance structures also provide less autonomy for subordinate organizations that are part of the parent organization.

Decentralized Governance Model

In decentralized cybersecurity governance structures, the authority, responsibility, and decision making power are vested in and delegated to individual subordinate organizations within the parent organization (e.g., business units). Subordinate organizations establish their own policies, standards, guidelines, procedures, and processes for ensuring the development and implementation of risk management and cybersecurity strategies, decisions, and mechanisms to communicate across the organization. A decentralized approach to cybersecurity governance accommodates subordinate organizations with divergent mission and business needs and operating environments. The effectiveness of this approach is greatly increased by the sharing of risk-related information among subordinate organizations, so that no subordinate organization is able to transfer risk to another without the latter's informed consent. It is also important to share risk-related information with parent organizations, as the risk decisions by subordinate organizations may have an effect on the organization as a whole.

APPENDIX D GOVERNANCE MODELS

Hybrid Governance Model

In hybrid cybersecurity governance structures, the authority, responsibility, and decision making power are distributed between the parent and the subordinate organizations. The central body establishes the policies, standards, guidelines, procedures, and processes for ensuring enterprise-wide involvement in the portion of the risk management and cybersecurity strategies and decisions affecting the entire organization (e.g., decisions related to shared infrastructure or common security services). Subordinate organizations, in a similar manner, establish appropriate policies, standards, guidelines, procedures, and processes for ensuring their involvement in the portion of risk management and cybersecurity strategies and decisions that are specific to their mission and business process needs and operational environments. A hybrid approach to governance requires strong, well-informed leadership for the organization as a whole and for subordinate organizations, and provides consistency throughout the organization for those aspects of risk and cybersecurity that affect the entire organization.



Appendix E Trust Models

APPROACHES TO ESTABLISHING TRUST RELATIONSHIPS

The following trust models describe ways in which electricity subsector organizations obtain the levels of trust needed to form partnerships internal and external to the organization, collaborate with other organizations, and share or receive information. No single trust model is inherently better than any other model. Rather, each model provides organizations with certain advantages and disadvantages on the basis of their circumstances (e.g., governance structure, risk tolerance, and criticality of organizational mission and business processes).

Validated Trust Model

In the *validated trust model*, one organization obtains information on the actions of another organization (e.g., the organization's cybersecurity policies, activities, and risk-related decisions) and uses the information to establish a level of trust with other organizations. An example of validated trust is when one organization develops an information technology (IT) or industrial control system (ICS) application and provides evidence (e.g., security plan, assessment results) that the application meets certain security requirements. The evidence offered may not fully satisfy the trust requirements or expectations. Additional evidence may be needed between organizations to establish trust. Trust is linked to the degree of transparency between two organizations with regard to risk and cybersecurity-related activities and decisions.

Historical Trust Model

In the *historical trust model*, the track record exhibited by an organization in the past, particularly in its risk and cybersecurity-related activities and decisions, can contribute to and help establish a level of trust with other organizations. While validated trust models assume that an organization provides the required level of proof needed to establish trust, obtaining such proof may not always be possible. In such instances, trust may be based on other deciding factors, including the organization's historical relationship or its recent experience in working with other organizations. For example, if one organization has worked with a second organization for years doing some activity and has not had any negative experiences, the first organization may be willing to trust the second organization in working on another activity, even though the organizations do not share any common experience for that particular activity. Historical trust tends to build up over time, with the more positive experiences contributing to increased levels of trust between organizations. Conversely, negative experiences may cause trust levels to decrease among organizations.

APPENDIX E TRUST MODELS

Third Party Trust Model

In the *third party trust model*, an organization establishes a level of trust with another organization on the basis of assurances provided by a mutually trusted third party. For example, two organizations attempting to establish a trust relationship may not have a direct trust history between them but do have a trust relationship with a third organization. The third party, which is trusted by both organizations, brokers the trust relationship between the two organizations, thus helping to establish the required level of trust, also known as transitive trust.

Mandated Trust Model

In the *mandated trust model*, an organization establishes a level of trust with another organization on the basis of a specific mandate issued by a third party in a position of authority. This mandate can be established by the respective authority through legislation, directives, regulations, or policies (e.g., a policy from an organization directing that all subordinate components of the organization accept the results of security assessments conducted by any subordinate components of the organization). Mandated trust can also be established when an organization is decreed to be the authoritative source for the provision of information resources, including IT products, systems, or services. For example, an organization may be given the responsibility and the authority to issue public key infrastructure (PKI) certificates for a group of organizations.

Hybrid Trust Model

In general, the trust models described above are not mutually exclusive. Each of the trust models may be used independently, as a stand-alone model, or in conjunction with another model. Several trust models may be used at times within the organization. Since electricity subsector organizations are diverse, it is possible that subordinate organizations may employ different trust models in establishing relationships with potential partnering organizations. The organizational governance structure may establish the specific terms and conditions for how the various trust models are employed in a complementary manner within the organization.



Appendix F Roles and Responsibilities

KEY PARTICIPANTS IN THE RISK MANAGEMENT PROCESS (RMP)

The following sections describe the roles and responsibilities of key participants involved in an organization's RMP.¹ Recognizing that organizations have widely varying missions and organizational structures, there may be differences in naming conventions for risk management-related roles and how specific responsibilities are allocated among organizational personnel (e.g., multiple individuals filling a single role or one individual filling multiple roles).² However, the basic functions remain the same. The application of the RMP across the three risk management tiers described in this publication is flexible, allowing organizations to effectively accomplish the intent of the specific tasks within their respective organizational structures to best manage risk.

RISK EXECUTIVE

The *risk executive* is a functional role (individual or group) established within organizations to provide a more comprehensive, organization-wide approach to risk management. The risk executive serves as the common risk management resource and coordinates with senior leaders and executives to:

- Establish risk management roles and responsibilities;
- Develop and implement an organization-wide Risk Management Strategy that guides and informs organizational risk decisions (including how risk is framed, assessed, responded to, and monitored over time);
- Manage threat and vulnerability information with regard to organizational information systems and the environments in which the systems operate;
- Establish organization-wide forums to consider all types and sources of risk (including aggregated risk);
- Determine organizational risk based on the aggregated risk from the operation and use of information systems and the respective environments of operation;
- Provide oversight for the risk management activities carried out by organizations to ensure consistent and effective risk-based decisions;
- Develop a greater understanding of risk with regard to the strategic view of organizations and their integrated operations;
- Establish effective vehicles and serve as a focal point for communicating and sharing risk-related information among key stakeholders internally and externally to organizations;
- Specify the degree of autonomy for subordinate organizations permitted by parent organizations with regard to framing, assessing, responding to, and monitoring risk;

¹ Organizations may define other roles (e.g., facilities manager, human resources manager, systems administrator) to support the RMP.

² Caution is exercised when one individual fills multiple roles in the RMP to ensure that the individual retains an appropriate level of independence and remains free from conflicts of interest.

APPENDIX F ROLES AND RESPONSIBILITIES

- Ensure that acceptance of the cybersecurity plan considers all factors necessary for mission and business success; and
- Ensure shared responsibility for supporting organizational missions and business functions through the use of external providers, receives an appropriate level of visibility and deliberation.

CHIEF INFORMATION OFFICER

The *chief information officer (CIO)* is an organizational official responsible for (1) designating a chief information security officer; (2) developing and maintaining cybersecurity policies, procedures, and control techniques to address all applicable requirements; (3) overseeing personnel with significant responsibilities for cybersecurity and ensuring that the personnel are adequately trained; (4) assisting senior organizational officials concerning their security responsibilities; and (5) coordinating with other senior officials.

INFORMATION OWNER

The *information owner* is an organizational official with statutory, management, or operational authority for specified information and is responsible for establishing the policies and procedures governing the generation, collection, processing, dissemination, and disposal of specified information. In information-sharing environments, the information owner is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility when the information is shared with or provided to other organizations. The owner of the information processed, stored, or transmitted by information technology (IT) and industrial control system (ICS) may or may not be the same as the IT and ICS owner. Information owners provide input to IT and ICS owners about the cybersecurity requirements and controls for the systems where the information is processed, stored, or transmitted.

CHIEF INFORMATION SECURITY OFFICER

The *chief information security officer* is an organizational official responsible for serving as the primary liaison for the CIO to the IT and ICS owners, common control providers, and information system security officers. The chief information security officer (1) possesses professional qualifications, including training and experience, required to administer the cybersecurity program functions; (2) maintains cybersecurity duties as a primary responsibility; and (3) heads an office with the mission and resources to assist the organization in achieving more secure information and IT and ICS.

IT AND ICS OWNER(S)

The *IT and ICS owner(s)* is/are responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an IT and ICS. The IT and ICS owner(s) also ensures/ensure for addressing the operational interests of the user community (i.e., individuals who depend upon the IT and ICS to satisfy mission, business, or operational requirements) with cybersecurity requirements.



SECURITY CONTROL ASSESSOR

The *security control assessor* is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an IT and ICS to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system). Security control assessors also provide an assessment of the severity of weaknesses or deficiencies discovered in the IT and ICS and their environments of operation and recommend corrective actions to address identified vulnerabilities. In addition to the above responsibilities, security control assessors prepare the final security assessment report containing the results and findings from the assessment. Prior to initiating the security control assessment, an assessor conducts an assessment of the security plan to help ensure that the plan provides a set of security controls for the IT and ICS that meet the stated security requirements.

INFORMATION SECURITY ARCHITECT

The *information security architect* is an individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organizational missions/business functions are adequately addressed in all aspects of enterprise architecture, including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes. The information security architect serves as the liaison between the enterprise architect and the information system security engineer. In addition, information security architects advise the chief information officer, chief information security officer, and risk executive on a range of security-related issues, including, for example, assessing the severity of weaknesses and deficiencies in the information system, risk mitigation approaches, security alerts, and potential adverse effects of vulnerabilities.

INFORMATION SYSTEM SECURITY ENGINEER

The *information system security engineer* is an individual, group, or organization responsible for conducting information system security engineering activities. Information system security engineering is a process that captures and refines information security requirements and ensures that the requirements are effectively integrated into IT component products and information systems through purposeful security architecting, design, development, and configuration. Information system security engineers employ best practices in software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques. System security engineers coordinate their security-related activities with the information security architects, chief information security officer, information system owners, and other security risk and compliance stakeholders.



Appendix G Risk Response Strategies

Organizations develop risk mitigation strategies based on strategic goals and objectives, mission and business requirements, and organizational priorities. These strategies provide the basis for making risk-based decisions for acceptance on the security solutions associated with and applied to information systems (information technology [IT] and industrial control system [ICS]) within the organization. Risk mitigation strategies are necessary to ensure that organizations are adequately protected against the growing threats to information processed, stored, and transmitted by organizational IT and ICS. The nature of the threats and the dynamic environments in which organizations operate demand flexible and scalable defenses, as well as solutions that can be tailored to meet rapidly changing conditions. These conditions include, for example, the emergence of new threats and vulnerabilities, the development of new technologies, changes in mission/business requirements, and/or changes to the operational environment. Effective risk mitigation strategies support the goals and objectives of organizations, and established mission and business priorities are tightly coupled with enterprise architectures and cybersecurity architectures.

