™

Cyberphysical System Integrations & Interoperability Communications Security (CSIICS/C6)

Michael Curnow

04.19.2022

Page Intentionally Left Blank

Table of Contents

Definitions

CPS – Cyberphysical System. Technological systems that integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other.

V2X – Vehicle-to-Everything is communication between a vehicle and any entity that may affect, or may be affected by, the vehicle.

CV2X – Cellular Vehicle-to-Everything is a 3GPP standard describing a technology to achieve the V2X requirements.

4G LTE – Long-Term Evolution is a standard for wireless broadband communication for mobile devices and data terminals, based on the GSM/EDGE and UMTS/HSPA standards.

5G NR – New Radio is a new radio access technology (RAT) developed by 3GPP for the 5G (fifth generation) mobile network. It was designed to be the global standard for the air interface of 5G networks.

Purpose

This document is an evolution of the prior document titled “Introductory to Cyberphysical System Integration Security (CSIS)”[9], and serves to propose a new discipline in the Cybersecurity field, titled “*Cyberphysical System Integrations & Interoperability Communications Security*”, to be otherwise abbreviated herein to “*CSIICS*” or “*C6*”.

Additional Contexts

1. This documents is written from the perspective of U.S. Critical Infrastructure. But points made are applicable to sectors outside of the U.S.
2. This document contains verbiage aligned with both the common parlance of Cyberphysical Systems and that of modern business practices. See definitions as needed.

Practical Application

Reading this document shall provide an understanding of the Cyberphysical landscape as it pertains to critical infrastructure and the technologies that influence the physical world, the need to secure the communications which underpin their cross-platform integration and interoperability with varying systems, and lastly what challenges solutions proposed from the C6 perspectives will have to meet and to cultivate to address these such.

Introduction

Interoperability of our critical Infrastructure is contingent upon *convergence*, or connectivity between technological systems that need to share information and interact with one another to perform necessary functions for the operation of intelligent transportation systems (ITS), power, water and waste water, fuel pipelines, global communication, critical manufacturing, food & agriculture, and emergency systems, etc.

The safety, availability, and uptime of our critical infrastructure and it’s cyberphysical system components are contingent upon robust, resilient, and secure communications. *Cyberphysical System Integrations & Interoperability Communications Security* (CSIICS/C6) as a discipline within the broader Cybersecurity umbrella seeks to address such threats to the communications layer(s) of these systems by working to identify threats, assess risk and impact to systems of critical infrastructure, and to research and develop ways to mitigate said threats in a resilient, flexible, and future-proof fashion that can be built-in and upon in order to stand the test of time and evolve with Cyberphysical Systems as they grow in complexity and scale.

Mission

The overall mission of C6 can be simply stated as “To Architect, Engineer, and Develop Methodologies, Best Practices, Protocols, Standards, and Specifications, to secure the communication layer of a multiplicity of cyberphysical system integrations and means of interoperability to ultimately mitigate as much loss of life and damage as possible while sustaining the level of freedom and agency necessary for a free society to function”.

C6 promotes these goals through the following methods defined herein (but not necessarily limited to, as later versions of this document may include additional items):

- Research & Development (Otherwise known as “Solution Development”)
    - Creation of Software and Hardware Solutions
    - Draft Specifications, Frameworks, or Best Practices
- Sector Engagement
    - Provide Feedback on Publications, Papers, and Standards
    - Collaboration with Industry Leaders to Promote Best Practices
- Community Involvement
    - Presenting the C6 Case on the Public Stage via:
        - Conferences
        - Panels
        - Seminars
        - Testimonials
        - Etc
    - Education and Outreach

Compass

C6 guiding focus is directed towards addressing the communications-layer’s safety & security concerns and implications of introducing *The Fourth Industrial Revolution* [1] (*Industry 4.0* for short), along with it’s increased hyper-connectivity, to various facets of critical infrastructure. With increased connectivity between all things also comes an increased attack surface. The common denominator among the varying Cyberphysical Systems that constitute our Critical Infrastructure is that they all require a layer of communications for interoperability and integration to occur. Areas of concentration include (but not limited to, as later versions of this document may include additional items):

Transportation

Intelligent Transportation Systems (ITS) [2]

Advanced applications meant to increase the safety and optimization of traffic systems by allowing vehicles and participants to make more informed actions as they pertain to travel of freight, goods, or travel of a personal nature.

Roadside equipment constantly receive data from various sensors and to other roadside units. i.e. traffic congestion sensors detecting an increase of idle vehicles at a major intersection, so subsequently an update is sent to nearby *Variable Messaging Signage* [10] (Dynamic Message Signs) on roadways prior to the congestion in order to present either a time-frame for congestion to quell, or perhaps to suggest a different route or exit to take altogether.

