High-Level Field-Device Event Verification (HFEV)

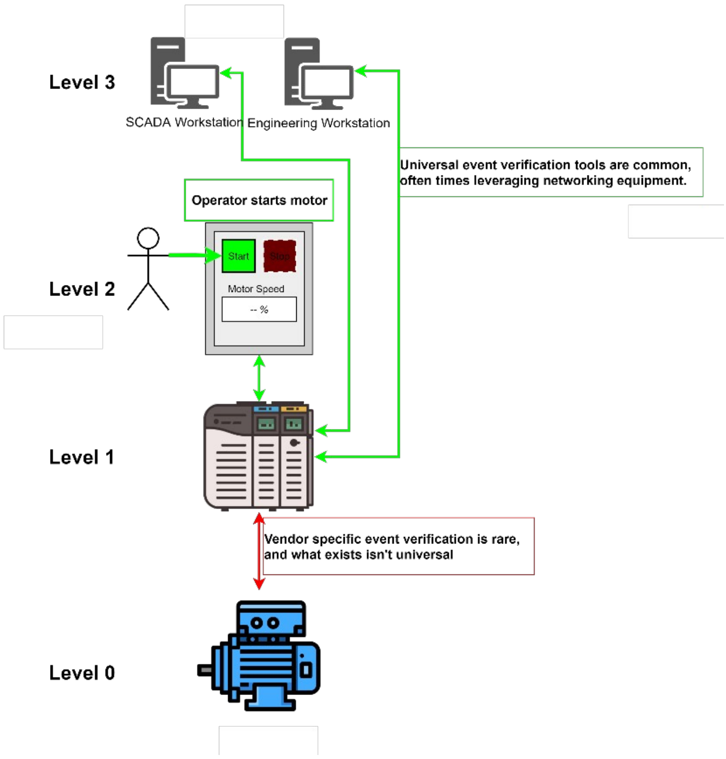
A Proposed Method of Validating Expected Command Execution to Field Devices in a Control Loop.

Michael (Mike) Curnow
C6
May 14, 2022

Page intentionally left blank.

Contents

Abstract


Level 3
SCADA Workstation
Engineering Workstation
Universal event verification tools are common, often times leveraging networking equipment.
Operator starts motor
Start
Stop
Motor Speed
-- %
Level 2
Level 1
Vendor specific event verification is rare, and what exists isn't universal
Level 0

Modern day Cybersecurity incident response and monitoring capabilities for owners of Industrial Control Systems (ICS) operations cover levels 1-5 of the Purdue Model, the networking model of logical segmentation of ICS & Enterprise security zones and assets. Currently no viable universal and **non-commercial** method to confirm an expected operation occurred on level 0 field devices are employed. This paper proposes to introduce a method of verifying expected command execution from PLC to Field Device, making use of a varying array of oscilloscopes to record voltage data as sinusoidal waveform signal data and correlate said data with commands the PLC is capable of executing, and ensure feedback input from field device corresponds to input command(s). The purpose of such data is to act as a source of truth to compare against known commands and operations recorded by systems at the local and site supervisory levels. When such a command discrepancy occurs between a given PLC and respective field sensor or device, this will indicate a high degree of risk that either the PLC is compromised or there is an issue with the field device, and the subsequent operation of either is a danger to site operations, potentially resulting in danger to life and property.