Organizational risk mitigation strategies reflect the following:

- Mission and business processes are designed with regard to cybersecurity requirements;
- Enterprise architectures (including cybersecurity architectures) are designed with consideration for realistically achievable risk mitigations;
- Risk mitigation measures are implemented within organizational IT and ICS and their operational environments by cybersecurity controls (i.e., safeguards or countermeasures) consistent with cybersecurity architectures; and
- Cybersecurity programs, processes, and cybersecurity controls are highly flexible and agile with regard to implementation, recognizing the diversity in organizational mission and business processes, the variations in IT and ICS implementations and capabilities, and the dynamic environments in which the organizations operate.¹

Traditional risk mitigation strategies, with regard to threats from cyber attacks, at first relied almost exclusively on monolithic boundary protection. These strategies assumed adversaries were outside of some established defensive perimeter, and the objective of organizations was to repel the attack. The primary focus of static boundary protection was penetration resistance of the IT products and systems employed by the organization, as well as any additional cybersecurity controls implemented in the environments in which the products and systems operated.

¹ Dynamic environments of operation are characterized, for example, by ongoing changes in people, processes, technologies, physical infrastructure, and threats.

APPENDIX G RISK RESPONSE STRATEGIES

Recognition that IT and ICS boundaries were permeable, or porous, led to defense-in-depth as part of the mitigation strategy, relying on detection and response mechanisms to address the threats within the protection perimeter. In today's world characterized by advanced persistent threats (APTs), a more comprehensive risk mitigation strategy is needed—a strategy that combines traditional boundary protection with agile defense.

Agile defense assumes that a small percentage of threats from purposeful cyber attacks will be successful by compromising organizational IT and ICS through the supply chain,² by defeating the initial cybersecurity controls implemented by organizations, or by exploiting previously unidentified vulnerabilities for which protections are not in place or are inadequate. In this scenario, adversaries are operating inside the defensive perimeters established by organizations and may have substantial or complete control of organizational IT and ICS. Agile defense employs the concept of *information system resilience*—that is, the ability of systems to operate while under attack, even in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack. The concept of information system resilience can also be applied to the other classes of threats, including threats from environmental disruptions and/or human errors of omission/commission. The most effective risk mitigation strategies employ a combination of boundary protection and agile defenses, depending on the characteristics of the threat.³ This dual protection strategy illustrates two important cybersecurity concepts known as defense-in-depth⁴ and defense-in-breadth.⁵

The IT and ICS needed for mission and business success may be the same technologies through which threat actors cause mission and business failure. The risk response strategies developed and implemented by organizations may consider the type of IT and ICS and their functions and capabilities. Clearly defined and articulated risk response strategies help to ensure that executive leadership/governing boards take ownership and be ultimately responsible and accountable for risk decisions.

² Draft NIST Interagency Report 7622 provides guidance on managing supply chain risk.

³ Threat characteristics include capabilities, intentions, and targeting information.

⁴ *Defense-in-depth* is a cybersecurity strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

⁵ *Defense-in-breadth* is a planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).



The purpose of risk response is to provide a consistent, enterprise-wide response by (1) developing alternative courses of action for responding to risk, (2) evaluating the alternative courses of action, (3) determining appropriate courses of action consistent with organizational risk tolerance, and (4) implementing risk responses that are based on selected courses of action. There are five basic types of responses to risk: (1) accept, (2) avoid, (3) mitigate, (4) share, and (5) transfer. While each type of response can have an associated strategy, there may be an overall strategy for selecting from among the basic response types. This overall risk response strategy and the strategy for each type of response are discussed below. In addition, specific risk mitigation strategies are presented, including a description of how such strategies can be implemented within organizations.

OVERALL RISK RESPONSE STRATEGIES

A decision to accept risk must be consistent with the stated organizational tolerance for risk. Yet, there is still need for a well-defined, established organizational business process for selecting one or a combination of the risk responses of acceptance, avoidance, mitigation, sharing, or transfer. Organizations are often placed in situations in which there is greater risk than the designated executive leadership/governing boards desire to accept. Each of the risk responses are based on the organization's statement of risk tolerance at each tier. The objective of establishing a statement of risk tolerance is to identify, in clear and unambiguous terms, a limit for risk; that is, how far executive leadership/governing boards are willing to go with regard to accepting risk to organizational operations, resources, and other organizations.

RISK ACCEPTANCE STRATEGIES

Organizational risk acceptance strategies are essential companions to organizational statements of risk tolerance. Real-world operations, however, are seldom so simple as to make such risk tolerance statements the end statement for risk acceptance decisions. Risk acceptance includes the impact(s) resulting from the implementation of avoidance, sharing, transference, and/or mitigation response strategies. Organizational risk acceptance strategies place the acceptance of risk into a framework of organizational perspectives on dealing with the practical realities of operating with risk and provide the guidance necessary to ensure that the extent of the risk being accepted in specific situations is compliant with organizational direction. Inherent in the risk acceptance strategy is the identification of risk monitoring triggers to provide reasonable assurance that the risk accepted remains at or below the risk acceptance strategy.

APPENDIX G RISK RESPONSE STRATEGIES

RISK AVOIDANCE STRATEGIES

Risk avoidance entails restructuring business processes or information systems, or ending activities to eliminate potential exposure.

RISK SHARING STRATEGIES

Organizational risk sharing strategies enable risk decisions for specific organizational missions and business functions through policies, contracts, and agreements. Risk sharing strategies consider and take advantage of a lessening of risk by sharing the potential impact across internal or external organizations. Sharing risk involves delegating only partial responsibility or accountability.

RISK TRANSFER STRATEGIES

Organizational risk transfer strategies enable risk decisions for specific organizational missions and business functions through policies, contracts, and agreements. Risk transfer strategies consider and take full advantage of transferring the potential impact across internal or external organizations. Transferring risk involves delegating full responsibility or accountability.

RISK MITIGATION STRATEGIES

Organizational risk mitigation strategies reflect an organizational perspective on what mitigations are employed and where the mitigations are applied to reduce risks to organizational operations and resources and to other organizations. Risk mitigation strategies are the primary link between organizational risk management programs and cybersecurity programs—with the former covering all aspects of managing risk and the latter being primarily a part of the risk response component of the RMP. Effective risk mitigation strategies consider the general placement and allocation of mitigations, the degree of intended mitigation, and cover mitigations at each tier.

Information has value and must be protected. Information systems (including people, processes, and technologies) are the primary vehicles employed to process, store, and transmit such information—allowing organizations to carry out their missions in a variety of environments of operation and to ultimately be successful.



Appendix H Common Controls

INTRODUCTION

Common controls are security controls employed at the organization level that typically serve multiple information systems. By centrally managing and documenting the development, implementation, assessment, authorization, and monitoring of common controls, organizations can amortize security costs across multiple information systems. Examples of business process areas having common controls include contingency planning, incident response, security training and awareness, personnel security, physical and environmental protection, and security program management. These business process areas are generally good candidates for common controls.

IDENTIFICATION

Common controls are generally identified through an enterprise-wide exercise with the active involvement of the risk executive (function) and information technology (IT) and industrial control system (ICS) owners. The enterprise-wide exercise considers the cybersecurity risks and risk mitigation strategies of the organization. Common controls may be assigned to specific organizational entities (designated as common control providers) for development, implementation, assessment, and monitoring. Common control providers may also be the IT and ICS owners when the common controls reside in the IT or ICS system.

IMPLEMENTATION AND ASSESSMENT

The electricity subsector organization consults IT and ICS owners when identifying common controls to ensure that the security capability provided by the inherited controls is sufficient to deliver adequate protection. When the common controls provided by the organization are not sufficient for information systems inheriting the controls, the information system owners supplement the common controls with system-specific or hybrid controls to achieve the required protection for the system and/or accept greater risk.

Tier 1 ensures that common control providers keep common control information current since the controls typically support multiple organizational information systems. Common controls are documented in the cybersecurity plan and IT and ICS information system-specific cybersecurity plans for the information systems inheriting those controls.

Electricity subsector organizations ensure that common control providers have the capability to rapidly broadcast changes in the status of common controls that adversely affect the protections

APPENDIX H COMMON CONTROLS

being provided by and expected of the common controls. Common control providers are able to quickly inform information system owners when problems arise in the inherited common controls (e.g., when an assessment or reassessment of a common control indicates the control is flawed in some manner, or when a new threat or attack method arises that renders the common control less than effective in protecting against the new threat or attack method).

EXTERNAL PROVIDERS

If common controls are provided to the organization (and its information systems) by entities external to the organization (e.g., shared and/or external service providers), arrangements are made with the external/shared service providers by the organization to obtain information on the effectiveness of the deployed controls.

DOE/OE-0003

evaluation and reporting requirements; and (4) established the Government Performance and Results Act (GPRA) indicators for TCPCTIP.

With these waivers and extension of the project period, the current two TCPCTIP grantees may request continuation awards for FY 2013. We will consider continuation award requests under the current TCPCTIP statutory authority, subject to the requirements of 34 CFR 75.253, including the requirement that each grantee demonstrate that it is making substantial progress performing its TCPCTIP grant activities based on the requirements in our May 2007 notice inviting applications.

We will make decisions regarding continuation awards based on information provided in grantee requests for continuation awards, including information provided in program narratives, budgets and budget narratives, and performance reports. Any activities to be carried out during the continuation year must be consistent with, or be a logical extension of the scope, goals, and objectives of, each grantee's application as approved in the 2007 TCPCTIP competition.

Waiver of Delayed Effective Date

The Administrative Procedure Act requires that a substantive rule must be published at least 30 days before its effective date, except as otherwise provided for good cause (5 U.S.C. 553(d)(3)). During the 30-day public comment period on the notice of proposed waivers and extension of project period, no comments were submitted. Therefore, except for minor editorial and technical revisions, there are no differences between the proposed and final notices of waivers and extension of the project period for TCPCTIP. In addition, given the fact that the additional period of funding is only for a 12-month period, or longer if Congress continues to appropriate funds for TCPCTIP under the existing program authority, and to be able to make timely continuation grants to the two entities affected, the Secretary has determined that a delayed effective date is unnecessary and contrary to the public interest.

Regulatory Flexibility Act Certification

The Secretary certifies that these waivers and extension will not have a significant economic impact on a substantial number of small entities.

The small entities that will be affected by these waivers and extension are the two current TCPCTIP grantees.

The Secretary certifies that these waivers and extension will not have a

significant economic impact on these TCPCTIP entities because these waivers and extension impose minimal compliance costs to extend projects already in existence, and the activities required to support the additional year or years of funding will not impose additional regulatory burdens or require unnecessary Federal supervision. Furthermore, the costs of carrying out these activities could be paid for with program funds.

Paperwork Reduction Act of 1995

This notice of final waivers and extension does not contain any information collection requirements.

Intergovernmental Review

The TCPCTIP is not subject to Executive Order 12372 and the regulations in 34 CFR part 79.

Accessible Format: Individuals with disabilities can obtain this document in an accessible format (e.g., braille, large print, audiotape, or compact disc) on request to the program contact person listed under **FOR FURTHER INFORMATION CONTACT**.

Electronic Access to This Document: The official version of this document is the document published in the **Federal Register**. Free Internet access to the official edition of the **Federal Register** and the Code of Federal Regulations is available via the Federal Digital System at: www.gpo.gov/fdsys. At this site you can view this document, as well as all other documents of this Department published in the **Federal Register**, in text or Adobe Portable Document Format (PDF). To use PDF you must have Adobe Acrobat Reader, which is available free at this site.

