Cyber Security and Information Systems Information Analysis Center 4/30/15, 11:07 AM

Login / Register

Cyber Security & Information Systems Information Analysis Center

About Resources Community Services

Software Engineering | Cybersecurity | Modeling & Simulation | Knowledge Management

Home » Resources » CSIAC Journal » Supervisory Control and Data Acquisition » The Efficacy and Challenges of SCADA and Smart Grid Integration

The Efficacy and Challenges of SCADA and Smart Grid Integration

The advent and evolution of the Smart Grid initiative to improve the electric utility power infrastructure has brought with it a number of opportunities for improving efficiencies, but along with those benefits come challenges in the effort to assure safety, security, and reliability for utilities and consumers alike. One of the considerations in designing the capabilities of the Smart Grid is the integration of Supervisory Control and Data Acquisition (SCADA) systems to allow the utility to remotely monitor and control network devices as a means of achieving reliability and demand efficiencies for the utility as a whole. Given the ability of these systems to control the flow of electricity throughout the network, additional planning and forethought is required to ensure all possible measures for preventing compromise are considered. This work discusses the overall architecture(s) used today and some of the measures currently implemented to secure those architectures as they evolve. More importantly, it considers simplifying the complexity of implementing the many standards put forth by applicable standards and regulatory bodies as a means to achieve realistic governance.

Introduction

Utility infrastructures represent privileged targets for cyber terrorists or foreign state-sponsored hackers. There are a number of challenges to achieve a base-level security across the utility spectrum. The challenges are due to limited budgets, privately owned control systems in utility infrastructures, and the complexity in decomposing the myriad sets of requirements from competing regulatory bodies each with their own frameworks. The process of developing a functional, secure infrastructure requires technology skills and understanding how and why all applied technologies interact with each other.

In this section, the SCADA and smart grid are explained to discuss the efficacy and challenges in the integration process.

SCADA

Supervisory Control and Data Acquisition (SCADA) systems are basically Process Control Systems (PCS) that are used for monitoring, gathering, and analyzing real-time environmental data from a simple office building or a complex nuclear power plant. PCSs are designed to automate electronic systems based on a predetermined set of conditions, such as traffic control or power grid management. Some PCSs consist of one or more remote terminal units (RTUs) and/or Programmable Logic Controllers (PLC) connected to any number of actuators and sensors, which relay data to a master data collective device for analysis. Gervasi (2010) described SCADA systems with the following components:

> *Operating equipment:* pumps, valves, conveyors, and substation breakers that can be controlled by energizing actuators or relays.
>
> *Local processors:* communicate with the site's instruments and operating equipment. This includes the Programmable Logic Controller (PLC), Remote Terminal Unit (RTU), Intelligent Electronic Device (IED), and Process Automation Controller (PAC). A single local processor may be responsible for dozens of inputs from instruments and outputs to operating equipment.
>
> *Instruments*: in the field or in a facility that sense conditions such as pH, temperature, pressure, power level, and flow rate.
>
> *Short-range communications*: between local processors, instruments, and operating equipment. These relatively short cables or wireless connections carry analog and discrete signals using electrical characteristics such as voltage and current, or using other established industrial communications protocols.
>
> *Long-range communications:* between local processors and host computers. This communication typically covers miles using methods such as leased phone lines, satellite, microwave, frame relay, and cellular packet data.
>
> *Host computers*: act as the central point of monitoring and control. The host computer is where a human operator can supervise the process, as well as receive alarms, review data, and exercise control.

Figure 1 displays a high-level overview of SCADA architecture, where the Remote Stations might be an Electric Substation, the SCADA network on one network segment, with other organization network on differing network segments. With advancements in the computing field, the integration of digital electronics devices play an important role in the manufacturing industry, wherein manufacturing plants utilize PLCs/RTUs to control the devices, and develop distributed and large complicated systems in which intelligent systems are part of the manufacturing control systems processes.