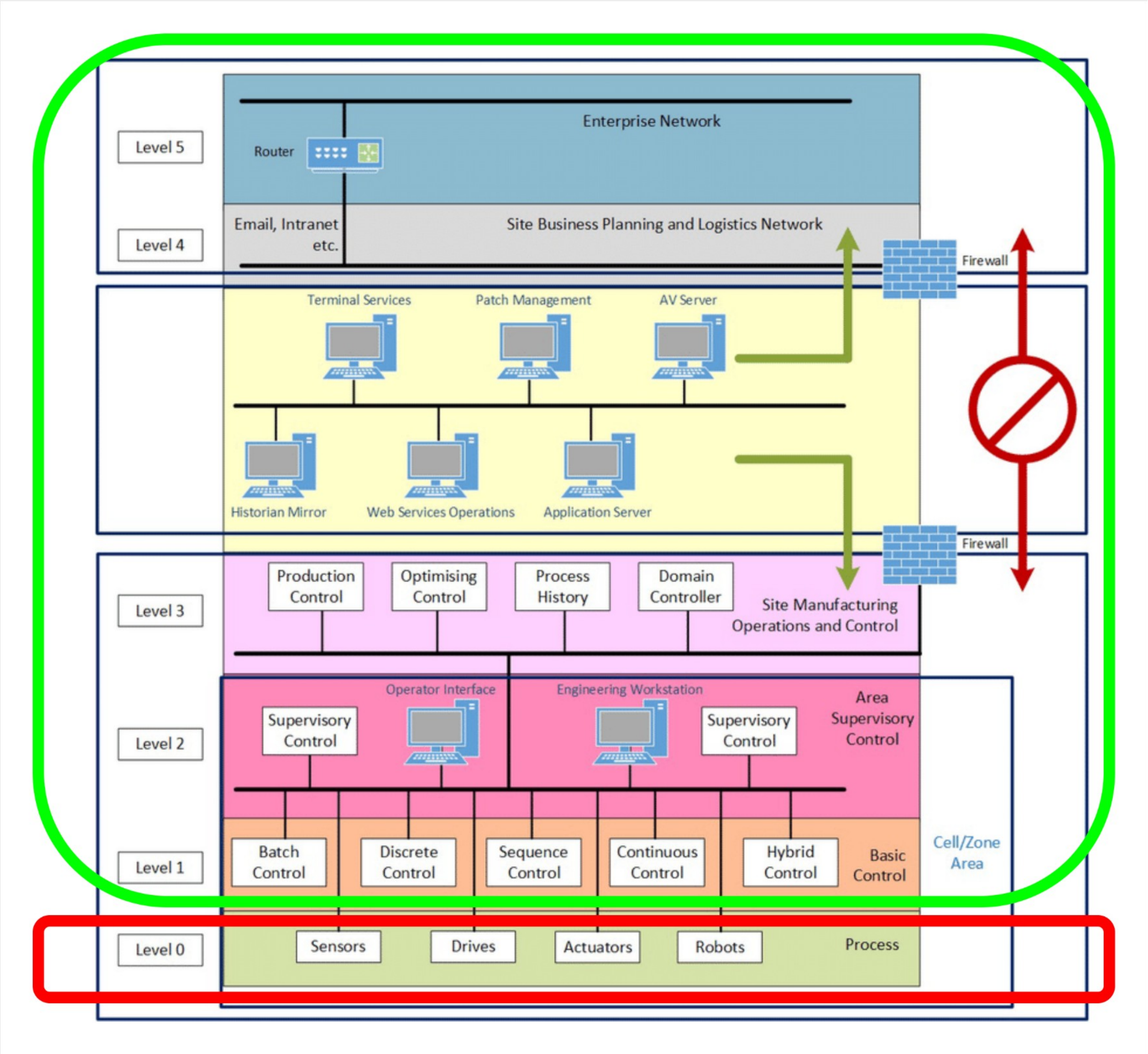
Introduction

Modern day technologies allow for a plethora of asset monitoring capabilities for Information Technology (IT) and Operational Technology (OT). With increased connectivity being the norm as The Internet of Things (IoT) movement, driven by the needs of the 4th Industrial Revolution (Industry 4.0), the ICS sector has adopted this approach to properly manage things like Overall Equipment Effectiveness (OEE), industrial automation, predictive maintenance, and a drastic increase in remote management by site operators and 3rd party vendors & contractors. This effort to increase connectivity with ICS assets to networked resources is referred to as “IT/OT Convergence”, and this *convergence* forces us to evolve the ways we approach the Cybersecurity of industrial assets and their respective networks. There is even already a sect of Cybersecurity products and services dedicated to monitoring and securing ICS devices & networks, and in some cases even their processes (when applicable).