You may also access documents of the Department published in the **Federal Register** by using the article search feature at: www.federalregister.gov. Specifically, through the advanced search feature at this site, you can limit your search to documents published by the Department.

Program Authority: 20 U.S.C. 2327.

Dated: May 18, 2012.

Johan Uvin,

Delegated Authority to Perform the Functions and Duties of the Assistant Secretary for Vocational and Adult Education.

[FR Doc. 2012-12542 Filed 5-22-12; 8:45 am]

BILLING CODE 4000-01-P

DEPARTMENT OF ENERGY

Electricity Subsector Cybersecurity Risk Management Process

AGENCY: Office of Electricity Delivery and Energy Reliability, Department of Energy.

ACTION: Notice of publication.

SUMMARY: This serves as public notification of the publication, by the Department of Energy (DOE) of the Electricity Subsector Cybersecurity Risk Management Process guideline. The guideline describes a risk management process that is targeted to the specific needs of electricity sector organizations. The objective of the guideline is to build upon existing guidance and requirements to develop a flexible risk management process tuned to the diverse missions, equipment, and business needs of the electric power industry. The document was posted on May 23, 2012.

FOR FURTHER INFORMATION CONTACT:

Request for additional information should be directed to Matthew Light at matthew.light@hq.doe.gov, phone 202-316-5115.

SUPPLEMENTARY INFORMATION: DOE has published the document entitled: Electricity Subsector Cybersecurity Risk Management Process. The primary goal of this guideline is to describe a risk management process that is targeted to the specific needs of electricity sector organizations. The objective of the guideline is to build upon existing guidance and requirements to develop a flexible risk management process tuned to the diverse missions, equipment, and business needs of the electric power industry.

The Electricity Subsector Cybersecurity Risk Management Process guideline was developed by the DOE, in collaboration with the National Institute of Standards and Technology (NIST), the North American Electric Reliability Corporation (NERC), and representatives from both the public and private sector. Additionally, the document was provided to the public during two public comment periods. The NIST Special Publication 800-39, Managing Information Security Risk provides the foundational methodology for this document.

The Electricity Sector Cybersecurity Risk Management Process Guideline is available at: <http://energy.gov/node/368191>.

Authority: Homeland Security Presidential Directive 7 (HSPD-7).

Issued at Washington, DC on May 18, 2012.

Patricia A. Hoffman,

Assistant Secretary, Electricity Delivery and Energy Reliability.

[FR Doc. 2012-12484 Filed 5-22-12; 8:45 am]

BILLING CODE 6450-01-P

DEPARTMENT OF ENERGY

Support of Deployment of Prototype Small Modular Reactors at the Savannah River Site

AGENCY: Savannah River Operations Office, Department of Energy (DOE).

ACTION: Notice of availability.

SUMMARY: DOE-Savannah River Operations Office (SR), in conjunction with the Savannah River National Laboratory (SRNL), announces the availability of support for deployment of Small Modular Reactors (SMR) on the Savannah River Site (SRS).

DATES: DOE-SR is available to discuss a program of support to domestic SMR developers until May 23, 2013.

ADDRESSES: The anticipated specific support available is outlined in a separate Document, "Products and Services Available to Small Modular Reactor (SMR) Vendors at the Savannah River Site (SRS)." Copies of that document may be obtained by contacting Sandra Johnson, the lead point of contact for siting SMRs at SRS. Ms. Johnson may be reached at 803-725-8997 or Sandra.Johnson@srs.gov.

FOR FURTHER INFORMATION CONTACT: Helen Belencan, DOE-SR, at 803-952-8696 or Helen.Belencan@srs.gov; or Ron Schroder, SRNL, at 803-952-6527 or Ronald.Schroder@srs.gov.

SUPPLEMENTARY INFORMATION: Support, via specific agreements between DOE-SR, SRNL and vendors, may include access to the SRS's real property, energy facilities, and nuclear expertise to support potential private sector development, testing and licensing of prototype SMR technologies for siting at SRS. DOE-SR welcomes inquiries from domestic SMR developers regarding the support that is available.

This Notice is not intended to create or remove any rights or duties, nor is it intended to affect any other aspect of DOE regulations. Furthermore, this Notice does not, and is not intended to, have the force and effect of law.

Issued at Aiken, South Carolina, on May 14, 2012.

David C. Moody,
Manager.

[FR Doc. 2012-12486 Filed 5-22-12; 8:45 am]

BILLING CODE 6450-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Project No. 9648-018]

Town of Springfield, Vermont and Siemens Westinghouse Technical Services, Inc., One Hundred River Street, LLC; Notice of Application for Transfer of License, and Soliciting Comments and Motions To Intervene

On November 15, 2011 and supplemented on April 27, 2012, the Town of Springfield, Vermont and Siemens Westinghouse Technical Services, Inc. (transferors) and One Hundred River Street, LLC (transferee) filed an application to transfer the license for the Fellows Dam Project No. 9648, located on the Black River in Windsor County, Vermont.

Applicants seek Commission approval to transfer the license for the Fellows Dam Project from the transferors to the transferee.

Applicants' Contacts: Transferors: Mr. Robert J. Forguites, Town Manager, Town of Springfield, 96 Main Street, Springfield, VT 05156, (802) 885-2104. Transferee: Mr. Richard Genderson, Managing Member, One Hundred River Street, LLC, 300 Massachusetts Ave. NE., Washington, DC 20002.

FERC Contact: Patricia W. Gillis (202) 502-8735, patricia.gillis@ferc.gov.

Deadline for filing comments and motions to intervene: 30 days from the issuance date of this notice. Comments and motions to intervene may be filed electronically via the Internet. See 18 CFR 385.2001(a)(1) and the instructions on the Commission's Web site under <http://www.ferc.gov/docs-filing/efiling.asp>. Commenters can submit brief comments up to 6,000 characters, without prior registration, using the eComment system at <http://www.ferc.gov/docs-filing/ecomment.asp>. You must include your name and contact information at the end of your comments. If unable to be filed electronically, documents may be paper-filed. To paper-file, an original plus seven copies should be mailed to: Kimberly D. Bose, Secretary, Federal Energy Regulatory Commission, 888 First Street NE., Washington, DC 20426. More information about this project can be viewed or printed on the eLibrary link of Commission's Web site at <http://www.ferc.gov/docs-filing/elibrary.asp>. Enter the docket number (P-9648) in the docket number field to access the document. For assistance, call toll-free 1-866-208-3372.

Dated: May 16, 2012.

Kimberly D. Bose,
Secretary.

[FR Doc. 2012-12446 Filed 5-22-12; 8:45 am]

BILLING CODE 6717-01-P

DEPARTMENT OF ENERGY

Federal Energy Regulatory Commission

[Project No. 1494-403]

Grand River Dam Authority; Notice of Application for Amendment of License and Soliciting Comments, Motions To Intervene, and Protests

Take notice that the following hydroelectric application has been filed with the Commission and is available for public inspection:

a. *Application Type:* Non-Project Use of Project Lands and Waters.

b. *Project No.:* 1494-403.

c. *Date Filed:* April 11, 2012.

d. *Applicant:* Grand River Dam Authority.

e. *Name of Project:* Pensacola Hydroelectric Project.

f. *Location:* The docking facilities will be located at Patricia Island on the west edge of Grove, Oklahoma in Delaware County, along the shoreline of the Grand Lake O' Cherokees.

g. *Filed Pursuant to:* Federal Power Act, 16 U.S.C. 791(a)-825(r).

h. *Applicant Contact:* Ms. Tamara E. Jahnke, Assistant General Counsel, Grand River Dam Authority, P.O. Box 409, Vinita, Oklahoma 74301, (918) 256-5545.

i. *FERC Contact:* Lorraine Yates at (678) 245-3084; or email: lorance.yates@ferc.gov.

j. *Deadline for filing comments, motions to intervene, and protests:* June 15, 2012.

All documents may be filed electronically via the Internet. See 18 CFR 385.2001(a)(1)(iii) and the instructions on the Commission's Web site at <http://www.ferc.gov/docs-filing/efiling.asp>. Commenters can submit brief comments up to 6,000 characters, without prior registration, using the eComment system at <http://www.ferc.gov/docs-filing/ecomment.asp>. You must include your name and contact information at the end of your comments. For assistance, please contact FERC Online Support at FERCOnlineSupport@ferc.gov or toll free at 1-866-208-3676, or for TTY, (202) 502-8659. Although the Commission strongly encourages electronic filing, documents may also be paper-filed. To paper-file, mail an original and seven copies to: Secretary,

From: [Kimberly Mielcarek](#)
To: [Kimberly Mielcarek](#)
Subject: NERC Announcements
Date: Wednesday, May 23, 2012 11:23:58 AM

Announcements

Spare Equipment Database Begins Operation

Click for [Database Announcement](#)

ATLANTA – The North American Electric Reliability Corporation’s (NERC) online spare equipment database is now operational. The inventory of spare equipment will be a helpful industry resource should a high-impact, low-frequency event result in damaged equipment. Providing information to the database is voluntary and meant to complement existing transformer sharing and mutual assistance agreements. The database is populated and managed by participating organization bound by a mutual confidentiality agreement. NERC’s initial focus is on high-voltage transmission and generator step-up transformers, which are vital for operation of the integrated bulk power system.

DOE Releases Risk Management Process Guideline

Click for [DOE Announcement](#), [RMP Guideline](#)

WASHINGTON, DC - The Department of Energy’s (DOE) Office of Electricity Delivery and Energy Reliability, in collaboration with the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC), today released guidance to help utilities better understand their cybersecurity risks, assess severity, and allocate resources more efficiently to manage those risks. The Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline, which provides a flexible approach to managing cybersecurity risks across all levels of the organization, was developed by a public-private sector team that was led by the Office of Electricity Delivery and Energy Reliability and included representatives from across the industry.

For more information or assistance, please contact [Kimberly Mielcarek](#).

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

You are currently subscribed to nerc-info as: lpedowicz@npcc.org
To unsubscribe send a blank email to leave-1292704-
325654.1ca6f85fb1574a8515cc07df72d3bfe0@listserv.nerc.com



**U.S. DEPARTMENT OF
ENERGY**

**OFFICE OF
ELECTRICITY DELIVERY
& ENERGY RELIABILITY**

News Media Contact: (202) 586-4940
For Immediate Release: May 23, 2012

Department of Energy Releases Electricity Subsector Cybersecurity Risk Management Process (RMP) Guideline

Public-Private Sector Collaboration Produces Guidance to Help Electric Utilities Better Understand and Assess Cybersecurity Risk

WASHINGTON, DC - The Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability, in collaboration with the National Institute of Standards and Technology (NIST) and the North American Electric Reliability Corporation (NERC), today released guidance to help utilities better understand their cybersecurity risks, assess severity, and allocate resources more efficiently to manage those risks. The Electricity Subsector Cybersecurity Risk Management Process (RMP) guideline, which provides a flexible approach to managing cybersecurity risks across all levels of the organization, was developed by a public-private sector team that was led by the Office of Electricity Delivery and Energy Reliability and included representatives from across the industry.

"Addressing cybersecurity is critical to enhancing the security and reliability of the nation's electric grid and must be done in a cost-effective manner," said Patricia Hoffman, Assistant Secretary for the Office of Electricity Delivery and Energy Reliability. "The Department of Energy has been working closely with the Department of Homeland Security, other government agencies, and industry for years to reduce the risk of energy disruptions due to cyber attack. The RMP guideline provides utilities with consistent, adaptable solutions that help them manage their cybersecurity risks more effectively."