JOURNAL ARTICLES

The Efficacy and Challenges of SCAD
and Smart Grid Integration

Author(s):
Les Cardwell

Case Study: Applying Agile Software Methods to Systems Engineering

Author(s):
Matthew Kennedy

Software Protection Against Side Channel Analysis Through a Hardwar
Level Power Difference Eliminating Mask

Author(s):
Capt John R. Bochert

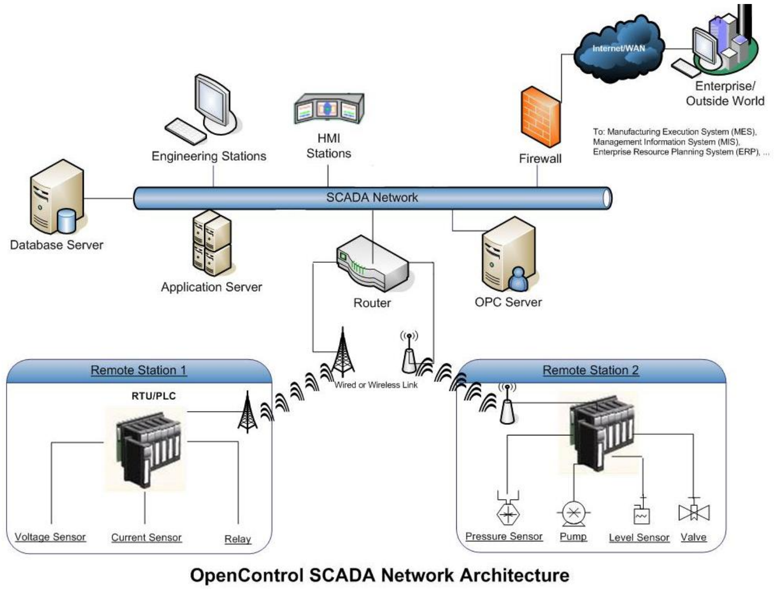


Figure 1: SCADA Network (Source: www.buraq.com)

“Most often, a SCADA system will monitor and make slight changes to function optimally; SCADA systems are considered closed loop systems and run with relatively little human intervention. One of the key processes of SCADA is the ability to monitor an entire system in real time. This is facilitated by data acquisitions including meter reading, checking statuses of sensors, etc. that are communicated at regular intervals depending on the system” (Abawajy & Robles, 2010).

Smart Grid

The Smart Grid domain is comprised of and concerned with distributed intelligence including data decentralization, distributed generation and storage, and distribution system automation and optimization. Customer involvement and interaction is a consideration, as are micro-grids, and high-consumption electric devices including plug- in hybrid electric vehicles (PHEV) (Collier, 2010).

The Smart Grid is by definition about real-time data and active grid management via fast two-way digital communications through the application of technological solutions to the electricity delivery infrastructure. Connectivity exists between (and within) the electric utility, utility’s devices, consumer devices (In Home Devices, or IHDs), and third-party entities either as vendors, consumers, or regulatory bodies. Smart Grid includes an intelligent monitoring system that tracks the flow of electricity throughout the electrical network, and incorporates the use of superconductive transmission lines to manage power fluctuations, loss, and co-generation integration from solar and wind.

At its most efficient, the Smart Grid can control in-home devices that are non-critical during peak power usage-times to reduce demand, and return their function during non-peak hours. Proposals for optimization include smart electric grid, smart power grid, intelligent grid (or intelligrid), Future Grid, and the more modern intergrid and intragrid. In addition to leveling (or normalizing) electric demand, the ability to manage consumption peaks can assist in avoiding brown-outs and black-outs when demand exceeds supply, and allow for maintaining critical systems and devices under such conditions (Clark & Pavloski, 2010).

Figure 2 displays a high-level communication flow between different components in a Smart Grid.

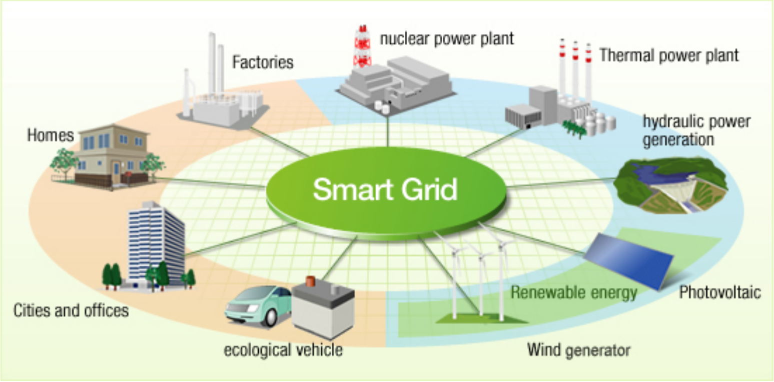


Figure 2: Smart Grid (Source: www.consoglobe.com)