These technologies involved in such monitoring of ICS networks and assets are evolved from the IT paradigm of employing Network Intrusion Detection Systems (NIDS), Host Intrusion Detection Systems (HIDS), File Integrity Management (FIM), and User and Entity Behavioral Analytics (UEBA). Some vendors go so far as to add abstracted computational layers of “Machine Learning” and “AI” to determine abnormal behavior of networked assets based on aggregation and computation of data, most of which are previously mentioned. These solutions are great for bolstering the cybersecurity of ICS operations. However, since IT and OT paradigms don’t necessarily run in parallel, this causes a dissonance in what constitutes “safety” and “security” in both realms. The quintessential example of this collide is the conflicting cybersecurity “Rules of engagement” between IT’s *Confidentiality, Integrity, and Availability* (CIA) the proposed and constantly echoed *Safety, Availability, Integrity, and Confidentiality* (SAIC). This gulf in operational understanding serves to actually often reward the cybersecurity solutions that are more fit-for-purpose regarding ICS Cybersecurity, whereas the more generic IT Networking and Asset monitoring services fall on the wayside. Currently most major industrial sector’s cybersecurity standards do not account for securing or monitoring the level 0 equipment, leaving gaps in the state of security for various industrial sectors.

With all this said, there is one glaring question in the ICS Cybersecurity space and community that has gone unanswered, or at least not answered well enough, and that is: “But what about the Field Devices”? As it stands now, the only real monitoring occurring on field devices are performed by utilizing physical sensors to relay telemetry of metrics such as vibration, temperature, location, etc. These solutions typically make use of 4G (and soon to be 5G) connections to relay telemetry to remote resources where OEE is calculated and predictive maintenance plans can accurately occur. These are operational use cases where the data *can* potentially be used as individual data feeds in the larger pipeline of what cybersecurity analysts could use to detect issues with field assets. But these scenarios are circumstantial, are extremely vendor driven, and there is no “across the board” solution to factor in these metrics to the larger picture that cybersecurity analysts need to effectively triage and investigate cybersecurity and safet incidents on a plant floor, a railway’s traction power system, or Advanced Transportation Controller (ATC) roadside equipment for a municipality’s Intelligent Transportation System (ITS).

In the following graphic, areas in red illustrate were the issue pertains to.



Right now, the only way to confirm that a PLC carried out commands via an HMI, management workstation, or it’s programmed functions, is to physically or visually monitor the field device executing on it’s given directive. However, a PLC can be compromised to provide false readings and feedback to oversight mechanisms in its managerial hierarchy. This is why the “Level 0 Problem” is such an extremely important issue to resolve as immediately as we can, independent of vendor and commercial motivations.

In order to protect critical infrastructure site operations, I am proposing an answer to the issue posed in the aforementioned question, a solution that can be universally deployed, is vendor agnostic and highly interoperable, and is indiscriminate to any network architecture. By using a multi-threaded array of virtual oscilloscopes in small form factor computers to monitor deltas in sinusoidal waveform signal data generated from Input/Output (I/O) when enacting known PLC commands and operations, where we can create a single universal “source of truth” to validate the fidelity of PLC operations in control loops to substantiate what it actually performs and what it reports from the field devices.