Feedback provided by industry, vendors, and other electricity subsector stakeholders during two comment periods was invaluable in refining the final RMP guideline. The guideline is now [available](#) for downloading.

The electricity subsector increasingly relies on digital technology to reduce costs, increase efficiency, and maintain reliability during the generation, transmission, and distribution of electric power. Managing cybersecurity risk is critical to the success of organizations in achieving their strategic goals and objectives, including reliability, resiliency, security, and safety. DOE has a long history of working closely and steadily with Federal partners, including the Department of Homeland Security, on cybersecurity on the North American electric grid. All of these activities align with the *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, which was released in September 2011 by DOE and outlines a strategic framework over the next decade to design, install, operate, and maintain a resilient energy delivery system capable of surviving a cyber incident while sustaining critical functions. The Electricity Subsector Cybersecurity Risk Management Maturity Initiative, which will tie together elements from existing cybersecurity

efforts to develop a common model that allows electric utilities and grid operators to assess their cybersecurity capabilities and assist in prioritizing their investments, is the next logical step in a continued effort by public and private stakeholders to identify steps to improve the cybersecurity of the electric grid. The Electricity Subsector Cybersecurity Capabilities Maturity Model is expected to be available to the electricity subsector this summer.

To learn more about national efforts to ensure a reliable, secure, and resilient electric grid, visit the [Office of Electricity Delivery and Energy Reliability](#).

###

From: [Monica Benson](#)
To: [monica.benson@nerc.net](#)
Cc: [Kruempel, Gary E](#); [sac@nerc.com](#); [sac_plus@nerc.com](#); ["rb@nerc.com"](#); ["standards@nerc.com"](#); ["nercroster@nerc.com"](#); ["nercroster_plus@nerc.com"](#); ["nerc-info@nerc.com"](#); [maureen.long@nerc.net](#); [laura.hussey@nerc.net](#)
Subject: NERC: Standards Announcement - Standards Committee Segment 5 Special Election Final Ballot Results
Date: Thursday, May 24, 2012 11:50:32 AM

Standards Committee Announcement

Standards Committee Segment 5 Special Election Final Ballot Results

Standards Committee Segment 5 Special Election Results:

The second ballot (runoff ballot) for the election of a Standards Committee member to represent Industry Segment 5 for the vacant term expiring December 31, 2012 ended on Friday, May 18, 2012. In the second ballot, Gary Kruempel of MidAmerican Energy Company received the greatest number of votes and is elected to represent Segment 5.

Questions may be addressed to Monica Benson or 404-446-2573.

For more information or assistance, please contact Monica Benson at [monica.benson@nerc.net](#).

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | [www.nerc.com](#)

You have received this email because you are a registered representative in the Registered Ballot Body.

From: [Sandy Shiflett](#)
To: [Sandy Shiflett](#)
Subject: NERC Announcement: Lessons Learned
Date: Tuesday, June 19, 2012 1:51:23 PM

Announcement

Lessons Learned

June 19, 2012

Seven new lessons learned have been posted on the NERC website under the "[Event Analysis – Lessons Learned](#)" tab:

The new lessons address the following topics:

- Alarm Interpretation leads to Generator Stator Coil Failure
- Auxiliary Relay Contact Contamination
- EMS Database Corruption Problem
- Excessive Resource Utilization
- Protective Relaying Digital Input Board Loading Resistance
- Remote Terminal Units Not on DC Sources
- Unmanned Forklift Contact with Energized Bus

For more information or assistance, please contact [Sandy Shiflett](#).

**3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com**

You are currently subscribed to nerc-info as: lpedowicz@npcc.org
To unsubscribe send a blank email to leave-1295266-325654.1ca6f85fb1574a8515cc07df72d3bfe0@listserv.nerc.com

Lesson Learned

Alarm Interpretation Leads to Generator Stator Coil Failure

Category: Generation Facilities

Primary Interest Groups

Generator Owners (GO)
Generator Operators (GOP)
Transmission Operators (TOP)
Balancing Authorities (BA)
Reliability Coordinators (RC)

Problem Statement

A thermocouple temperature alarm condition was received at different times by Generator operators following a scheduled generation unit outage. The alarm was interpreted as an individual thermocouple device issue by personnel and not an actual temperature problem based on their past experience and procedures. It was actually an indication of localized heating from undetected internal damage to the generator that progressed to further, significant damage over a short period of time. While personnel responded to the initial alarm and subsequent alarm conditions per procedures, the low probability of generator internal problems was not considered until significant damage tripped the unit and required extensive further outage for repairs.

Details

Over the period of a week, a thermocouple temperature alarm on a generator stator coil was received at various times by plant operators. Other stator thermocouple temperature devices did not show abnormal temperatures. The following timeline provides the details of the event.

On Day-0, the unit was brought on-line following a scheduled outage. Note: Following the outage, a complete set of electrical tests were conducted on the stator and did not reveal any problems.

On Day-4 at approximately 2100 hours, the unit control room received a Stator Coil Water Differential Temperature high alarm. The plant operators responded by implementing their standard annunciator response procedure used by the operators to diagnose and address annunciator alarms in the control room.

On Day-5 at approximately 0200 hours, the instrumentation and control (I&C) technicians measured the coil thermocouple temperature and reported to the control room that the coil thermocouple was reading 160.7 °F, still below the 174 °F threshold established for engineering to continue further tests. At the time that 160.7 °F was communicated from the field, the control room indication for the same thermocouple was 163 °F leading the plant staff to believe the thermocouple was malfunctioning. Shortly after the I&C technicians disconnected their testing equipment, at approximately 0222 hours, the thermocouple coil temperature rose to 168 °F and continued to rise unnoticed until it read greater than 175 °F. Since the I&C maintenance crews

earlier report that the coil temperature was reading 160.7 °F at the generator, it was believed the higher temperature indicated a malfunctioning thermocouple.

At 0244 hours, the control room received the Generator Condition Monitor (GCM) Verified Alarm. The GCM detects combustible gasses in the generator hydrogen system. At 0254 hours, the GCM Verified Alarm cleared.

At 0342 hours, the crew removed the coil thermocouple from service by substituting a constant value for the thermocouple data to their computer system. There were still other coil thermocouple devices in service to provide measurements.

On Day-7 at 0216 hours, the GCM Warning Alarm began to cycle in and out. The staff was focused on other activities and believed the GCM was malfunctioning as believed on two days earlier. At 0229, the GCM Verified Alarm was again received. At 0310 hours, the control room received Stator Cooling System Trouble alarm and promptly redirected the plant operator to check the Stator Cooling Water System. When the plant operator arrived at the Stator Cooling Water skid, he noted that the tank level was high and water conductivity was rising. The plant operator immediately contacted personnel to sample the cooling water for conductivity. At 0329 hours, the unit tripped.

The apparent cause of the unit damage was a leak that appears to have existed in a hollow strand within the stator coil. This leak most likely existed for a long time and allowed moisture to travel inside the coil. The moisture degraded the resin in the coil over time allowing the conductor bundle to come loose from the ground wall and allow some individual conductor strands to move and vibrate. The strand-to-strand vibrations and movement eventually wore away the insulation between the strands and created strand-to-strand shorts. The shorts caused excessive heating. The area affected by these shorts grew as the coil insulation was thermally damaged and failed. As the affected area grew, more heat was created until the coil melted and eventually arced violently across the missing melted area of the coil. A generator ground fault occurred after melted copper exited the ground wall of the coil slot.

Corrective Actions

The generator underwent extensive on and off-site repairs due to the damage affecting stator core iron, rotor, exciter and stator coils. Additional work included complete stator cooling system flush along with testing and re-termination of all stator coil thermocouples as well as the following:

- Evaluated improvements to protective relaying, fault recording and sequence of event recording
- Reviewed operator procedures and made changes where necessary
- Reviewed I&C procedures to cross check thermocouple device accuracy
- Appropriate improvements in operator training have been made based on the lessons learned.

Lesson Learned

- 1) **The Operator Alarm standard annunciator response procedure did not support good decision-making**

When the unit control room received the Stator Coil Water Differential/Temperature High annunciator, the crew referred to the annunciator response procedure for guidance to address the alarm per the Operations department expectation. The current practices are biased toward declaring a thermocouple reading higher than the other thermocouples as an invalid indicator and removing it from service as soon as possible. This bias to make the thermocouple invalid is motivated by the need to restore the alarm's capability to re-arm and notify the operator, because the alarm will not re-flash until the affected thermocouple is removed from the differential temperature calculation. Other thermocouples and Resistive Temperature Devices (RTDs) that monitor the generator did not indicate excessive temperatures. The procedure did not highlight the importance of removing one point from scan or declaring it invalid and the risk of that action regarding a single stator coil.

2) The indications of high temperature on a single stator coil were misinterpreted.

The understanding by Operations personnel and Engineering personnel was that high Stator Coil Water differential temperatures were most likely due to cumulative long term failures that would affect the main generator and not the low probability indication of a single stator coil failure.

3) The significance of the GCM Verified Alarm was not recognized.

The procedural instructions to address the GCM "Verified alarm" were in an addendum in the Operations Alarm Instructions procedure versus in an Operator Annunciator response procedure. In addition, there has been limited training on the GCM. Operator training should include all procedural instructions.

4) The Control Room had situational awareness issues as it did not have an annunciator to signal critical GCM alarms

The GCM alarms are annunciated on an alarm screen; the system does not include a control board annunciator as customary for a system used for making important operating decisions to take the unit offline. With this arrangement, the individual importance of certain GCM alarms can be overlooked. The plant staff did not recognize the need for additional GCM related annunciators since the initial design.

5) Standard monitoring methods did not detect the leak or generator failure mode

Routine conductivity measurements of the stator cooling water did not detect the leak. Electrical tests conducted during the scheduled outage also did not reveal any indication of the impending failure. An improved methodology to detect possible failure modes for a single stator coil is being sought.

6) Plant staffing levels

Plant engineering and operations staff levels during the period of the outage and subsequent event were not identified as an issue.

For more information please contact:

Earl Shockley
Senior Director of Reliability Risk Management
earl.shockley@nerc.net
404-446-2560

David Penney
Senior Reliability Engineer
david.penney@texasre.org
512-583-4958

Source of Lesson Learned: Texas Reliability Entity

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing reliability standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

Lesson Learned

Auxiliary Relay Contact Contamination

Category: Relaying and Protection Systems

Primary Interest Group

Transmission Owners
Generation Owners
Distribution Providers

Problem Statement

A substation circuit breaker may have failed to operate because of possible auxiliary relay contact oxidation.

Details

A fault occurred that required the associated protection system to actuate. One of the substation circuit breakers designed to open by the scheme failed to do so, correctly initiating a breaker failure operation. This caused adjacent protection schemes to correctly operate to isolate the fault.

Following the event, during troubleshooting, the breaker once again failed to trip on the first test attempt. In subsequent tests, the breaker operated properly.

Upon further investigation, the contacts for the auxiliary relays were examined and were noted to be visibly tarnished. This sequence of events indicates that possible sulfidation may have degraded circuit integrity and prevented the breaker from tripping.

Corrective Actions

The entity burnished the contacts for all auxiliary relays in the affected protection scheme, and performed functional tests that verified the integrity of the circuit before returning the protection scheme to service.

The entity evaluated its auxiliary relay contact maintenance practices and modified its inspection procedures to include inspecting (where possible and practical) for signs of contamination (corrosion, oxidation, sulfidation, environmental) and to clean the contacts if necessary as part of the maintenance interval.