The Smart Grid initiative has spawned a significant movement toward the modernization and evolution of the electric utility infrastructure, and aims to bring it into today's advanced communication age both in function and in architecture. That evolution brings with it a number of organizational, technical, socio-economic, and cyber security challenges. The breadth and depth of those challenges is not trivial, and a number of regulatory bodies have taken up the initiative to bring their own requirements into alignment with these new challenges. The initiative has also offered many opportunities for researchers, scientists, and enterprise architects to advance the state of security assurance; it also affords technologists the opportunity to explore new areas for exploiting means of data communication among distributed and remote networks and their devices.

Smart Grid / SCADA Integration

SCADA integration into the Smart Grid is not difficult, and connected by both electrical and data networks, allows for central and distributed aggregation of information and control over the entire utility electrical device network as depicted in Figure. 3.

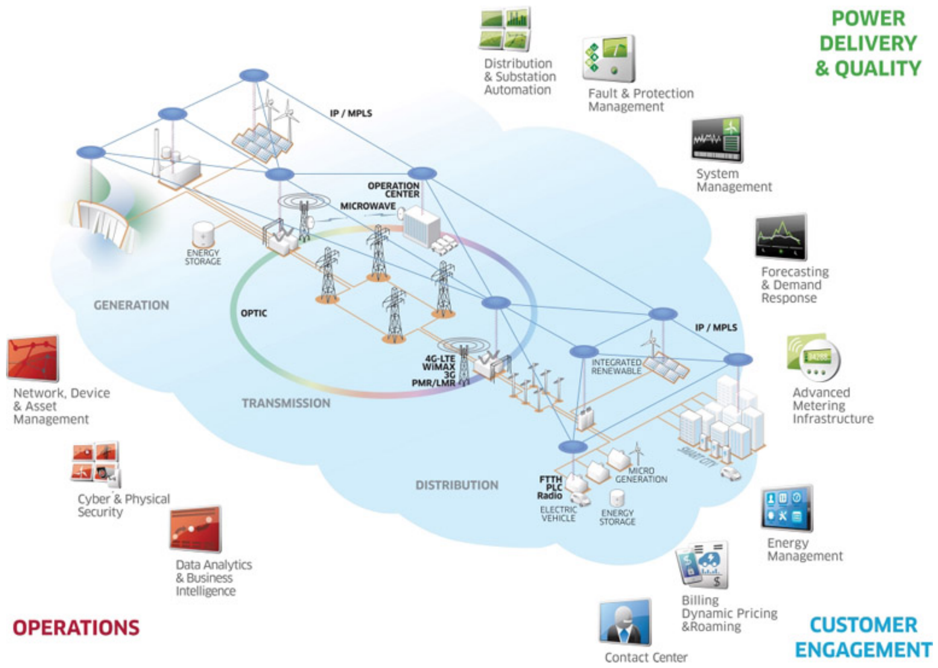


Figure 3: SCADA/Smart Grid Integration (Source: http://www2.alcatel-lucent.com)

SCADA empowers the consumer by interconnecting energy management systems to enable the customer to manage their own energy use and control costs. It allows the grid to be self-healing by instantly responding automatically to outages, power quality issues, and system problems. Properly configured, it is tolerant to attack—both physical and cyber-attacks—and optimizes the grid assets by monitoring and optimizing those assets while minimizing maintenance and operations costs. Further, it also enables competitive energy markets and mitigates the bloat often incurred in the effort to obtain pricing guarantees.

To adequately deliver and administer the products and services made possible by the Smart Grid, intelligence and control need to exist along the entire supply chain. This includes the generation and transmission of electricity from inception to delivery end-points at the customer's side of the meter, and includes both fixed and mobile devices in the architecture.

Digital communications on a Smart Grid occur over a variety of devices, technologies, and protocols that include wired and wireless telephone, voice and data dispatch radio, fiber optics, power line carriers, and satellite. Decision Control Software (DCS) allows for dynamic grid management that involves monitoring a significant number of control points. To be fully effective and operational, monitoring occurs for every power line and piece of equipment in the distribution system, in addition to allowing the customers to monitor and control their own devices and usage. This results in considerable volumes of data to be organized, analyzed, and used for both manual and automated decision software that comes in two basic categories: decentralized and back office.