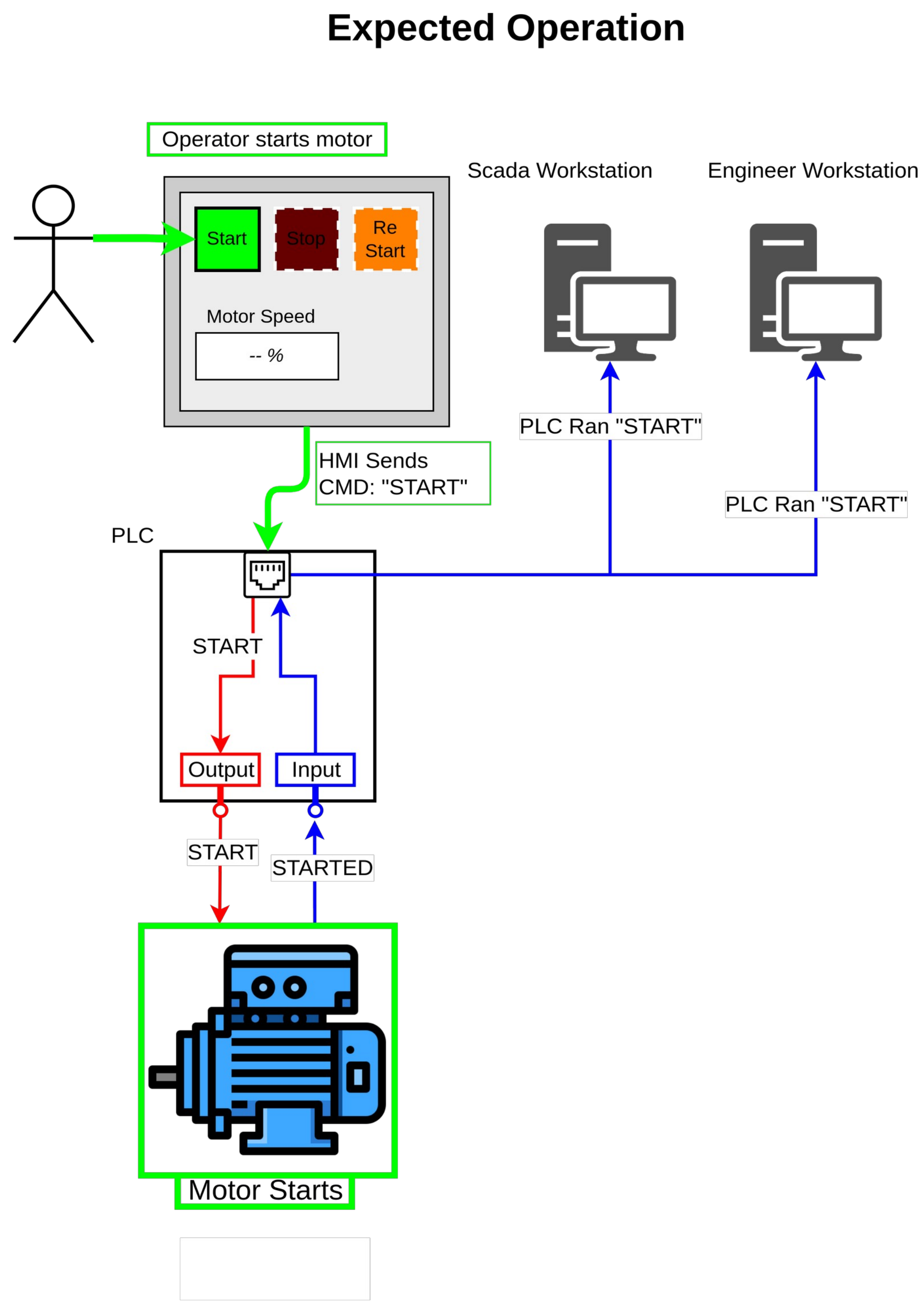
I’ve designated this method “High-Level Field-Device Event Verification” (HFEV), as this proposed solution does not employ any mechanism on the level 0 field device itself, instead we’re operating at level 1 to ascertain the validity of field device action by monitoring the PLC’s I/O voltage amplitude and frequency to confirm the desired action of the level 0 field device occurred. It may help to think of this solution as “Level 0.5 monitoring”.

Exploring the Current Problem

When a PLC acts on its designated programming, there is an implicit trust in the PLC itself and the data & status rendered in the HMI and other monitoring and execution mechanisms. However, a compromised vendor can ship out PLCs with malicious code in it, backdoors in vendor PLCs can allow bad actors to modify PLCs in various ways, bad actors with physical or network access can commit acts detrimental to PLCs and it’s processes and field devices, and malicious firmware updates or patches can act as additional vectors to introduce malicious code and functions into the target PLC(s). To further illustrate the point, we will explore expected vs unexpected operation.

Expected Operation

Below is an illustration of a PLC properly turning on a simple motor.