To varying degrees these systems have agency and effect on other systems which facilitate freight corridor optimization for single and multi-modal freight (when freight travels by multiple modes of transportation), so implications apply to the sectors of Rail, Aviation, and Maritime.

Internet of Things (IoT) [3]

The Internet of things is a very broad terms used to describe either singular groups of physical technological objects with sensing and processing capabilities that connect with and exchange data with other devices and/or systems over communications networks such as the Internet, WiFi, Cellular, etc.

There are varying applications for IoT, to include (but not necessarily limited to, as later versions of this document may include additional items):

- Consumer
    - Smart Home
    - Self Care / Health
- Organizational
    - Medical and Healthcare (IoMT)
    - Transportation and V2X/CV2X
    - Building and Home Automation
- Industrial
    - Manufacturing
    - Agriculture
    - Maritime
- Infrastructure
    - Metropolitan Planning

  - Energy
  - Water & Waste Water
- Military
  - Internet of Battlefield Things (IoBT)
  - Ocean of Things

Overall, IoT provides the capability to monitor and manage various ecosystems to perform predictive maintenance of systems to plan replacements & upgrades, gather operating equipment effectiveness for a manufacturing plant, and so much more.

Manufacturing & Critical Manufacturing [4]

> *"This sector is crucial to economic prosperity and continuity of the United States. A direct attack on or disruption of certain elements of the manufacturing industry could disrupt essential functions at the national level and across multiple critical infrastructure sectors."*
>
> - ***Cybersecurity and Infrastructure Security Agency***

And as previously mentioned, manufacturers make use of IoT and other means of convergent cross-system connectivity to fulfill business use cases and perform predictive maintenance of systems for facilities that create goods and supplies necessary for use in supply-chains for other areas of critical infrastructure and overall quality of life items. The currently identified core industries of critical manufacturing are as follows:

- **Primary Metals Manufacturing**
  - Iron and Steel Mills and Ferro Alloy Manufacturing
  - Alumina and Aluminum Production and Processing
  - Nonferrous Metal Production and Processing
- **Machinery Manufacturing**
  - Engine and Turbine Manufacturing
  - Power Transmission Equipment Manufacturing
  - Earth Moving, Mining, Agricultural, and Construction Equipment Manufacturing
- **Electrical Equipment, Appliance, and Component Manufacturing**
  - Electric Motor Manufacturing
  - Transformer Manufacturing
  - Generator Manufacturing
- **Transportation Equipment Manufacturing**
  - Vehicles and Commercial Ships Manufacturing
  - Aerospace Products and Parts Manufacturing
  - Locomotives, Railroad and Transit Cars, and Rail Track Equipment Manufacturing

Food & Agriculture [5]

> *"The Food and Agriculture Sector is almost entirely under private ownership and is composed of an estimated 2.1 million farms, 935,000 restaurants, and more than 200,000 registered food manufacturing, processing, and storage facilities. This sector accounts for roughly one-fifth of the nation's economic activity."*
>
> - ***Cybersecurity & Infrastructure Security Agency***

This particular sector has varying critical dependencies with many sectors, particularly the following:

- Water and Wastewater Systems, for clean irrigation and processed water
- Transportation Systems, for movement of products and livestock
- Energy, to power the equipment needed for agriculture production and food processing
- Chemical, for fertilizers and pesticides used in the production of crops

Water and Waste Water [6]

> *"Safe drinking water is a prerequisite for protecting public health and all human activity. Properly treated wastewater is vital for preventing disease and protecting the environment. Thus, ensuring the supply of drinking water and wastewater treatment and service is essential to modern life and the Nation's economy."*
>
> - ***Cybersecurity & Infrastructure Security Agency***

In recent times, the Water sector has been identified as a tempting target for bad actors, often targeting remote connectivity as the point of egress. Clean water and management of waste water are vital for the health and safety of citizens.

Global Communications Systems [7]

"The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. "

- ***Cybersecurity & Infrastructure Security Agency***

The criticality of this sector is attributed to provision of enabling functions essential for integrations and interoperability in critical infrastructure. Examples of global communications systems are:

- The Internet
- Data Over Radio Applications
  - Mobile Networks
  - Emergency Communications
- Etc.