Decentralized software is necessary due to the magnitude of the devices and data collection and computation, which precludes a centralized data collection solution. As the technology matures, intelligent electronic devices (IEDs) will evolve to mitigate the collection, organization, and data analysis necessary for performing data routing, decision making, and other actions that may be necessary based on the information received. This functionality exists either as part of the firmware, or via configurable functions and settings within each device.

Back office software is typically that software which is used as part of the utility's line-of-business (LOB) software solutions necessary to conduct the business of the organization. This typically includes, but is not limited to the following:

Accounting & Business Systems (ABSs)

- Customer Information Systems (CISs)
  - Customer Billing & Payment
  - Customer Relationship Management (CRM)
- Work & Workforce Management
  - Performance & Productivity Management
- Engineering & Operations (E&Os)
- Engineering Analysis
  - Circuit Modeling & Analysis
  - Reliability Analysis
- Real-Time Distribution Analysis
  - Outage Management System (OMS)
  - Active Distribution Grid Management
- Geographic Information Systems (GISs)
- Interactive Voice Response (IVR)

The net effect on these solutions by the deployment of IEDs and two-way digital communications is a more powerful, useful, and effective solution set for both the utility and the consumer.

SCADA and Smart Grid Security Considerations

Hentea (2008) discusses the evolution and security issue escalation of SCADA and the Smart Grid due in large part to the advent of the internet and rise in terrorist threats. Additionally, the introduction of new protocols, LAN/WAN architectures, and new technologies such as encryption and information assurance applications on the shared network(s) raise new sets of security concerns.

The increased functionality of SCADA and the Smart Grid architecture leads to control systems that are escalating in complexity and have become time critical, embedded, fault tolerant, distributed, intelligent, large, open sourced, and heterogeneous, all which pose their own program vulnerabilities. Ranked high on the list of government concerns are threats against SCADA systems. Unfortunately, mostly due to the complexities involved and resources required, the threats are too often trivialized and most organizations are slow to implement enhanced security measures to combat these threats. Key requirement areas for addressing these threats are critical path protection, strong safety policies, procedures, knowledge management, and system development skills that place security architecture at the forefront of requirements.

In considering potential risks in the act of collecting data from distributed access points using wireless radio frequency technology, “The very nature of Radio Frequency (RF) technology makes Wireless LANs (WLANs) open to a variety of unique attacks. Most of these RF-related attacks begin as exploits of Layer 1 (Physical – PHY) and Layer 2 (Media Access Control – MAC) of the 802.11 specification, and then build into a wide array of more advanced assaults, including Denial of Service (DOS) attacks. In Intelligent Jamming, the jammer jams physical layer of WLAN by generating continuous high power noise in the vicinity of wireless receiver nodes” (Jha, Kumar & Dalal, 2010).

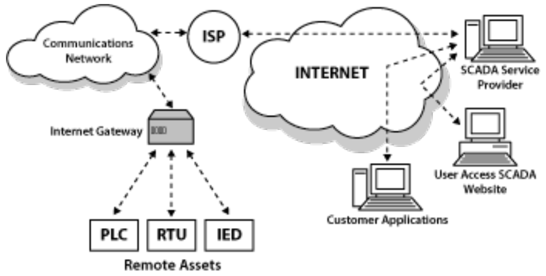


Figure 4: Internet and SCADA Systems Architecture (Source: Gervasi, 2010)

To combat some of these risks, Teixeira, Dán, Sandberg, and Johansson (2010) discuss the need for the use of litmus and metrics in the form of state estimators commonly used in power networks to detect problems and optimize power flows. These are usually located in central control centers and receive significant data measurements sent over unencrypted communication channels, making cyber security an important issue. Bad data detection (BDD) schemes exist as energy management systems (EMSs) state estimation algorithms to detect outliers and inconsistencies in the data, and are based on high measurement redundancy. While these methods may detect a basic cyber-attack, additional security considerations should be implemented to deter an intelligent attacker intent on gaining access and control of a SCADA system directly or through one of the Smart Grid devices.

Integration into the Internet Figure. 4 provides a delivery medium available to most consumers, and can provide advantages in the form of control, distribution, and communication. The Internet utilizes Hybrid fiber-cable (HFC), digital subscriber line (DSL), broadband over power lines (BPL), wireless (Wi-Fi and WiMAX), fiber, satellite, and utilizes wholly-owned and operated networks and third-party networks where feasible and cost effective.