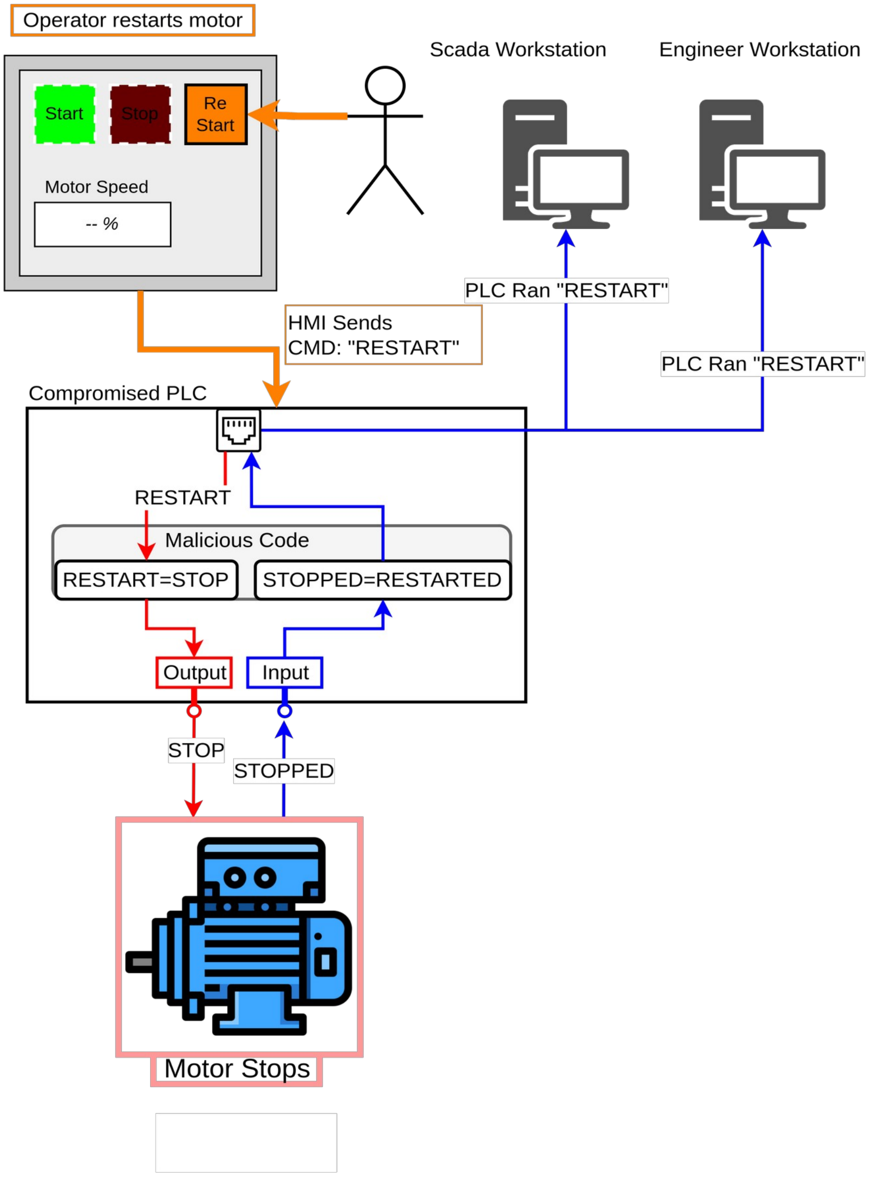


Operator successfully starts the motor via the HMI without issue.

Unexpected Operation

Below is an illustration of a compromised PLC executing a different command than what the operator input to the HMI.

Unexpected Operation



The operator executed the “RESTART” command, however when that command was received, a malicious code function flipped that command from “RESTART” to “STOP”, thus rendering the initial command function inert, all the while reporting to it’s supervisory control systems that the command successfully ran.