Lesson Learned

The entity periodically functionally tests its protection system, which includes functional checks of auxiliary relay contacts. However, this event raised questions about contact integrity due to possible sulfidation, oxidation, and contamination. Entities should review and evaluate their maintenance and inspection practices for the auxiliary relay contacts to ensure these problems do not occur. Entities may

also want to consider if any environmental factors warrant more frequent inspection of auxiliary relay contacts.

For more information please contact:

Earl Shockley
Senior Director of Reliability Risk Management
earl.shockley@nerc.net
404-446-2560

Steve Ashbaker
Director Operations
ashbaker@wecc.biz
801-883-6840

Source of Lesson Learned: Western Electric Coordinating Council

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing reliability standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

Lesson Learned

EMS Database Corruption Problem

Category – Bulk Power System Operations

Primary Interest Group

Balancing Authorities (BA)
Transmission Operators (TOP)
Reliability Coordinators (RC)
Transmission Owners (TO)

Problem Statement

An entity's Energy Management System (EMS) ceased operating due to the EMS vendor's "delete" software. This software is used to clear configuration database directories before an update is made to the database. In this particular instance, the software did not completely work causing the revised configuration database to contain mismatched and corrupted data. There was no loss of situational awareness during the event because operators implemented procedures that were developed to handle times when the EMS was not available. These procedures included, for monitoring and control purposes, physically manning the hydro plants and major substations.

Details

An entity's EMS staff deployed a revised EMS configuration database within the EMS production systems. It was deployed in order to configure Supervisory and Control Data Acquisition (SCADA) and Automatic Generation Control (AGC) applications to accommodate generator upgrade commission testing. While deploying the above database change, the redundant EMS application servers failed to accept the revised configuration database causing the EMS to quit functioning.

The entity's EMS workgroup procedure included a step to delete previous configuration files from the database build directory. This "Delete" operation is now known to not always completely erase the directory. Analysis by the EMS vendor determined that the new database was built with some previous database files present in the database build directory which corrupted the configuration database. In order to identify the source of the corrupted files in the database build directory, the entity and vendor reviewed the procedure used to build and update the configuration database. It was during this review that the vendor's technical support staff stated that the "Delete" operation to remove previous database files has been unreliable at times in other systems. Until this incident, this command has worked reliably for the entity's EMS.

To maintain situational awareness and control when the EMS quit functioning, operations placed personnel in unmanned generation plants and critical substations. They also utilized a back-up AGC load controller that is completely separate from the EMS system. The controller calculates Area Control Error (ACE) from separate inputs from EMS and allows for pulse control of the generators. The entity was also able to manually participate in their reserve sharing agreements.

Corrective Actions

Once the problem was discovered, EMS staff ensured the delete step worked and rebuilt the database. These actions allowed the EMS to return to normal service. The entity's EMS workgroup procedure to build new configuration databases was reviewed and changed to include a step to confirm that previous configuration data files have been deleted. EMS staff checklist for configuration database deployment was modified to include the verification step that all previous database files have been deleted.

Lesson Learned

Entities should check with their EMS vendor to make sure they have not experienced any problems with current vendor software to change data bases. EMS staff should review its EMS workgroup process and software to ensure configuration databases are built without the presence of previous data files. The EMS staff checklist for configuration database deployment should include the verification step that all previous database files have been deleted.

Software vendors and their user groups should inform all users, as soon as possible, about any problems that have been found even if the problem has a random occurrence. This notification allows all users to put in place safeguard procedures to ensure such problems do not affect their systems.

For more information please contact:

Earl Shockley
Senior Director of Reliability Risk Management
earl.shockley@nerc.net
404-446-2560

Steve Ashbaker
WECC – Director Operations
ashbaker@wecc.biz
801-883-6840

Source of Lesson Learned: Western Electric Coordinating Council

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing reliability standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

Lesson Learned Excessive Resource Utilization

Category: Telecommunications

Primary Interest Groups

Balancing Authorities
Reliability Coordinators
Transmission Operators

Problem Statement

Due to a failed interface device, a registered entity had internal data communications partially interrupted during a period of excessive network traffic across its optical wide area network links. There was no loss of situational awareness by operations as a result of this issue.

Details

The optical telecommunications network, which connects routers on a registered entity's network, experienced excessive traffic because of a failed interface on a device at one of the regional locations. Simultaneously, two network routers experienced issues where they were unable to reestablish communication with the rest of the network after the excessive network traffic finalized. The increased traffic caused unnecessary resource utilization on affected routers connected to the optical network. The high resource utilization rose to one hundred percent on these devices, which in turn; caused devices to drop incoming traffic.

This event would be analogous to congestion on a telephone network affecting a customer's ability to complete a call. A home telephone is connected to a central office phone switch which is networked to many other central office switches across the country. The event that occurred would be equivalent to a central office switch having problems that caused it to lose its connection to the other central office switches and then overwhelming the network by attempting to reestablish the connections. During this period, home telephone users would not be able to complete their calls because the network would be congested with the switches trying to communicate to each other. After the switches would reestablish communications with each other, the congestion would be reduced, the telephone network would return to normal and customer calls could be completed.

Corrective Actions

The two faulty network routers were removed from the network, ending their interference with other devices. In order to correct the synchronous optical network problem, one data link interface module was identified as being faulty on the optical network and had to be replaced.

Lessons Learned

Resource threshold monitoring should be established on applicable devices to trigger when an abnormally high threshold is exceeded. This will allow support personnel to identify which specific

resource on a device is contributing to an issue. Monitoring will provide proactive identification of issues and promote rectifying those issues in an expedient manner. Traffic throttling options should also be researched.

In addition, entities should consider adding bandwidth aggregation alarms on optical network's data link interface modules. Support personnel will be able to detect earlier signs of which optical connections are experiencing issues before a failure occurs.

For more information please contact:

Earl Shockley
Senior Director of Reliability Risk Management
earl.shockley@nerc.net
404-446-2560

Jacquie Smith
Principal Engineer
jacquie.smith@rfirst.org
303-247-3067

Source of Lesson Learned: ReliabilityFirst Corporation

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing reliability standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

Lesson Learned Protective Relaying Digital Input Board Loading Resistance

Category: Relaying and Protection Systems

Primary Interest Groups

Transmission Owners
Transmission Operators
Transmission Service Providers

Problem Statement

The digital input board in a relay circuit that protects a main circuit transformer was overly sensitive to transient signals, noise, or high resistance contact bridging from outdoor mounted relay devices, resulting in a false trip of a transmission line breaker.

Details

On two separate occasions and at two different stations, protective relay actions associated with power transformers resulted in false tripping of the main circuit breaker. Both incidents were initiated by outdoor mounted protective relaying devices. While the protection systems responded correctly and in accordance with design to isolate equipment, the protective trip was triggered by voltages at the digital input board that were not produced from an actual closure of a protective relay trip contact. The resulting trip of the main circuit breaker was determined to be false in nature and unnecessary.

Protective relaying devices and circuitry that protect outdoor power equipment (e.g. transformers or capacitors) are periodically exposed to severe weather conditions throughout their service life and are specifically designed to withstand harsh environments. One of these incidents was preceded by an extended period of bad weather but the protective trip occurred after the weather cleared while the second incident occurred during a period of good weather. As a result, it was concluded that there was no obvious correlation with either poor weather or wet conditions.

Thorough analysis showed that one of the protection circuits that produced a false trip was associated with a sudden gas pressure relay and the second with oil temperature monitoring. Although these are entirely different relay mechanisms with essentially no common parts or equipment, they both provide information to the protection system via a digital input circuit board installed in the control room. There are multiple inputs to the digital input circuit boards, and the boards are failsafe such that a failure of the board itself would not result in a protective signal being generated. Investigation and field testing of the control cables and protection systems involved verified that the equipment was operating within specifications.

All evidence collected during field inspections, circuit analysis and subsequent monitoring supported the conclusion that the protective trips were caused by the protection digital inputs being too sensitive to voltages from transient signals, signal noise, or high resistance contact bridging across the trip contacts on outdoor mounted protective devices.

Corrective Actions

Field modifications were performed on the protective relaying digital input circuit boards to introduce loading resistors in order to de-sensitize (dampen) the voltage signals to the digital input digital circuit boards. The loading resistors are installed across the digital input to lower the input resistance and limit the voltage level from transient signals, signal noise and contact bridging. The loading resistors have minimal impact on the voltage applied to the digital input from an actual protective trip contact closure. During approximately six months of operation after the modifications had been made, there have been no protective trips initiated from transients, signal noise or contact bridging. This period of time saw a number of severe weather events that included lightning storms through the summer, a hurricane, and a snow storm during the late fall. There were numerous nearby transmission level faults during these weather events which were seen by the protection systems and handled correctly. Continued monitoring of the modified digital input boards performance will be documented for further analysis.

Lesson Learned

Outdoor mounted protective relays and circuitry have the potential to be exposed to a wide range of disturbances that may disturb the voltage across a digital input in the control room. Modern digital relaying and control systems may be subjected to mechanical shocks, vibrations and other signal or noise interference events which, in turn, may cause transients to be detected as a full contact closure by the protection circuit digital input boards. The digital inputs associated with the protection of outdoor mounted devices should be designed or modified as necessary to reduce their sensitivity to voltages from transients, signal noise or high resistance contact bridging.

Methods to reduce the sensitivity to these voltages are:

- Add a loading resistor to the input of the digital input circuit board.
- Tightly twist the insulated send and return wires together to prevent induced voltages from picking up digital inputs. This makes the circuit more immune to any other voltage being induced from an outside source.
- Use interposing relays to electrically separate the input board from other devices. This requires more wiring but provides a solution to the problem where there are many cables located which may provide spurious signals near the protection circuit digital input board.

For more information please contact:

Earl Shockley
Senior Director of Reliability Risk Management
earl.shockley@nerc.net
404-446-2560

John G. Mosier
NPCC Assistant Vice President – System Ops.
jmosier@npcc.org
212-840-1070

Source of Lesson Learned: Northeast Power Coordinating Council, Inc. (NPCC)

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing reliability standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

Lesson Learned

Remote Terminal Units Not on DC Sources

Category: Facilities Design, Commission and Maintenance

Primary Interest Group

Transmission Owners

Generation Owners

Distribution Providers

Problem Statement

The power supply to a remote terminal unit (RTU) for a High Voltage Direct Current (HVDC) converter station was not designed to be fed from station batteries, resulting in a loss of the RTU when all AC feeds to the substation were lost due to an event. The RTU could not be restored until a source of AC power was restored. This resulted in the loss of visibility of the substation, however visibility remained on the surrounding substations and in this case the affected substation was de-energized, thus situational awareness was not impacted.

Details

An HVDC converter station RTU was designed to be powered from three redundant substation AC power supplies. Two of these AC power supplies were unavailable due to an external event and a third AC backup from a station emergency generator was also unavailable due to a generator overload; therefore the RTU did not have a power source. This circumstance affected retrieval of post event information and remote operation of equipment.

Corrective Actions

Staff is evaluating the feasibility to power the RTU with DC from station batteries and is also investigating the cause of the emergency generator overload.

Lesson Learned

While the availability of multiple AC sources provides a deep degree of reliability for RTUs, entities should evaluate the practicality and feasibility of powering RTUs needed for control, situation awareness, system restoration and/or post analysis from the station batteries.

