Edge Deployed Cyber Security Hardware Architecture for Energy Delivery Systems

Sterling S. Rooke[1] and Peter L. Fuhr[2*]

[1]University of Tennessee, Dept. of Electrical Engineering and Computer Science, Knoxville, Tennessee, 37996, USA
[2]Oak Ridge National Laboratory, One Bethel Valley Road, Oak Ridge, Tennessee, 37831 USA

Abstract - *At a time of accelerated cyber conflict, an "edge deployed" system will supply sensor based cyber ground truth to live grid models, and under secure command, take complete control of suspected rogue programmable logic controllers (PLCs) to maintain bulk power delivery to chosen critical sites. This hardware solution is purpose built to be agnostic to PLC vendor or protocol with the realization that a widely deployed solution must function with existing devices for rapid adoption by industry. An overview of the situation and how this developed system functions is provided.*

Background

Critical Infrastructure is defined as "systems and assets, whether physical or virtual, so vital to a nation that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters". Critical Infrastructure Protection (CIP) consists of actions taken to prevent, remediate, or mitigate the risks resulting from vulnerabilities of critical infrastructure assets. Depending on the risk, these actions could include changes in tactics, techniques, or procedures; adding redundancy; selection of another asset; isolation or hardening; guarding, etc.

The comprehensive U.S. federal program for cybersecurity in energy delivery originated largely in 2000 under the National Plan for Information Systems Protection, which identified the electric power system and pipelines as critical infrastructure "that could be a target for significant cyber or physical attacks."[1] In particular, the plan stated:

The cyber nation of our infrastructures has created an intense reliance upon an underlying fabric of telecommunications and information networks. The infrastructures also rely heavily upon the Nation's energy production and distribution networks, especially through the I&C [information and communications] infrastructure's energy requirements.

Within the U.S., the electric grid consists of over 700,000 miles of transmission lines and over 55,000 substations linking over 7,000 power plants to around 150 million customers. Similarly, the U.S. energy pipeline network is composed of over 2.9 million miles of pipeline transporting natural gas, oil, and hazardous liquids; the natural gas transmission pipelines feed approximately 1,400 local distribution systems serving over 67 million customers. These vast networks comprise the critical backbone of the U.S. energy delivery system (and energy supply), supporting the vast majority of U.S. economic activity and playing a vital role in national operation. Consequently, the secure operation of both the power grid and pipelines are national priorities. In May 2018, the U.S. Department of Energy (DOE) released the Multiyear Plan for Energy Sector Cybersecurity, which provides a vision of resilient energy delivery systems designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions. The plan serves as guidance for private, public and academic sectors to coordinate research, development and deployment of tools, techniques and policies that are to enhance the cyber and physical security of EDS systems and operations.

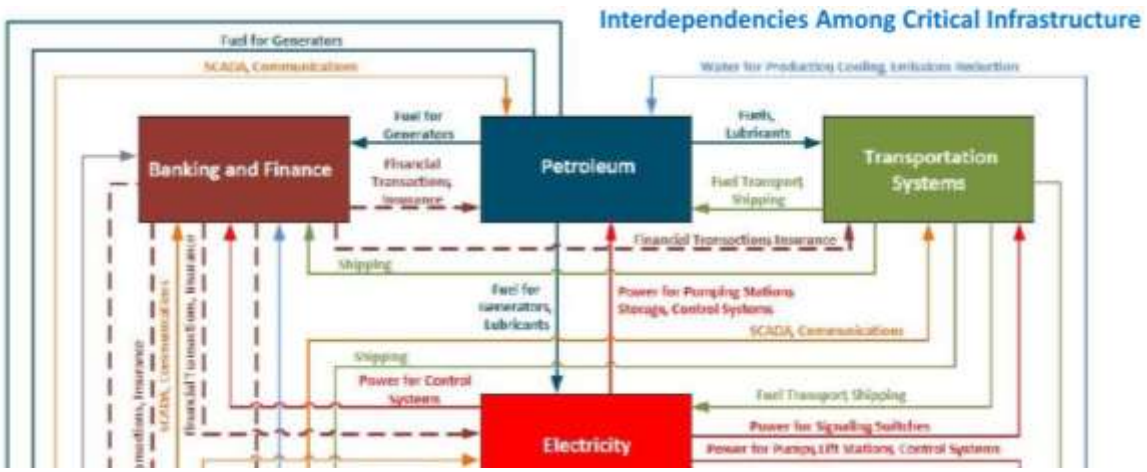
Energy Delivery Systems and Connectivity

Fig. 1 shows the interdependence of energy delivery systems. This was a key topic discussed at the NASEO Energy Policy Outlook in 2018, with the summary that a system that directly addresses cyber vulnerabilities and intertwined functionality across these energy delivery systems is needed. A question that frequently arises is how real is the threat to critical infrastructure?