SCADA also creates a number of additional security issues since the electrical power network is a critical infrastructure. Without Internet connectivity, SCADA already contends with security issues, and additional methods of penetration via the internet make it more vulnerable. There are a number of common security issues with SCADA:

- A lack of concern about security and authentication in the design, deployment, and operation of existing Control System networks
- The belief that SCADA systems have the benefit of security through obscurity, through the use of specialized protocols and proprietary interfaces
- The belief that SCADA networks are secure because they are purportedly physically secured
- The belief that SCADA networks are secure because they are supposedly disconnected from the Internet
- IP Performance Overhead of Control Systems connected to the Internet

Among the suggestions to further enhance SCADA and Internet security, Gervasi (2010) offers a "Crossed-Crypto Scheme" for securing communications. "There are major types of encryptions in cryptography: the symmetric encryption and the asymmetric encryption. From the two major types of encryptions we can say that Asymmetric encryption provides more functionality than symmetric encryption, at the expense of speed and hardware cost." The scheme integrates into the communication of the SCADA master and SCADA assets wherein the plain text data transmits using the AES algorithm for encryption, then encrypts the AES key using ECC. The cipher text of the message and the cipher text of the key are then sent to the SCADA assets, also encrypted using ECC techniques. "The cipher text of the message digest is decrypted using ECC technique to obtain the message digest sent by the SCADA Master. This value is compared with the computed message digest. If both of them are equal, the message is accepted; otherwise it is rejected."

Chauvenet and others also consider enhancements to the communication stack for power-line communication (PLC) based on and the adaption of the IEEE802.15.4 standard protocol, which is constrained by the low-power, lossy, and low data-rate context of power-line transceiver using pulse modulation, using open standards using IPv6 at the network level with the 6LoWPAN adaption (Chauvenet, Tourancheau, Genon-Catalot, Goudet, and Pouillot,2010). In their paper, they posit that "this allows for a full network layer stack and results in efficient routing in our low power, low data-rate and lossy network context" and cross compare their posit with other available communication solutions.

Other standards and maturity models are being developed to address the growing security concerns for the evolving energy distribution models (Fries, Hof, & Seewald, 2010) such as security enhancements to the IEC61850, which is a standardized communication services and standardized data model for communication in energy automation. Therein lies the challenge. The number of standards, recommendations, requirements, and frameworks that are evolving in the attempt to address the growing security challenges for securing SCADA and the Smart Grid is not trivial. Further, each utility, depending on the services the utility provides, are subject to many of these standards, each prescribing recommendations that are redundant across standards. Wading through multiple sources of these in an effort to be thorough is daunting, resource intensive, and a moving target that requires policies and procedures to ensure all recommendations are vetted against both existing assets and any new assets. Ensuring that the risks, many as unknown and potentially pervasive, are not trivialized and rationalized away is a challenge.

Security Integration Improvement – Addressing Cybersecurity Risks

A posit by Langner and Pederson (2013) suggests that putting emphasis on establishing frameworks for risk management, and relying on voluntary participation of the private sector that owns and operates the majority of US critical infrastructure are together a recipe for continued failure. The reason for this is the reliance on the concept of risk management framed as a problem in business logic, which ultimately allows the private sector to argue the hypothetical risk away. The authors suggest that a policy-based approach (vs. a risk-assessment based approach) that sets clear guidelines would avoid perpetuating the problem. They also argue the distinction between a critical and a non-critical systems only contradicts pervasiveness and sustainability of the effort in arriving at robust and well-protected systems.

As was recently asserted by Cardwell (2013) in response to the National Institute of Standards and Technology's (NIST) "RFI – Framework for Reducing Cyber Risks to Critical Infrastructure" driven by the recent Executive Order "Improving Critical Infrastructure Cybersecurity" (NIST, 2013), the "…issue is the 'expanding redundant complexity' of the current approach to the problem domain. While one can appreciate the efforts in gathering more information from the industry at large for establishing and improving frameworks to raise the overall level of cybersecurity across the utility industry, the problem is that it does not address the inherent complexity of the problem. It only exacerbates it by creating yet more administrative requirements for decomposing and resolving the problem domain for each utility."