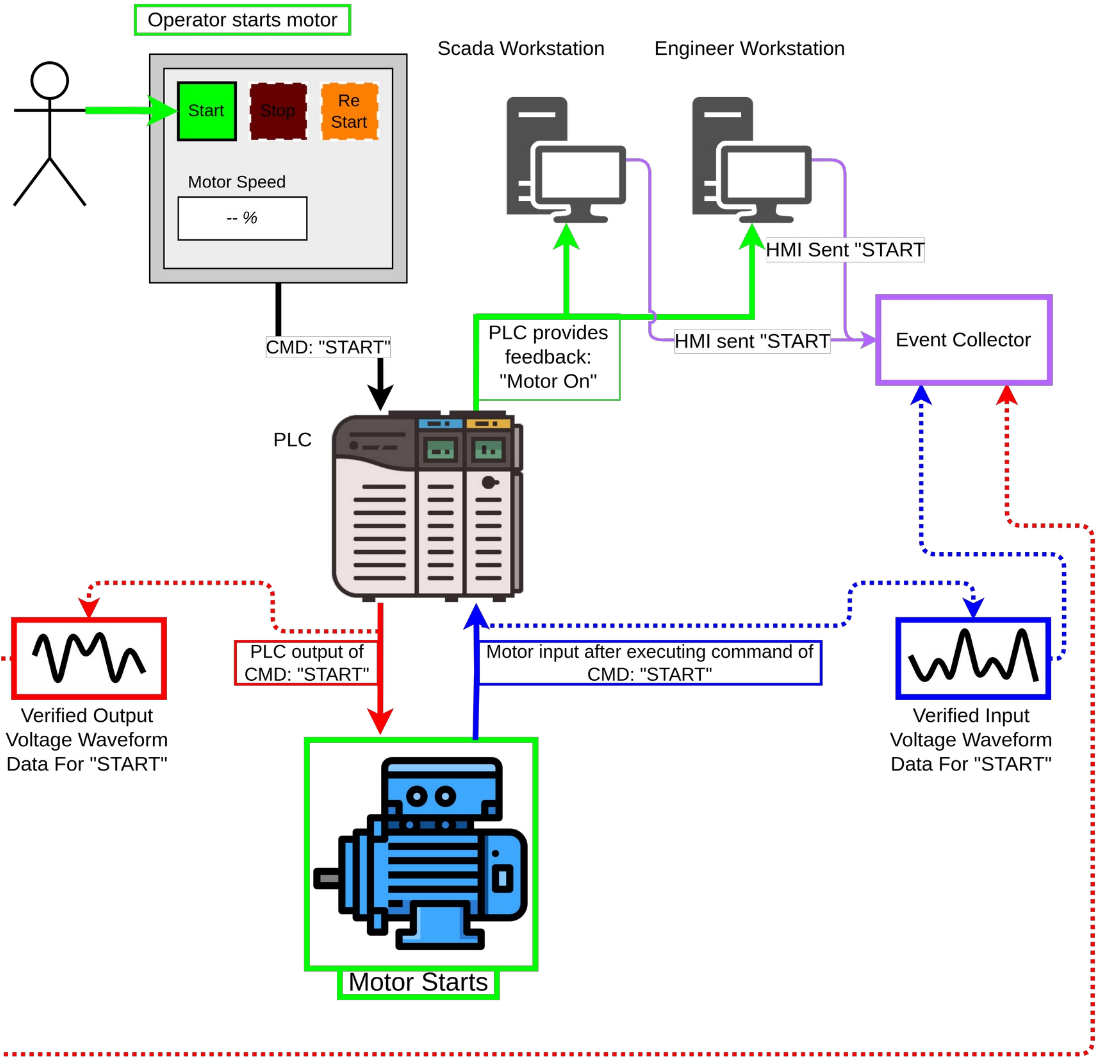
Solving the Current Problem

The following scenarios illustrate the deployment of the aforementioned form factor on a site network providing an industrial cybersecurity monitoring solution (client-owned or 3rd party) with verified PLC command I/O waveform data to a level 0 field device.

Valid Operation with HFEV

In this diagram we observe the command of “START” being input to the HMI, and the waveform data matching the proper I/O of that PLC’s command to “START” the motor.