From the Liberty Eclipse DOE and NASEO energy cyber exercise, a key finding directly outlined concern with the loss of petroleum and power outages from cyber of kinetic events.

Key Finding #2[1] – The public will face a great deal of uncertainty following a significant cyber incident that causes physical damage (such as a long-term power outage or petroleum disruption), creating a considerable challenge for public information and expectation management, particularly around restoration times. [3]

[1] Key Finding 2 was selected from the Liberty Eclipse Action Report



(Representative only, diagram truncated)

Fig. 1. Energy Delivery Systems and their many connections [2].

The ever-increasing global demand for energy has propelled supporting sectors to innovate and adopt evolving technologies in order to deliver bulk power to growing demanding populations. The adoption of technologies such as Programmable Logic Controllers, Personal Computers, Routers and Switches, Computerized Human Machine Interfaces (HMI), etc. in the power production and other Critical Infrastructure and Key Resource (CIKR) industries has innocently introduced vulnerabilities, which, if exploited and leveraged, could have massive negative consequences. In order to prevent such catastrophic scenarios from occurring, a hardware device that will monitor, secure, and provide assurance to operations in the bulk power generation industry is needed.

As indicated by a recent alert published by the United States Department of Homeland Security's (DHS) Computer Emergency Readiness Team (US-CERT) the threat to CIKR is not a farfetched illusion. The alert pointed out that circa March 2016 Russian government sponsored cyber assailants had been targeting US government interests as well as organizations and companies associated with power production, including nuclear, water treatment and distribution, manufacturing, and aviation. Investigations by law enforcement agencies and DHS uncovered a vast repertoire of tactics, techniques, procedures, and capabilities employed to gain access and maintain persistent access to the different victims' systems and networks. The alert stated that "in multiple instances, the threat actors accessed workstations and servers on a corporate network that contained data output from control systems within energy generation facilities. The threat actors accessed files pertaining to ICS or supervisory control and data acquisition (SCADA) systems." Unfortunately, the alert does not provide the reason why the actors where gaining access to these systems but with the level of access they had one can only imagine what they could have done had their intent changed from data gathering to sabotage.[1]

As another example, although this piece of malware did not target PLCs, the devastating effects of NotPetya were felt throughout the shipping, retail, and power generation and distribution industries. This malware seems to have been developed to mimic ransomware behavior; however, analysis has shown that once the malware encrypted files on disk, the encrypted content could not be decrypted even after paying the requested ransom.[2] Some of the reports indicated that Russian hackers may have been behind these attacks.[3] In particular, the Ukrainian power grid was one of the major victims of this ransomware.

Russian sponsored cyber assailants have exploited vulnerabilities and gained access to CIKR throughout the globe. In addition, they have leveraged their access to manipulate the generation, control, and distribution of electricity.[4] This section provides a small sample of what is now taking place throughout the world. We've focused in the alleged Russian cyber-attacks to CIKR due to their newness and news reporting but there are other countries with cyber capability that we should also be concerned about.

Leveraging New Technologies to Solve Cyber Threat Challenges:

Given the potentially wide-ranging implications for such cyber-attacks on CIKR – coupled with the variety of such cyber-attacks - there are a number of new technologies that can be used in addressing the challenges. The technologies lie at the intersection of computational systems, collaborative sensors, communications, and logical architectures for Internet of Things (IoT) and related application areas. While the notion of correlating measurements taken at different times and locations is hardly new and crosses into the realm of sensor/data

fusion[2] [4], having measurements with accurate geolocation and time stamped metadata provides a basis for a variety of mathematical tools to be applied in the analysis – both trends and predictions – of seemingly disparate information sets.

Use of Distributed Databases for IoT Synchronization:

- Message Propagation
- Command verification
- Correct operations

The use of distributed ledger technology to assure device cyber posture and integrity of industrial controls data. By using distributed data sets and ledgers, a cyber attacker or simple equipment failure will have minimal impact upon operations.