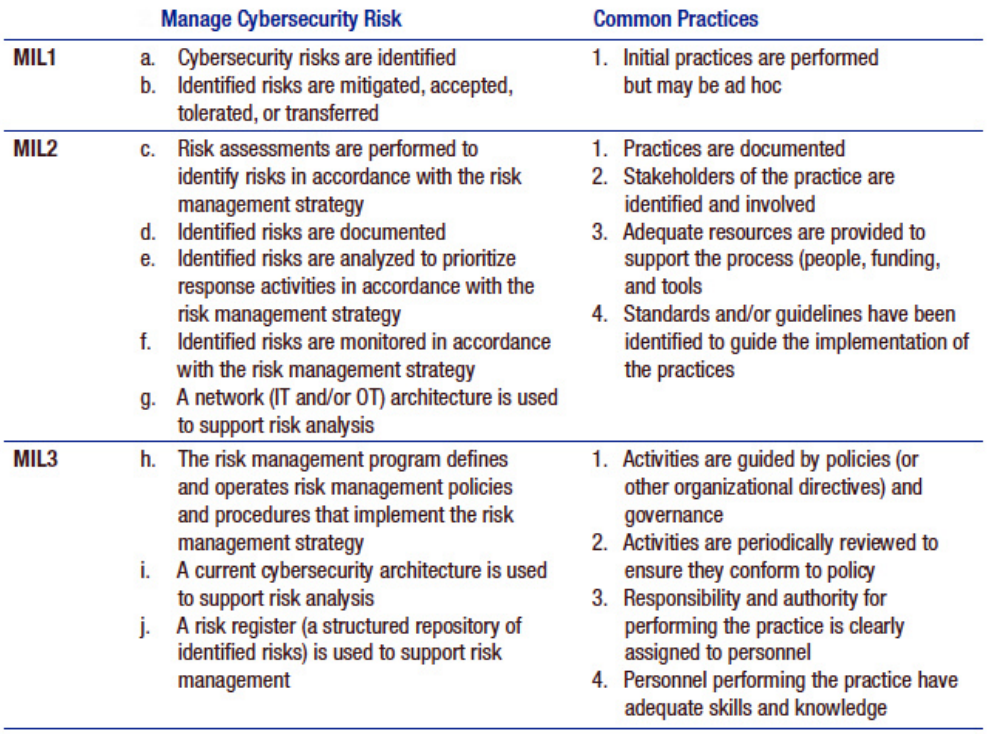
Rather than asking every utility to wade through every applicable (to that utility) standard, recommendation, and framework, the assertion suggests that a "single-source" methodology that eliminates redundancy across all frameworks be adopted and provided for addressing the complexity and achieving a Digital Systems Security (DSS) Cybersecurity standard across the US Utility spectrum. Using a single-source tool as litmus, the outcome is a reduction in administrative and redundant efforts otherwise required to manage the information between multiple systems, and serves as a living digital document of the DSS domain, thus simplifying the process further.

One such tool does currently exist: the Cyber Security Evaluation Tool (CSET) (DHS, 2011) by the Department of Homeland Security (DHS), although improvements are still being applied to improve its efficacy. Even with such an application, while the process is certainly not "easy" for any utility, it is relatively simple in comparison to wading through all the various requirements and recommendations, hoping to achieve a full decomposition of each. Simplifying the DSS Cybersecurity process in this fashion will save utilities —both individually and collectively—significant amounts of time, and resources, and could galvanize the DSS efforts for both the regulatory bodies and the utility industry combined.

While establishing such a tool as litmus for evaluating the level of DSS maturity for a given utility, some additional thought went into the subject using the Capability Maturity Model Integration (CMMI Institute, 2010) to assist utilities in that effort. That effort resulted in a modified CMMI model labeled as the Electricity Subsector Cybersecurity Capability Maturity Model (DHS, 2012).