For more information please contact:

Earl Shockley
Senior Director of Reliability Risk Management
earl.shockley@nerc.net
404-446-2560

Steve Ashbaker
Director Operations
Ashbaker@wecc.biz
801-883-6840

Source of Lesson Learned: Western Electric Coordinating Council

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing reliability standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

Lesson Learned

Unmanned Forklift Contact with Energized Bus

Category: Procedural Controls

Primary Interest Group

Transmission Owner

Transmission Operator

Problem Statements

Contact of an energized bus by an unmanned forklift being used in construction work in a 345-kV generating station switchyard caused the breakers connected to a 345-kV bus to open, as well as opening breakers at the remote ends. As a result, transfer trip occurred on a 115-kV line and 2-345-kV lines as well as electrical service to a coal mine was partially interrupted.

Details

After a work shift was completed, an unmanned, still running forklift made inadvertent contact with a 345-kV substation bus, causing a fault and clearing the bus. The forklift had been used for the purpose of material handling and was not being used as a means of elevating material. The forklift fork rose due to either faulty controls or by drift elicited by the electro-magnetic field of the bus or a combination of the two. The fault also resulted in tripping of a 115-kV line and two 345-kV lines. Additionally, a line serving a coal mine was de-energized, causing a partial interruption of service to the mine. The mine personnel had not been notified of the work taking place and therefore mine management had not made preparations for a potential outage of the site power to the mine. All lines were returned to service. The forklift was removed, the faulted bus section was confirmed to be suitable for re-energization and continued use, and the bus section was returned to service. No injuries, generation outages or other customer service outages occurred as a result of the event.

Corrective Actions

The TOP/TO assembled a cross-functional and technically qualified team to perform its Root Cause Analysis on the forklift contact and the team identified several controls to eliminate the risk of the root cause hazard and identified the personnel responsible for implementing the control(s). The following is a brief list of the corrective actions with respect to the forklift contact event to be executed going forward:

- At the end of the shift, all equipment shall be moved to a designated parking area away from energized or potentially energized equipment.
- At the end of the shift, equipment should be checked to make sure it is not running and all keys to equipment shall be removed and locked in a secure place.
- When heavy equipment, such as forklifts, is not in use during breaks or if they are not needed during the work day, they will be turned off and keys removed and locked in a secure place.

- Machines used in tight space working environments, as determined by the job hazard assessment, may be left in place at the end of the shift. Keys shall be removed and secured.
- Job site shall be inspected at the end of shift to check equipment to ensure it is not running and the keys have been removed and stored in a designated secured area.
- Job site shall be inspected at the end of shift to check fencing and gates to ensure the work site is secured.
- Perform a Failure Mode and Effects Analysis* (FMEA) for the switchyard and other critical locations to identify hazards and how to mitigate them. Communicate with all possible affected entities, including Power System Operations and Generator owners/operators to inform them when work is being performed that might impact them.

Lesson Learned

- Construction equipment in a switchyard should never be left running unmanned. There are numerous components which can fail and cause the equipment to change position. Also, keys to the equipment should always be removed and stored in a designated secured area.
- Construction work sites in energized switchyards shall be inspected at the beginning and end of each shift to ensure all barriers are identified and in place for potential hazards of accidental electrical contact of construction equipment. Where reasonably possible, all heavy equipment such as forklifts should be moved to a designated parking area away from energized or potentially energized equipment at the end of each shift or when not in use. If the equipment cannot be moved, it should put into a lockdown position and inspected to ensure it could not make contact with other equipment in the substation. Equipment should not be left running and all keys shall be removed and locked in a secure designated location.
- Before work is started in switchyards, notify and coordinate with all possible affected entities.

For more information please contact:

Earl Shockley
Senior Director of Reliability Risk Management
earl.shockley@nerc.net
404-446-2560

Steve Ashbaker
Director of Operations
Ashbaker@wecc.biz
801 883 6840

Source of Lesson Learned: Western Electric Coordinating Council

This document is designed to convey lessons learned from NERC's various activities. It is not intended to establish new requirements under NERC's Reliability Standards or to modify the requirements in any existing reliability standards. Compliance will continue to be determined based on language in the NERC Reliability Standards as they may be amended from time to time. Implementation of this lesson learned is not a substitute for compliance with requirements in NERC's Reliability Standards.

*Failure modes and effects analysis (FMEA) is a step-by-step approach for identifying all possible failures in a design, a manufacturing or assembly process, or a product or service. "Failure modes" means the ways, or modes, in which something might fail. Failures are any errors or defects, especially ones that affect the customer, and can be potential or actual. "Effects analysis" refers to studying the consequences of those failures. Failures are prioritized according to how serious their consequences are, how frequently they occur and how easily they can be detected. The purpose of the FMEA is to take actions to eliminate or reduce failures, starting with the highest-priority ones. Failure modes and effects analysis also documents current knowledge and actions about the risks of failures, for use in continuous improvement.

From: [Guy V. Zito](#)
To: [tfist](#)
Cc: [rsc](#)
Date: Friday, June 22, 2012 8:12:21 AM

Greg and TFIST,

The following is an excerpt from some notes taken at the recent NERC Operating Committee (OC) meeting by NPCC staff. I thought you might find this interesting and initiate a discussion at an upcoming meeting to determine if there are similar concerns in NPCC. If the below is a valid concern and shared, how could NPCC mitigate risk?

"Mr. Hamdar (Vice-Chair of NERC OC) introduced Mr. Todd Lucas of Southern Company, who discussed the September 15, 2011, partial loss of visibility by the Southern Company EMS system. Since the event was not a complete loss of visibility, it was not a defined Category 2 event, but it was reported by Southern due to the lessons learned which could be shared with the industry. Mr. Lucas observed that, due to the updates required by the cyber standards, Southern has seen a nearly tenfold increase in revisions to EMS software, and the EMS system is particularly vulnerable to failures during such periods.

Mr. Holeman (Chair of the NERC OC) observed that Category 2.b EMS failures had accounted for twenty-eight events reported through the NERC Event Analysis Program."

Thanks,

Guy V. Zito
Assistant Vice President-Standards
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas, 10 th Floor
New York, NY 10018
212-840-1070
212-302-2782 fax

NERC Operating Committee

Meeting Notes

June 19 and 20, 2012

Introductory Remarks

Mr. David Goulding, current member of the NERC Board of Trustees and former CEO of the Independent Electricity System Operator, welcomed the NERC Operating Committee to Toronto and discussed current operating challenges facing the OC.

Operating Reliability Subcommittee (Colleen Frosch)

Ms. Frosch highlighted the following issues contained in her written report submitted to the NERC Operating Committee and included in the meeting material:

- The Operating Reliability Subcommittee recommended the termination of the pilot program of the “Guideline for Operating State Alert Levels,” and it further recommended that the industry discontinue any efforts to incorporate the Guideline in a NERC Reliability Standard.

The original intent of the ORS in its development of the “Guideline for Operating State Alert Levels” was to augment the existing definitions of Emergency Energy Alerts (EEAs) presented in NERC Reliability Standard EOP-002-3, “Capacity and Energy Emergencies,” with parallel alert states defined for transmission and operational security, the Transmission Emergency Alert (TEA) Level and the Security Emergency Alert (SEA) Level, respectively.

The NERC Operating Committee approved the recommendation of the Operating Reliability Subcommittee that the Transmission Emergency Alert (TEA) and the Security Emergency Alert (SEA) no longer be issued.

- In order to facilitate the approval by the Reliability Coordinator of the TOP Restoration Plans within its footprint, the ORS developed and accepted a “Checklist” to be used by the Reliability Coordinator in its review of a TOP Restoration.
- Upon the recommendation of the Operating Reliability Subcommittee, the OC approved the revised Reliability Plan of the Midwest ISO subject to the successful certification of the MISO, necessitated by the transfer of the Entergy Balancing Authority from the SPP footprint to the MISO footprint. The ORS did not feel there were reliability issues or gaps in the incorporation of the Entergy BA within the MISO footprint.

Events Analysis Subcommittee (EAS) Scope (Sam Holeman)

Mr. Holeman introduced the proposed draft scope, noting that it represented the culmination of two trial periods of the NERC Event Analysis Program conducted over a period of 1 ½ years. The ultimate goal of the program is to rapidly disseminate to the industry actionable lessons learned derived from the events which are assessed. He stressed that the program is a voluntary outreach to the registered entities, and it is not to be perceived as a compliance tool.

The OC suggested that, to stress the appropriate priority of the effort, items IV.a and IV.b following be reversed:

- IV. “The EAS will partner with regional entities, registered entities and other industry forums to:
- a. Obtain input of Regional personnel and reliability stakeholder groups as resources to the EAS, leveraging their experience and knowledge.
 - b. Address reliability issues.”

With the above revision, the NERC Operating Committee approved the scope of the proposed Events Analysis Subcommittee. The NERC Operating Committee also rejected the suggestion of another name for the EAS and retained “Events Analysis Subcommittee.”

With the approval of the scope for the Events Analysis Subcommittee, the following the positions of Chair and Vice Chair became effective:

Chair	J. Sam Holeman (Duke Energy)
Vice Chair	Hassan Hamdar (FRCC)

Mr. Hamdar introduced Mr. Todd Lucas of Southern Company, who discussed the September 15, 2011, partial loss of visibility by the Southern Company EMS system. Since the event was not a complete loss of visibility, it was not a defined Category 2 event, but it was reported by Southern due to the lessons learned which could be shared with the industry. Mr. Lucas observed that, due to the updates required by the cyber standards, Southern has seen a nearly tenfold increase in revisions to EMS software, and the EMS system is particularly vulnerable to failures during such periods.

Mr. Holeman observed that Category 2.b EMS failures had accounted for twenty-eight events reported through the NERC Event Analysis Program.

Human Performance Subcommittee (HPS) Scope (Bob Schwermann)

Mr. Schwermann described the Subcommittee as offering a set of tools and methodologies to make the job safer by the mitigation or elimination of events linked to human performance.

The NERC Operating Committee expressed concerns with the initiative due to its focus on “best practices” and its potential for compliance implications, and it did not vote on the proposed scope. The NERC Operating Committee suggested that alternative venues were available through which to disseminate lessons learned associated with human performance incidents.

Arizona-Southern California Outages on September 8, 2011-Causes and Recommendations (Tom Bowe)

Mr. Bowe asked the OC to address the issues in the report by first dividing the OC members into four groups, each of which was asked to identify what it perceived as the most critical factors contributing to the event:

Is the skill set of system operators today still sufficient?

What is the proper cut-off for the BES threshold? Contributing elements were 92 kV facilities, but monitoring too many elements can masque problems.

Is the right data shared among entities?

Margins should be established between facility ratings and trip points.

How deep is it necessary to model the neighboring system ahead studies?

Will the State Estimator become less stable with an increased volume of neighboring data?

Are operating reserves adequately dispersed and deliverable?

Do generating units have adequate “ride-through” capability?

Do the seams of the planning authorities present problems?

In assessing the event, it was noted that there were no longer NERC transmission maps of North America. The NERC Operating Committee approved a motion for a return to the release of the NERC map and asked that NERC determine how it can be released to the registered entities and the regulatory agencies.

Mr. Bowe agreed to draft a summary of actionable steps that the NERC Operating Committee can pursue in the immediate time frame.