Visualization of Interconnected Energy Delivery System Information: Many data valuation tools exist, one in particular to highlight is EAGLE-I. In recent years the U.S. Department of Energy identified a need for a capability that could display the nationwide status of the electric grid. The capability named EAGLE-I leverages web technology to aggregate electrical grid service status data and display it over a map. This information can be fused with other data sets to show multiple overlays each depicting unique patterns such as weather, oil pipeline, and electric distribution. This integration of information present in a network-centric application (and associated database) provides the platform for modeling, simulation, and data display capabilities to provide another overlay of status of the involved sensor network(s).

Machine Learning: The need for rapid response – operating a "machine speed" rather than human speed – requires integration of machine learning to gain a better understanding of each PLC. The associated sensor monitors leverage supervised learning utilizing the optimal operating parameters for the PLC that are stored in the distributed database. Over time, machine learning provides a better understanding of the day to day operations of the PLC allowing the system to have a fine grained knowledge of normal PLC operations. The pattern of life data is then used to update the current models of the power infrastructure.

Detection of Anomalous Behavior in Programmable Logic Controller: Leveraging the machine learning and distributed information set architecture allows the sensor monitor to have insight into all components of the PLC as well as the commands sent to the PLC. This command set – when compared with the broader time set of information – allows for classification of deviations from the device's pattern of life. The anomaly detection system automatically assigns registers into one of the three classes, learns and models their behavior, and raises alerts when register values deviate from the learned models.

A Dynamic Architecture

The high-level objective for this hardware based dynamic architecture solution was; to protect bulk electrical power supplies to critical sites of our choosing. Some examples of sites are: hospitals, communications facilities, water/wastewater facilities, etc. This is achieved by maintaining oil & gas pipeline flows for bulk power generation. This is done by:

1. Protecting the pipeline from cyber attack and thus disruption
2. Promoting resilience in the face of kinetic and cyber events

Informed by grid, pipeline, and Programmable Logic Controller (PLC) models; a hardware based solution for dynamic controls architecture is formed. This, in turn, leads to a hardware based solution (PLC overlay module) with a flexible design informed by models and industrial constraints. Furthermore, the models used to design such a hardware based solution will serve a control mechanism should the system be activated during a heightened cyber or kinetic posture.

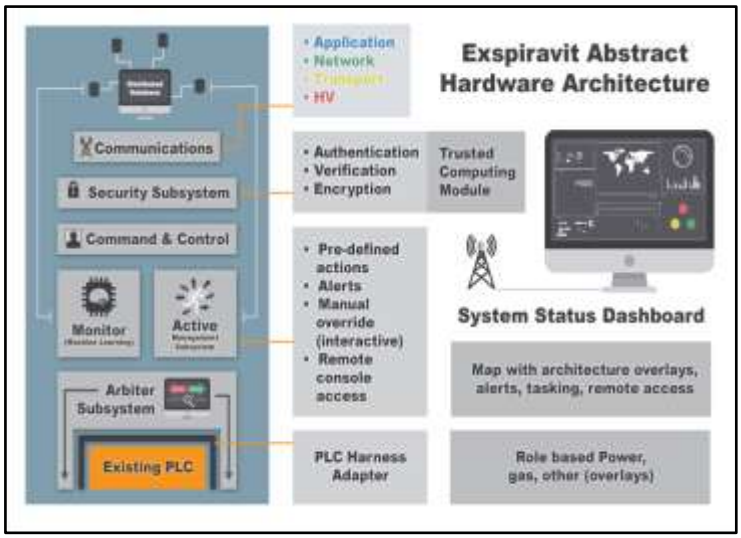


Fig. 2. A hardware architecture abstraction.

[2] The following data fusion description has been extracted from New World Vistas: Air and Space Power for the 21st Century, Chapter 3 (accessed at http://www.au.af.mil/au/awc/awcgate/vistas/vistas.htm): "…there is a greater demand to expand the dimensionality of sensed information acquired—driving the need for multiple sensors and the combination of that data. This demand to expand the time and space dimensionality of sensed data adds two important themes to New World Vistas: (1) sensors must be designed to be integrated and coordinated to maximize the overall system measurement process, and (2) processes are required to efficiently and accurately correlate and fuse data from a variety of sensors."