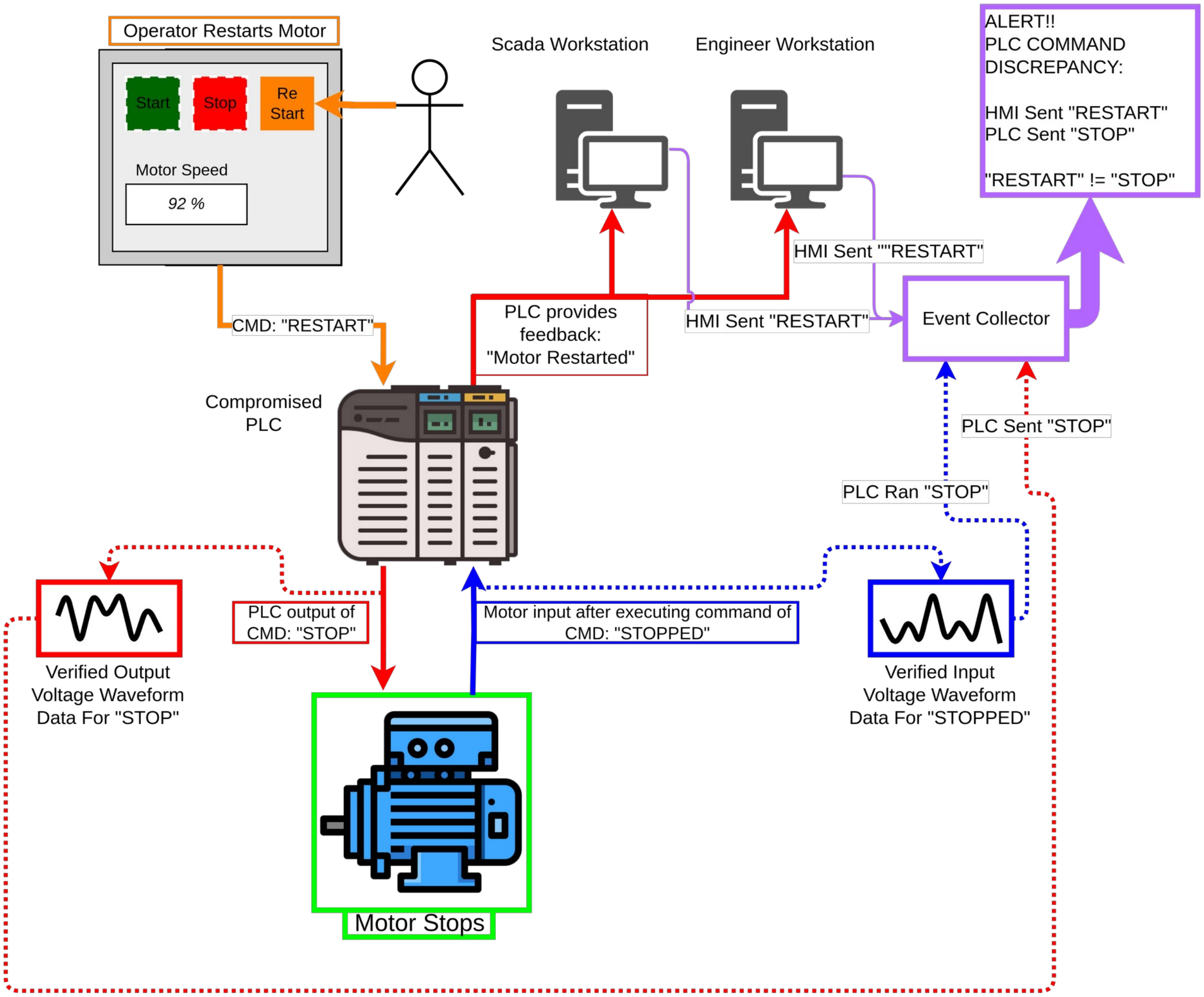
Valid Operation With HFEV


Operator starts motor
Start
Stop
Re Start
Motor Speed
-- %
Scada Workstation
Engineer Workstation
HMI Sent "START
CMD: "START"
PLC provides feedback: "Motor On"
HMI sent "START
Event Collector
PLC
PLC output of CMD: "START"
Motor input after executing command of CMD: "START"
Verified Output Voltage Waveform Data For "START"
Verified Input Voltage Waveform Data For "START"
Motor Starts