Industrial Control Systems (ICS) [8]

This is a broad term which covers varying technologies which are relied upon for industrial process control instrumentation, functionality, and operations. ICS and their components are pervasive in all matter of infrastructure and comprise the systems in which infrastructure sectors enact their functions in the physical world. They cover a wide breadth of applications, i.e. carrying out functions of a Level 0[11] process sensor, relaying functionality to other devices to carry out certain functions, to the engineering and managerial applications contingent upon maintaining agency over such underlying systems.

Implications

Cyberphysical Systems make use of various means and modes of communications in order for components to carry out their functions. Weaknesses in communications protocols and their implementations render the communications layer of a CPS susceptible to compromise. Examples of such can include (but not necessarily limited to, as later versions of this document may include additional items):

- Using current 4G LTE & 5G NR mobile communications network leveraged to carry out attacks on transportation infrastructure.
- Perform attacks on medical devices, such as an insulin pump which uses wireless communications to receive command input and relay information and status.
- Leveraging industrial devices found on the internet to disrupt service of operations.

Challenges

The existing challenges for solutions proposed through the C6 perspective are identified currently as the following (but not necessarily limited to, as later versions of this document may include additional items):

Seamless Integration and Adoption Into (Current) Systems

Coming up with the solution is often the easy part. However enacting the solution can become complicated due to varying factors such as current technology in use and the hurdles that come with employing such solutions. They need to be low-risk enough as to keep drastic system modifications to a minimum and acceptable enough to the managers and engineers of systems to keep the barrier to adoption as low as possible.

Robust, Future-Proof, and Scalable

Proposed solutions to communications problems need to be robust for increased uptime of a CPS. It needs to be able to stand the test of time, and survive in an environment where changes are inevitable and are the norm. And size must not be an issue. As connectivity increases, the solution availability need not be an issue for employers of said solutions.

Current Culture and Buy-In

The core value of a solution needs to be easily understood by various stakeholders in a system or project. That understanding should seek to transcend the executive, administrative, managerial, architectural, technical, and marketing culture barriers as much as possible. C6 goal is not to occupy a slice of real estate in the cybersecurity market and sell to businesses, but rather to create solutions which permeate all sectors of infrastructure and may effect multiple deployable tools or mechanisms.

Mitigating Encroachment to Privacy and Civil Autonomy

A solution must not facilitate any means or mechanism which may jeopardize the personal rights and freedoms of citizens. Mechanisms that endanger a single individual's freedoms essentially endanger everyone's freedoms. On the communications layer, this may include (but not necessarily limited to, as later versions of this document may include additional items):

- Adding additional interfaces to user equipment to suit a use where the desired function can either be performed on an upstream device, or the functionality holds no merit.
- Implementing a backdoor to a communications protocol, specification, implementation, or to utilized encryption.
- Limiting use based on a basis of demographics and personal traits or characteristics.

Conclusion

The increased hyper-connectivity inherent to Industry 4.0 and the IoT movement carry with it an ever expanding attack surface of cyberphysical systems. Critical infrastructure makes use of this connectivity for purposes of optimizing processes, collecting and relaying data, and other communications or industrial needs. The C6 discipline seeks to mitigate as much loss of life and physical damage as possible by securing the communications CPS in critical infrastructure utilize for their integrations and interoperability, and to do so in ways that are robust, intuitive to implement, transcend business & industry culture barriers, and work to preserve the freedoms of citizens that participate in these systems of infrastructure.

References

1. The Nine Pillars of Industry 4.0 - Transforming Industrial Production
   https://circuitdigest.com/article/what-is-industry-4-and-its-nine-technology-pillars
2. ITS Research Fact Sheets
   https://www.its.dot.gov/factsheets/benefits_factsheet.htm
3. Internet of things
   https://en.wikipedia.org/wiki/Internet_of_things
4. Critical Manufacturing Sector
   https://www.cisa.gov/critical-manufacturing-sector
5. Food and Agriculture Sector
   https://www.cisa.gov/food-and-agriculture-sector
6. Water and Wastewater Systems Sector
   https://www.cisa.gov/water-and-wastewater-systems-sector
7. Communications Sector
   https://www.cisa.gov/communications-sector
8. Securing Industrial Control Systems
   https://www.cisa.gov/publication/securing-industrial-control-systems
9. Introduction to Cyberphysical System Integration Security (CSIS)
   https://beta.ideablock.io/idea/lgq
10. Travel Time Messages on Dynamic Message Signs
    https://ops.fhwa.dot.gov/TravelInfo/dms/signs.htm
11. The Purdue Model and Best Practices for Secure ICS Architectures
    https://www.sans.org/blog/introduction-to-ics-security-part-2/

Changelog		
Date	Party/Editor	Change Summary
April 19, 2022	Michael Curnow	Publish Version 1.0 of document.