There is, currently, no ability to regain control of a fielded PLC following a cyber intrusion or reform the overall system architecture in real-time after a cyber or kinetic attack or even a general failure. This multi-domain consideration is addressed by combining grid, PLC (industrial control), and energy pipeline information with dynamic control architectures implemented by the hardware solution. Through this edge deployed system, at a time of accelerated cyber conflict, the system will supply sensor based cyber ground truth to grid models, and under secure command take complete control of suspected rogue PLCs to maintain bulk power delivery to chosen critical sites. The essence of deployment at the network edge lies in having a dynamic architecture invoked – and if deemed necessary – reconfigured by a hardware based solution that is linked to a cyber risk management framework. Failing to account for cybersecurity in what appears to be an isolated system, not only renders an approved Authority to Operate (ATO) invalid, it exposes critical sites to power loss at a time of cyber or kinetic conflict.

Considerations must be given to Internet of Things (IoT), growing Industrial (IoT or IIoT), and Platform IT (PIT) standards. Deployed PLC-based architectures are guided as a monolithic solution that simply overlooks any real consideration of dynamic cyber vulnerabilities and threat environments. Moreover, there is no true lifecycle consideration that accounts for changes in technology, changing and evolving adversaries, and associated cyber intersections. IoT, IIoT and PIT systems may lie throughout the utility's network (IT and OT). Having the edge deployed cyber sensor system may allow for network-centric isolation of such devices if they are deemed to be cyber vulnerable (or have been cyber compromised).

As cyber technologists know, today's control systems are most frequently specially designed digital systems that operate real-time physical processes by dispatching commands to numerous sensors, actuators, communication nodes, and devices dispersed across the automation infrastructure. These systems can exchange massive amounts of data at high speeds over communication networks to monitor and control physical devices. Industrial Command and Control (C2) systems operate within the operational technology (OT) environment under rules that have different priorities and policies from standard information technology (IT) systems. In the past, OT and IT systems were largely isolated from one another, with the Internet connected to the "IT side." However, in today's modern automation systems, OT and IT systems are connected, which implies that cyberattacks can originate in business systems and migrate to operational systems-or in demonstrated occurrences the attack reverses with the malware entering via the "OT side."

The Systems Design

Historically, automation systems were physically separated from the Internet and other networks. With the advent of commodity platforms and common Internet protocols, automation and control systems can now be built at a much lower cost and can use generally available Internet protocols. This results in increased efficiency and significant cost savings, but as the Industrial Control Systems - Computer Emergency Response Team (ICS-CERT) (https://ics-cert.us-cert.gov) reported, the convergence of closed control systems with open Internet-based networks, commodity operating systems, and commodity Internet protocols has brought increased security risk.

Inherent network security arises through a hardware based solution – with its ability to instantly isolate a PLC and then operate in its place – being always positioned upstream of IP (IT) communication and downstream of OT communication. Such an architecture implemented via edge-deployed sensors with Machine Learning capabilities provides the control system with a historical perspective which is used for refined change detection. Operating at machine-speed allows the system the ability to send indication and warning (I&W) and take automated responsive actions. Through knowledge of the historical operational basis, the edge devices may assume control and shunt a suspect PLC. This is true no matter if the PLC is suspected of cyber intrusion or simply electrical failure, learning over time will inform responsible action. The net result is a system comprised of two component classes: (1) deployable sensors, which is the physical hardware that would interact with an existing PLC or RTU, and, (2) a control instrument panel, which aggregates sensor data, provides situational awareness of all deployed sensors, and allows for command and control of deployed devices.

Sensor System components:

The principal components of the edge deployed cyber sensor system are presented in Fig. 3. Descriptions of the components are provided.

PLC Harness Adapter: Provides a versatile connector interface for the sensor to connect and communicate to various models of PLCs manufactured by companies such as Allen Bradley, Siemens, Omron, etc. Through this harness adapter the Exspiravit will be able to see and enable interaction with all inputs and outputs to and from the PLC. Fig. 3 depicts this interface as a dark line between the Existing PLC and the Arbiter Subsystem.

Arbiter Subsystem: The arbiter has two modes of operation; passive and active. Passive mode allow for the Monitor Subsystem to watch all transactions without any interaction or making changes to any telemetry or commands. Active mode is enabled by either an external command or by a set of predefined conditions and has full interaction with all input and output signals from the PLC.