Invalid Operation Detected with HFEV

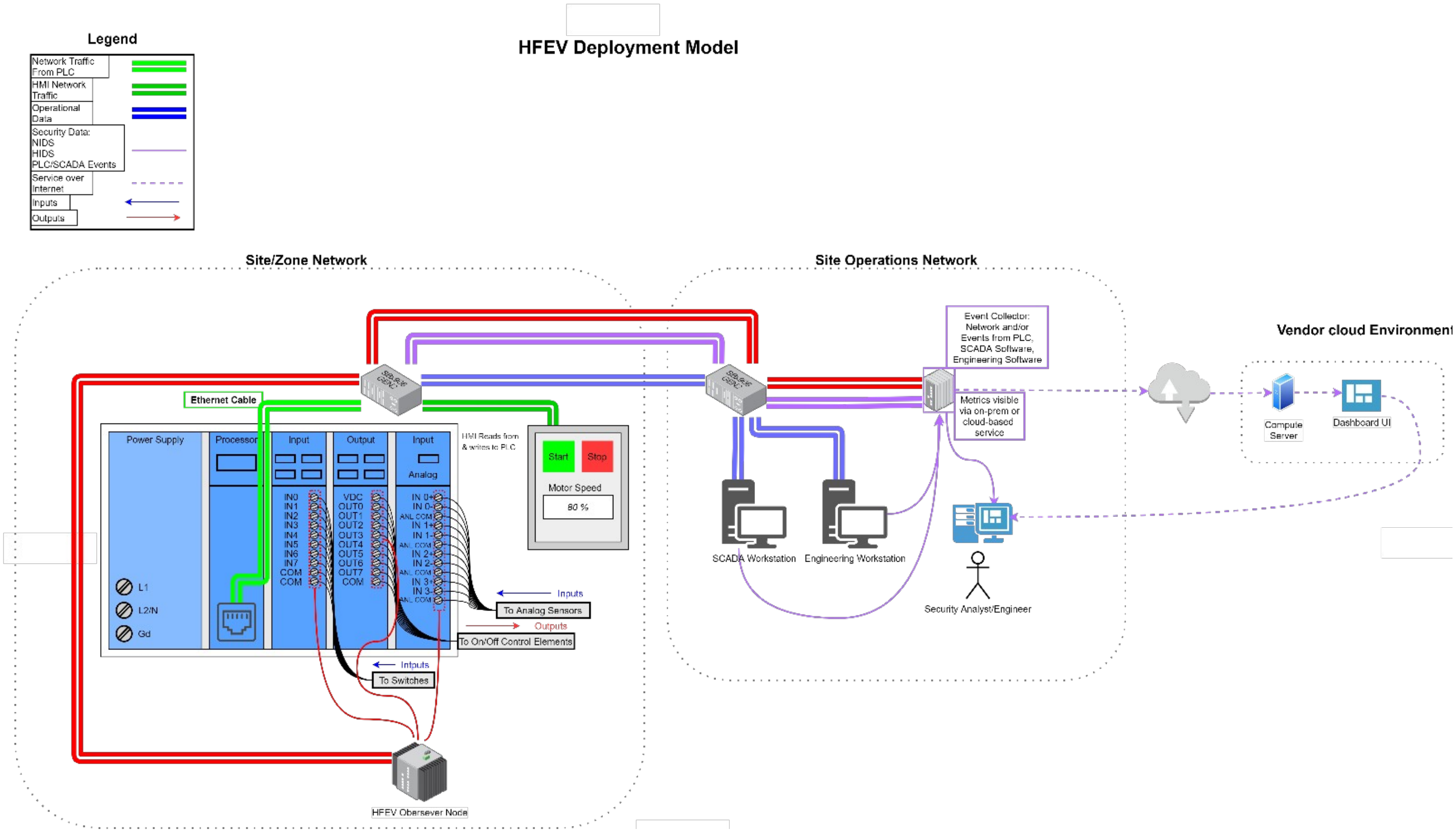
Here we see that while the command “RESTART” was input to the HMI, the compromised PLC modified the command to “STOP” and rendering the initial command null and reported a successful “RESTART” operation to supervisory systems. However, in this scenario with an HFEV mechanism deployed, where this command discrepancy occurrence was recorded as the I/O waveform data did not match up with what the PLC reported to its supervisory systems, thus creating an alert which both cybersecurity analysts can triage those incidents and operators can triage for safety and operation uptime.

Invalid Operation Detected With HFEV



The Bigger Picture of ICS Cybersecurity Monitoring

Computer units deployed to handle HFEV operations would be flexible in how they're deployed, how they work with leads & I/O contacts, and how they drive data upstream to client's security monitoring solutions, ITSM systems, and Enterprise Resource Planning (ERP) systems (i.e. this data can be sent anywhere it's needed). Waveform data will be converted to generic information that can be consumed by varying collection mechanisms, and network traversal can be handled at the site's switch or by 4G/5G cellular modems if necessary.



Additional Use Cases

Though HFEV was conceived through the aperture of solving the "Level 0" problem of cybersecurity monitoring, there are many applications this solution can suit. These include (but are not limited to):

- Alerting site operators to field device malfunctions
- Alerting site operators to PLC malfunctions
- Additional supplemental data-feed to calculate OEE
- Additional supplemental data-feed factored for predictive maintenance
- Additional supplemental data-feed for service management or ERP