Reliability Guideline: System Operator Verbal Communications- Current Industry Practices (David Zwergel)

Mr. Zwergel discussed the proposed draft, noting that it was largely a compilation of what is currently being done within the industry as based on the discussions at the March, 2012, meeting of the NERC Operating Committee. He indicated that it was made clear within the Guideline that it was not a compliance document.

The NERC Operating Committee approved the draft for posting to receive public comment.

Discussion of NERC Reliability Standard COM-003-1, “Operating Personnel Communications Protocols” (David Zwergel)

The NERC Operating Committee accepted the draft document defining how and when three-part communication is to be used. The Protocols

state that three-part communication is to be implemented for the following conditions:

“Verbal three-part communication should be used during the operation or alteration of Facility equipment. Applicable entities are to use three-part communications when performing steps or actions using an approved procedure that impact equipment or activities, the safety of personnel, the environment, or the Facility. Finally, three-part communication should be implemented for tasks where the consequences of a mishap are unacceptable and could lead to instability, uncontrolled separation, or Cascading. As a best practice, it may also be used when discussing the condition of Facility equipment or the value of an important parameter in utility operations.”

Messrs. Bowe and Castle agreed draft a letter transmitting the “COM-003-1 Operating Communications Protocols White Paper” to the Standards Drafting Team for its consideration.

The OC also suggested that possibly a communication standard could ask for an organizational set of protocols with training, follow-up and monitoring, with the White Paper providing guidance to the industry.

Coordinated Action Plan (Phase 2)-Implementing the HILF Task Force Recommendations (Stuart Brindley)

Mr. Brindley advised the OC that, of fifty-seven separate recommendations from the collective HILF reports, five will be directed to the OC with respect to the resilience of operations following an extraordinary event.

Request for Feedback-Draft Impact of Loss of GPS Signals in Power System Operations (Mark Lauby)

Mr. Lauby summarized the draft report, observing that it does not see an immediate reliability issue. The issue could be seen a future concern, suggesting that a “master plan” for loss of GPS time signals could be considered by the entities. Offering comments, the OC suggested that the tone of the report did not make clear that there was no immediate risk. It also asked that an Executive Summary be added.

Geomagnetic Disturbance Task Force (GMDTF) Phase 2 Scope (Greg Henry)

Mr. Henry reported that the Geomagnetic Disturbance Task Force (GMDTF) would be reconvened to address the outstanding recommendations of the original report, including enhancing the NERC Alerts process, enhancing training and the modeling of ground conductivity and geomagnetically induced currents (GIC). The industry would be advised of the GMDTF progress through quarterly Webinars.

The NERC Operating Committee endorsed the direction of the second phase of the NERC GMD Task Force.

Recovery from Losses Greater Than Most Severe Single Contingency Within 15-Minutes (David Zwergel)

Mr. Zwergel introduced the discussion with an overview of the February 14, 2008, event in PacifiCorp. The subsequent FERC Order accepting a settlement, released on December 1, 2011, stated:

“The Reliability Standards set forth the parameters that a Balancing Authority and Transmission Operator, such as PacifiCorp, must monitor and address to ensure the reliability of the Balancing Authority Area and the Interconnection following a disturbance. Area Control Error, or ACE, is one those parameters. Enforcement and NERC concluded that PacifiCorp did not ensure it was operating reliably because it did not restore its ACE within fifteen minutes of the Reportable Disturbance as required by BAL-002-0, Requirement R4. Because PacifiCorp did not restore its ACE to zero until forty-five minutes after the start of the disturbance, Enforcement and NERC determined that PacifiCorp violated BAL-002-0, Requirement R4. Enforcement and NERC concluded that, during this forty-five minute period, PacifiCorp leaned on the Interconnection using the resources from other Balancing Authorities to maintain its own operations. Enforcement and NERC also determined that PacifiCorp again violated BAL-002-0, Requirement R4, during the 10:00 hour.”

The OC was asked if it was the intent of the Standard to shed load when frequency is stable and all loadings are within limits. The OC was further advised that, in response to this directive, a Reliability Coordinator had ordered load shedding by one member of a Reserve Sharing Group still negative, although the collective ACE of the RSG had fully recovered.

Mr. Bowe will draft a letter to the NERC Board of Trustees, capturing the discussion of the OC and seeking the guidance of the BOT.

It was also pointed out that a request for interpretation submitted by the Northwest Power Pool had yet to be addressed by NERC, and Mr. Bowe will ask that it be expedited.

Standards Driven Index (SDI) White Paper (Bill Adams)

Mr. Adams summarized the compliance violation metrics which are incorporated into the concept of the Standards Driven Index. The OC pointed out that the index was not driven by the most critical standards but rather those standards realizing the largest number of violations. As an example, the BAL Standard is not represented in the index because of no violations.

The OC endorsed the Standards Driven Index with the suggestion that the Performance Analysis Subcommittee develop a title more consistent with its actual metric components.

Proposed Changes to the Standards Process Manual (Ben Li)

Mr. Li discussed the draft document, "Recommendations to Improve the NERC Standards Development Process," developed by the Standards Process Input Group (SPIG) of the Member Representatives Committee (MRC). In an effort to streamline the standards process, a number of recommendations are offered, including the suggestion to:

- provide only one formal comment period, the minimum required by the American National Standards Institute (ANSI);
- eliminate the formal response to every comment (not required by ANSI); and
- move the associated "Measures" into the RSAW document.

Mr. Li also indicated that cost effectiveness would be introduced into the process, and more focus would be given to consensus building in the drafting of a standard. He indicated that the currently anticipated schedule targets a filing with FERC on December 14, 2012.

**Round Table Discussion of Requirement 1 of NERC Reliability
Standard PRC-001, “System Protection Coordination” (Tom Bowe)**

Requirement 1 of NERC Reliability Standard PRC-001, “System Protection Coordination,” states:

“Each Transmission Operator, Balancing Authority, and Generator Operator shall be familiar with the purpose and limitations of protection system schemes applied in its area.”

Mr. Bowe deferred the round table discussion of the requirement to the September meeting of the NERC Operating Committee, providing ample time for an adequate discussion of the concerns surrounding the issue. In preparation for the September discussion, each Subcommittee of the OC was charged to discuss its interpretation of the phrase “... shall be familiar with ...”

Prepared by:

John G. Mosier, Jr.
June 20, 2012

Member Representatives Committee Pre-Meeting Conference Call

July 10, 2012 | 11:00 a.m. Eastern

Dial-in: 1-800-617-7643

No pass code necessary

Introductions and Chair's Remarks

NERC Antitrust Compliance Guidelines and Public Announcement

Agenda

- 1. MRC Draft Agendas**
- 2. Preliminary Agenda Items for the Board of Trustees and Board Committees**
- 3. Schedule of August Meetings**
- 4. Request for Policy Input**
- 5. Nominations and Elections**
 - a. Proposed membership slate for the Reliability Issues Steering Committee (RISC)
 - b. Upcoming MRC Officer elections and MRC nominations

Member Representatives Committee Pre-Meeting Conference Call

July 10, 2012 | 11:00 a.m. Eastern

Dial-in: 1-800-617-7643

No pass code necessary

Introductions and Chair's Remarks

NERC Antitrust Compliance Guidelines and Public Announcement

Agenda

- 1. MRC Draft Agendas***
- 2. Preliminary Agenda Items for the Board of Trustees and Board Committees***
- 3. Schedule of August Meetings***
- 4. Request for Policy Input**
- 5. Nominations and Elections**
 - a. Proposed membership slate for the Reliability Issues Steering Committee (RISC)
 - b. Upcoming MRC Officer elections and MRC nominations

*Background materials included

Antitrust Compliance Guidelines

I. General

It is NERC's policy and practice to obey the antitrust laws and to avoid all conduct that unreasonably restrains competition. This policy requires the avoidance of any conduct that violates, or that might appear to violate, the antitrust laws. Among other things, the antitrust laws forbid any agreement between or among competitors regarding prices, availability of service, product design, terms of sale, division of markets, allocation of customers or any other activity that unreasonably restrains competition.

It is the responsibility of every NERC participant and employee who may in any way affect NERC's compliance with the antitrust laws to carry out this commitment.

Antitrust laws are complex and subject to court interpretation that can vary over time and from one court to another. The purpose of these guidelines is to alert NERC participants and employees to potential antitrust problems and to set forth policies to be followed with respect to activities that may involve antitrust considerations. In some instances, the NERC policy contained in these guidelines is stricter than the applicable antitrust laws. Any NERC participant or employee who is uncertain about the legal ramifications of a particular course of conduct or who has doubts or concerns about whether NERC's antitrust compliance policy is implicated in any situation should consult NERC's General Counsel immediately.

II. Prohibited Activities

Participants in NERC activities (including those of its committees and subgroups) should refrain from the following when acting in their capacity as participants in NERC activities (e.g., at NERC meetings, conference calls and in informal discussions):

- Discussions involving pricing information, especially margin (profit) and internal cost information and participants' expectations as to their future prices or internal costs.
- Discussions of a participant's marketing strategies.
- Discussions regarding how customers and geographical areas are to be divided among competitors.
- Discussions concerning the exclusion of competitors from markets.
- Discussions concerning boycotting or group refusals to deal with competitors, vendors or suppliers.

- Any other matters that do not clearly fall within these guidelines should be reviewed with NERC's General Counsel before being discussed.

III. Activities That Are Permitted

From time to time decisions or actions of NERC (including those of its committees and subgroups) may have a negative impact on particular entities and thus in that sense adversely impact competition. Decisions and actions by NERC (including its committees and subgroups) should only be undertaken for the purpose of promoting and maintaining the reliability and adequacy of the bulk power system. If you do not have a legitimate purpose consistent with this objective for discussing a matter, please refrain from discussing the matter during NERC meetings and in other NERC-related communications.

You should also ensure that NERC procedures, including those set forth in NERC's Certificate of Incorporation, Bylaws, and Rules of Procedure are followed in conducting NERC business.

In addition, all discussions in NERC meetings and other NERC-related communications should be within the scope of the mandate for or assignment to the particular NERC committee or subgroup, as well as within the scope of the published agenda for the meeting.

No decisions should be made nor any actions taken in NERC activities for the purpose of giving an industry participant or group of participants a competitive advantage over other participants. In particular, decisions with respect to setting, revising, or assessing compliance with NERC reliability standards should not be influenced by anti-competitive motivations.

Subject to the foregoing restrictions, participants in NERC activities may discuss:

- Reliability matters relating to the bulk power system, including operation and planning matters such as establishing or revising reliability standards, special operating procedures, operating transfer capabilities, and plans for new facilities.
- Matters relating to the impact of reliability standards for the bulk power system on electricity markets, and the impact of electricity market operations on the reliability of the bulk power system.
- Proposed filings or other communications with state or federal regulatory authorities or other governmental entities.

Matters relating to the internal governance, management and operation of NERC, such as nominations for vacant committee positions, budgeting and assessments, and employment matters; and procedural matters such as planning and scheduling meetings.