Electricity Subsector Cybersecurity Capability Maturity Model

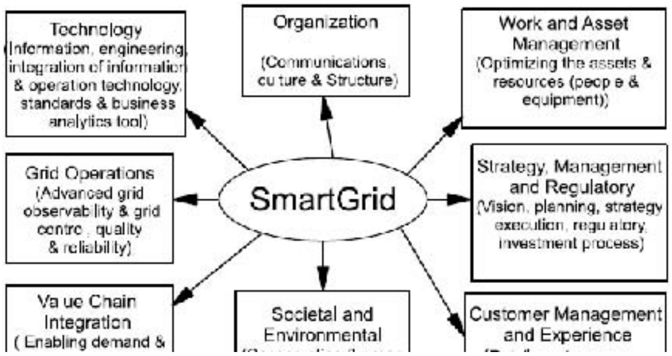
Efforts in establishing standard security practices that can be broadly applied and implemented for the electric utility industry can be found in the evolving "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), and is discussed by Balijepalli, Khaparde, Gupta, and Pradeep (2010) as a tool which "can guide the transformation of an entire power grid forward towards smarter grid. This will assess the utility grid state for moving towards the vision of Smart Grid. Some of the utilities are planning their Smart Grid road maps and investments using ES-C2M2. This helps to establish a shared picture of the Smart Grid journey, communicate the Smart Grid vision, and internally and externally assess current opportunities, choices, and desired levels. This also helps in the strategic and decision making framework to develop business, investment and rate cases, build an explicit plan to move from one level to another, measure progress using key performance indicators (KPIs), benchmark and learn from others." The ES-C2M2 parallels the CMMI model in form as follows, although the ES-C2M2 to date only measures through Level 3.



	Manage Cybersecurity Risk	Common Practices
MIL1	a. Cybersecurity risks are identified b. Identified risks are mitigated, accepted, tolerated, or transferred	1. Initial practices are performed but may be ad hoc
MIL2	c. Risk assessments are performed to identify risks in accordance with the risk management strategy d. Identified risks are documented e. Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy f. Identified risks are monitored in accordance with the risk management strategy g. A network (IT and/or OT) architecture is used to support risk analysis	1. Practices are documented 2. Stakeholders of the practice are identified and involved 3. Adequate resources are provided to support the process (people, funding, and tools 4. Standards and/or guidelines have been identified to guide the implementation of the practices
MIL3	h. The risk management program defines and operates risk management policies and procedures that implement the risk management strategy i. A current cybersecurity architecture is used to support risk analysis j. A risk register (a structured repository of identified risks) is used to support risk management	1. Activities are guided by policies (or other organizational directives) and governance 2. Activities are periodically reviewed to ensure they conform to policy 3. Responsibility and authority for performing the practice is clearly assigned to personnel 4. Personnel performing the practice have adequate skills and knowledge

Figure 5: ES-C2M2 Maturity Levels (Source: DHS, 2011)

There are eight domains of logical groupings with related capabilities and characteristics at each maturity level as shown in Figure 6. Maturity Levels are defined for each domain to assess the current state of a utility's overall maturity level.


Technology (Information, engineering, integration of information & operation technology, standards & business analytics tool)
Organization (Communications, culture & Structure)
Work and Asset Management (Optimizing the assets & resources (people & equipment))
Grid Operations (Advanced grid observability & grid control, quality & reliability)
SmartGrid
Strategy, Management and Regulatory (Vision, planning, strategy execution, regulatory, investment process)
Value Chain Integration (Enabling demand &
Societal and Environmental
Customer Management and Experience

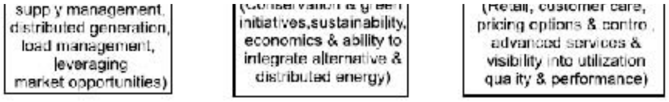

supp y management, distributed generation, load management, leveraging market opportunities)
(Conservation & green initiatives,sustainability, economics & ability to integrate alternative & distributed energy)
(Retail, customer care, pricing options & contro , advanced services & visibility into utilization qua ity & performance)

Figure 6: Eight-Domain Elements of Smart Grid - the Logical Grouping (Source: DHS, 2011)

It has been suggested by Cardwell (2013) that the ES-C2M2 be used as litmus for helping utilities achieve and maintain a Maturity Level 3 status, though it is currently used simply as a tool for a utility to assess their own status.

Conclusion

In this paper, we explored the Smart Grid initiative and described integration of SCADA systems into the Smart Grid, including an overview of the problem domain as a whole. We then showed that the outer bounds and limits of the security requirements are as yet not known, and until the architecture and its implementation are complete, repeatable, and mature, the “wicked complexity” of systems will exist due to the “unknown” aspects of cybersecurity. Also discussed are possible approaches for addressing the complexities in securing a utility’s cyber-structure, and some of the efforts that seek to address the security concerns and requirements of the initiative. While solutions are forthcoming, a pervasive industry-wide answer to the challenge is still evolving.