When Active mode is enabled, the subsystem converts commands from the Active Management subsystem to commands that can be processed by the PLC. The Arbiter has the ability to change commands if it detects malicious commands being sent to the PLC. Commands are routed from the arbiter subsystem through the PLC harness adapter to the PLC.

Sensor Monitor: This monitor leverages machine learning technology to build a model of normal and abnormal behavior. The sensor monitor passively parses telemetry data from the PLC to build a pattern of life for the PLC. The PLC telemetry data is then examined to be within operating ranges as specified by the sensor distributed database and/or within normal pattern of life parameters. PLC pattern of life operations behavior are be used to enable identification of anomalies in the PLC. If the telemetry data deviates from normal operation the command and control subsystem is notified to send an alert. The sensor monitor continuously writes telemetry data to a 64 megabyte ring buffer. This data can be used forensically to determine possible cause of the sensor alert.

Command and Control (C2) subsystem: The C2 subsystem receives alerts from the monitor subsystem when the PLC deviates from normal operating parameters. Upon receiving an alert, the C2 notifies the active management subsystem to take control of PLC operations. C2 then communicates with security module to initiate sending out a status message to Dashboard backend system. C2 also sends the alert message to the active management subsystem to enable it to perform necessary actions.

Authentication subsystem: The function of this subsystem is to authenticate remote access to the server. This provides validation of sensor configuration files secured with distributed ledger technology.

Communication subsystem: While the communication subsystem serves as the framework for information exchange it also transmits the status of the sensor to central monitoring system. The transmission consist of a sensor Universal Unique Identifier (UUID) and sensor status code.

Due to the system being inherently geographically dispersed, it lends itself to employ a distributed database propagated through encrypted communications and validated using blockchain technology. This technology allows each device to securely communicate with other sensors, update the PLC supervised learning data, maintain the overall status of the network, and send the latest status to the control panel interface even if sensors go offline.

Fig.3. Built-in Resiliency via Distributed Secure Communications and Data Storage

Summary

The advancements in computational capabilities of inexpensive microcontrollers, microcomputers and software development tools provide the framework upon which such a cyber sensor system may be constructed. This, in turn, allows for "sensors-on-the-edge" to perform local signal processing capabilities and respond to network-centric cybersecurity queries. The convergence of these technologies and capabilities leads to a class of sensors that are, depending on implementation, capable of performing varying levels of distributed monitoring and actuation/control possibilities thereby reducing the risks associated with losing communications with a centralized controller (e.g., SCADA). In this realm, regions within an electric utility that have such intelligent, operationally flexible sensors may collectively function as an information and controls microgrid possessing, for example, a reduced time history distributed ledger historian with AI capabilities to operate the associated electrical microgrid in varying manners.

References

[1] The White House, National Plan for Information Systems Protection, February 2000, https://fas.org/irp/offdocs/pdd/CIP-plan.pdf

[2] 2018 NASEO Energy Policy Outlook Conference, Washington D.C., February 7, 2018

[3] 2016 Liberty Eclipse DOE & NASEO Exercise, December 8-9 2016

[4] New World Vistas: Air and Space Power for the 21st Century, Chapter 3 (accessed at http://www.au.af.mil/au/awc/awcgate/vistas/vistas.htm):

[5] "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors." https://www.us-cert.gov/ncas/alerts/TA18-074A, March 15, 2018

[6] Thompson, Lain, Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide, https://www.theregister.co.uk/2017/06/28/petya_notpetya_ransomware/, 28 Jun 2017

[7] Fox-Brewster, Thomas. NotPetya Ransomware Hackers 'Took Down Ukraine Power Grid,' https://www.forbes.com/sites/thomasbrewster/2017/07/03/russia-suspect-in-ransomware-attacks-says-ukraine/#dcf8bae6b89d,

[8] Bingham, Christopher M. Russia's Continued Cyber Operations Targeting its Adversaries' Energy Sectors. Diss. Utica College, 2018.

[9] The Development of EAGLE-I: the First-Ever Technology to Track Power Outages Nationwide

[10] Hong, Junho, Chen-Ching Liu, and Manimaran Govindarasu. "Integrated anomaly detection for cyber security of the substations." IEEE Transactions on Smart Grid 5.4 (2014): 1643-1653.