Draft Agenda Member Representatives Committee Informational Session Conference Call and Webinar

August 8, 2012 | 11:00 a.m. Eastern

Introductions and Chair's Remarks

NERC Antitrust Compliance Guidelines and Public Meeting Notice

Agenda

1. **Update on the Recommendations from the Standards Process Input Group (SPIG)**
2. **2012 Long-Term Reliability Assessment and Emerging Issues**
3. **Progress Reports and Informational Updates**
 - a. Risk-Based Compliance Monitoring and Entity Assessments
 - b. Compliance Enforcement Initiative, including Find, Fix, Track and Report (FFT) Initiative
 - c. FFT Order - Paragraph 81
 - d. NERC Compliance Process Bulletin #2012-001: Applicability of PRC-023-1 for Generator Owners

Draft Agenda Member Representatives Committee

August 15, 2012 | 1:00-5:00 p.m. Eastern

Hilton Quebec
1100, Rene-Levesque Blvd East
Quebec, QC
Canada G1R 4P3
418-647-6500

Introductions and Chair's Remarks

NERC Antitrust Compliance Guidelines and Public Meeting Notice

Consent Agenda

1. **Minutes — Approve**
 - a. July 10, 2012 Conference Call
 - b. May 8, 2012 Meeting
2. **Future Meetings**
3. **Remarks from Gerry Cauley, NERC President and CEO**
4. **Elections and Nominations**
 - a. MRC Officer and Sector Elections
 - b. Update from the Board of Trustees Nominating Committee
5. **ERO Business Plan and Budget Process**
6. **Status of SPIG Recommendations and RISC Mandate**
 - a. Nominate Slate for the Reliability Issues Steering Committee (RISC)
7. **Status of and Policy Input for Standards Projects**
 - a. Bulk Electric System (BES) Definition
 - b. Adequate Level of Reliability (ALR) Definition
 - c. Status of communications standards
8. **Additional Discussion of MRC Informational Session Items, August 8**
 - a. Update on Entity Assessments
 - b. Compliance Enforcement Initiative, including Find, Fix, Track and Report (FFT)
 - c. FFT Order - Paragraph 81

- 9. **Report on Rules of Procedure Process Improvements**
- 10. **Follow-Up Activities from the 2011 Southwest Outage**
- 11. **Regulatory Update**

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Member Representatives Committee

Pre-Meeting Webinar
July 10, 2012

RELIABILITY | ACCOUNTABILITY



- Review preliminary agenda topics for August 8 Informational Session and August 15 Member Representatives Committee (MRC) meeting.
- Preview proposed list of agenda topics for the Board of Trustees and associated board committee meetings (August 15 and 16).
- Determine adjustments to the August 8 and 15 MRC agendas based on today's discussion.

- Recommendations from the Standards Process Input Group (SPIG)
- 2012 Long-Term Reliability Assessment (LTRA) and Emerging Issues
- Progress Reports and Informational Updates
 - Risk-based compliance monitoring and entity assessments
 - Find, Fix, Track, and Report (FFT) and Paragraph 81
 - NERC bulletin #2012-001: PRC-023-1

- Elections and Nominations
- ERO Business Plan and Budget Process
- Status of SPIG Recommendations and Reliability Issues Steering Committee (RISC)
- Status of and Policy Input for Standards Projects
 - Bulk Electric System (BES) and Adequate Level of Reliability (ALR) Definitions
 - Communications standards
- Additional Discussion of August 8 Items
- Rules of Procedure Process Improvements
- Follow-up Activities from Southwest Outage
- Regulatory Update

- Self-Assessment and Effectiveness Surveys
- Overall Composition of the Board
- Sarbanes-Oxley Issues
- 2012 Corporate Goals Update
- Human Resources and Staffing/Recruiting Updates

- Reliability Standards Status Report
- Standards Committee Report
- NERC Technology Quarterly Update
 - Compliance Reporting Analysis and Tracking System (C-RATS)
 - Public website
- Standards Oversight and Technology Committee (SOTC) Mandate

- Compliance Enforcement Initiative (CEI)
 - FFT Statistics to date and preparation for the 12-month Report
 - Pathway for CEI
- Compliance Operations
 - CIP-002, Option for Transitioning Version 3 to 4
 - Risk-Based Compliance Monitoring Update
 - 2013 Annual Implementation Plan and Actively Monitored List
 - Reliability Standards Audit Worksheet
- Maximizing Use of Self-Certifications
- Quarterly Statistics

- Third Quarter Calendar of Finance and Audit Committee (FAC) Responsibilities
 - Review and accept second quarter statement of activities
 - Working capital policy and contingency reserve guidelines
 - NERC and Regional Entity proposed 2013 Business Plans and Budgets (BP&B) and associated assessments
 - FAC mandate amendment

- Committee Membership Appointments and Mandate Amendments
- Standards
 - VAR-002-2, IRO-001-3, PRC-005-2
 - Communications
 - Section 1600 data request in response to Order No. 754
 - Retirement of BAL-004-1
- 2013 BP&B and Associated Assessments
- Rules of Procedure Process Improvements

- SPIG Recommendations
 - RISC mandate
 - Status of other recommendations
- Follow-up on Southwest Outage Recommendations
- Critical Infrastructure Department (CID) Update
 - Cyber Security Risk Maturity Model
 - ES-ISAC portal
 - Risk management guidelines
 - High-Impact, Low-Frequency (HILF) Coordinated Action Plan, Phase II
- Standing and Board Committee Reports
- Forum and Group Reports

Schedule of Events – Industry
August 15-16, 2012 — Quebec City, Canada

Wednesday, August 15, 2012	
7:30-8:30 a.m. Room name: Main Ballroom	Corporate Governance and Human Resources Committee <u>OPEN</u> Session
8:30-9:30 a.m. Room name: Main Ballroom	Standards Oversight and Technology Committee – <u>OPEN</u> Session
9:45-10:45 a.m. Room name: Main Ballroom	Compliance Committee – <u>OPEN</u> Session
10:45 a.m.-Noon Room name: Main Ballroom	Finance and Audit Committee <u>OPEN</u> Session
Noon to 1:00 p.m.	LUNCH
1:00-5:00 p.m. Room name: Main Ballroom	Member Representatives Committee – <u>OPEN</u> Session
6:00 p.m. Location:	Reception
Thursday, August 16, 2012	
8:00 a.m.–Noon Room name: Main Ballroom	Board of Trustees Meeting

MEETING LOCATION

Hilton Quebec
1100, Rene-Levesque Blvd East
Quebec, QC
Canada G1R 4P3
418-647-6500

SPCS June 26-28, 2012 Meeting Notes:
PG&E Offices
San Francisco, CA

FERC Order 754

Status of Data Request on Single Point of Failure. SPCS held a webinar last week and will incorporate further clarification based on comments received. NERC Staff will be assembling comments received in Open Process Posting of the Data Request which ended June 25, 2012 and will provide the comments to the SPCS for the development of the responses at a conference call scheduled on July 9, 2012. SPCS will finalize the Data Request and the responses to comments during the week of July 16-20 for a submission to the NERC Board of Trustee for approval at the August meeting. If all goes as expected, the Data Request will be posted on September 1, 2012.

SPCS reviewed the NERC responses to the request for interpretation of TPL-003 and TPL-004 regarding (1) required assessment for stuck breaker or protection system failure and (2) modeling of single point of failure of a protection system in the evaluation of delayed clearing in Category C and Category D contingencies. SPCS will submit a comment to the drafting team's response to (2) suggesting the highlighted additions below for clarification:

The term "Delayed Clearing" that is described in Table 1, footnote (e) refers to fault clearing that results from a failure to achieve the protection system's normally expected clearing time. Any failure of a protection system component that **affects the operation (disables or increases clearing times)** of one or more protection systems requires the Transmission Planner and Planning Authority to simulate the full impact on the Bulk Electric System performance. **For example, if a single current transformer provides AC current input to a primary and secondary protection system then simulating failure of the CT must include the effect of disabling both local protection systems. This may require modeling clearing from remote terminals to expose the full impact on the BES performance.**

Order 758

SPCS further developed the draft technical paper on the application of auto reclosing on the bulk power system and will further coordinate this effort with SAMS.

SPCS also further developed the draft technical paper on sudden pressure relays and other protective devices which respond to non-electrical quantities.

Protection System Commissioning

SPCS was asked to review and respond to the need/request for a protection system commissioning standard. The request stated “improper or inadequate commission testing practices are common cause of protection system misoperations. Undesired outcome have immediate negative impact on the reliability of the bulk power system and no reliability standard exists to prevent them. Example given: an entity failed to employ proper commission testing practices during the installation of a new transformer. As a result, associated line relays were placed in service with the incorrect CT ratio. The defect remained undetected until the occurrence of a severe system disturbance when the relaying operated incorrectly, greatly increasing the magnitude and scope of the disturbance.” SPCS members noted the issue was inadequate commission testing which resulted from apparent lack of training or testing procedure.

SPCS initiated development of a technical paper to address the issue raised. MRO reported that review of their misoperation reports indicated about 10% could have been caught during commissioning. SPCS will attempt to respond to the following questions

1. Is the development of a standard the appropriate manner to solve that problem, or should alternative approaches be used?
2. Does the concern need to be addressed and how?

SPCS may attempt to collect data from misoperation reports to support the request for commissioning testing standard. NPCC noted that it has requirement for protection system commissioning testing in its Bulk Power System Protection Criteria and as a result has not experienced misoperations due to a lack of commissioning testing.

SPCS also noted CAN 43 states that “CEAs are to use commissioning test records to verify compliance of new equipment with PRC-005 R2.”

Development of Draft Survey on Application and Maintenance of Sudden Pressure to Trip

SERC presented the results of its survey on a number of SERC members regarding the use of sudden pressure relays to trip and the maintenance practices associated with these relays. SERC survey results indicate that

- 80% of generator owners do trip with sudden pressure relays and of those who trip with sudden pressure relays, 85% have a maintenance program between 3-6 years in conjunction with their equipment maintenance interval.
- 50% of transmission owners do trip with sudden pressure relays and of these transmission owners, 50% have a maintenance program. The maintenance intervals vary widely between companies and are tied to the company's relay maintenance intervals.

SPCS updated the SERC survey questionnaire and will consider conducting a NERC-wide survey on the application and maintenance of sudden pressure to trip.

Special protection systems

SPCS further updated the draft technical paper on Special Protection System based on the latest changes made by the NERC System Assessment and Modeling Subcommittee (SAMS). SPCS reviewed the apparent confusion between the definition for protection system and special protection system. NPCC suggested that this confusion can be mitigated by clarifying that a protection system protects an element of the power system whereas a special protection system protects the power system from an adverse system condition and take corrective actions. SPCS also reviewed and will consider re-write or eliminate “schemes automated as operator aids that respond to conditions which an operator could detect and complete the necessary action in the timeframe required (e.g., T_V for IROL, 30-minute thermal rating)” as an exclusion to the SPS definition since some view this as a potential loophole.

SPCS will incorporate in the paper examples for common applications of SPS and will further develop the background and introductory sections of the report.

Considering the additional work that must be done to complete the draft paper, it is unlikely that the paper will be ready to be presented to the PC in September.

Protection System Misoperations

SPCS further updated the SPCS Recommended Criteria for Reporting Protection System Operations Document to clarify that “Operations which are initiated by control systems (not protection systems) such as those associated with generator controls, or turbine/boiler controls, static VARS compensators, FACTS, HVDC transmission systems, circuit breaker mechanism, or other facility control systems are also not operation of a protection system.”; SPCS also recommends that the collection of protection system operations data includes classification by voltage levels. An example on the breaker failure operation will be added to the document.

SPCS further reviewed the comments received from the ERO-RAPA group on the proposed changes to the misoperation template. SPCS will add clarification to note that facilities below 100 kV are to be BES only and that the voltage for a generator misoperation is to be the high side of the GSU.