References

Abawajy, J., & Robles, R. J. (2010). Secured Communication Scheme for SCADA in Smart Grid Environment. *Journal of Security Engineering, 7*(6), 12.

Balijepalli, V. S. K. M., Khaparde, S., Gupta, R., & Pradeep, Y. (2010). *SmartGrid initiatives and power market in India*.

Cardwell, L. (2013, February 28). *Comments received in response to: Federal register notice developing a framework to improve critical infrastructure cybersecurity*. Retrieved on April 10 from http://csrc.nist.gov/cyberframework/rfi_comments/central_lincoln_pud_022...

Chauvenet, C., Tourancheau, B., Genon-Catalot, D., Goudet, P. E., & Pouillot, M. (2010). *A communication stack over PLC for multi physical layer IPv6 Networking*.

Clark, A., & Pavlovski, C. J. (2010). Wireless Networks for the Smart Energy Grid: Application Aware Networks. *Proceedings of the International MultiConference of Engineers and Computer Scientists, 2*.

CMMI Institute. (2010, November). Capability maturity model integration. Retrieved from http://cmmiinstitute.com/

Collier, S. E. (2010). Ten steps to a smarter grid. *Industry Applications Magazine, IEEE, 16*(2), 62-68.

DHS. (2011, January 24). Cyber security evaluation tool. Retrieved from http://ics-cert.us-cert.gov/satool.html

DHS. (2012, May 31). Electricity subsector cybersecurity capability maturity model. Retrieved from http://energy.gov/oe/services/cybersecurity/electricity-subsector-cybers...

Fries, S., Hof, H. J., & Seewald, M. (2010). *Enhancing IEC 62351 to Improve Security for Energy Automation in Smart Grid Environments*.

Gervasi, O. (2010). Encryption scheme for secured Communication of web based control systems. *Journal of Security Engineering, 7*(6), 12.

Hentea, M. (2008). Improving security for SCADA control systems. *Interdisciplinary Journal of Information, Knowledge, and Management, 3*, 73-86.

Jha, R. K., Kumar, R. A., & Dalal, U. D. *Performance Comparison of Intelligent Jamming in RF (Physical) Layer with WLAN Ethernet Router and WLAN Ethernet Bridge*. Paper presented at the Proceedings of the 2010 International Conference on Advances in Communication, Network, and Computing.

Langner, R., & Pederson, P. (2013). Bound to fail: Why cyber security risk cannot simply be “managed” away. Retrieved on April 10 from http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-im...

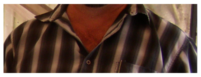
NIST. (2013, February 12). Cybersecurity framework. Retrieved from http://www.nist.gov/itl/cyberframework.cfm

Teixeira, A., Dán, G., Sandberg, H., & Johansson, K. H. (2010). A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator. *Arxiv preprint arXiv:1011.1828.*

Author(s)

Les Cardwell

Dr. Les Cardwell is an Enterprise Data Architect at Central Lincoln People’s Utility District on the Oregon Coast, one of the a recipients of the ARRA Smart Grid Grants. He re-



ceived his doctorate (DCS-DSS) from Colorado Technical University, and received both a MIT and BIT from American InterContinental University. Les is a subject matter expert (SME) for the DOE’s Electric Subsector Cybersecurity Capability Maturity Model (ES-C2M2), is a Certified Enterprise Architect (EACOE), and an evangelist for solving the Cybersecurity challenges through an Enterprise Architecture perspective. His experience spans 30 years improving ICT efficiencies, with a passion for reducing complexity to its simplest form.

Post new comment

Login or register to post comments

CSIAC on the Web

- Linkedin
- Twitter
- Vimeo
- Wikipedia

Contact Us

Phone:	800-214-7921
Fax:	315-351-4209
Email:	**info@csiac.org**
Address:	100 Seymour Road Suite C102 Utica, NY 13502

CSIAC Products & Services

FREE Technical Inquiry
Core Analysis Tasks (CATs)
Resources
Event Calendar
Submit an Event
FAQ's
CSIAC Store

About CSIAC

The CSIAC is a DoD-sponsored Center of Excellence in the fields of Cybersecurity, Information Assurance, Software Engineering, Modeling & Simulation, and Knowledge Management & Information Sharing ...[**more**]

For Best Browsing Experience:IE8 / Firefox 9.0+ / Chrome 10+, 1024x768+, 96 DPI