SANS ANALYST PROGRAM

Sponsored by NitroSecurity

Securing a Smarter Grid: Risk Management in Power Utility Networks

A SANS Whitepaper – October 2009

Written by Matt Luallen

Advisors:

***Paul A. Henry**, Certified SANS Instructor, industry veteran and published co-author of books on network security and SCADA*

***Gary J. Finco**, Senior Advisory Engineer, Idaho National Laboratory*

Executive Summary

Electricity provides the foundation on which all of society stands. It has come a long way from the early days, when Thomas Edison and George Westinghouse competed to gain support for their respective DC and AC technologies. Today's power grids circle the world, providing AC electricity to billions of people. And now these grids themselves are getting smarter, thanks to modern-day technologies supporting what were once decentralized pneumatic manual controls.

Transmissions over these networks involve human operators coupled with advanced computing systems to achieve an intricate balance between the production and consumption of electrons. Fuels such as wind, solar, coal, natural gas, hydro, and nuclear generate electrons that are transmitted long distances and distributed to residential, business, military/government, educational and every other operational community in a civilized society. These electrons provide power to heat, air conditioning, lights, televisions, refrigerators, and even the heart pumps attached to our dearest loved ones.

Each stage of this energy transmission cycle typically includes more than one automated control, or cyber asset. These cyber assets undeniably enhance safety and reliability of the grid network. The problem is, as the grid gets smarter, the propensity for successful cyber intrusion and disablement dramatically increases. These networks are no longer proprietary. They run on commercially-available hardware, operating systems, applications, code, and protocols the bad guys have been exploiting ever since the 1980s.

Consider, as well, the interconnectedness of these transmission networks. In order to buy, sell and transfer various forms of power, these networks must intrinsically connect along supply and distribution routes. For example, energy purchased by the Independent System Operator in Folsom, Calif., might actually come from an Idaho power company that's selling off excess energy at a discount. This means that security considerations do not end where the specific control network does: They continue on through partner connections. In all verticals, partner connections made up 32 percent of breaches investigated, according to the 2009 Verizon Business Breach Report.[1]

This paper will address the security issues facing smarter grid operators and will provide policy advice points.

[1] www.verizonbusiness.com/products/security/risk/databreach

Industry Landscape

Many countries are taking an active role in developing cyber asset security within power utilities. For example, the U.S., Canada and part of Mexico similarly interpret the North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) reliability standards.[2] Should utilities fail to meet implementation plan deadlines for these regulations,[3] penalties can reach up to $1 million daily per non-compliant requirement. This stringency is pushing awareness to the power utility industry worldwide.

Rigid compliance requirements may prove to be onerous, however, as these transmission control networks do not play nicely with typical corporate IT security mechanisms. Because of their complexity, many control system cyber assets, including PLCs (Programmable Logic Controllers), RTUs (Remote Telemetry Units), relays and other intelligent electronic devices (IEDs) are not able to meet the NERC CIP requirements. For example, some cyber asset controls outlined in NERC CIP-007 require compensating technical or procedural controls, such as limiting ports and services, implementing security patches, enabling anti-virus and malware protection, requiring password complexity, modifying/removing default accounts, and monitoring security status. Today's IEDs and control systems may have user accounts, ports and services that organizations cannot disable without harming operations. For the same reason, some of these control systems aren't even protected by anti-virus software or patched appropriately.

Several of the NERC CIP reliability standards allow entities to define alternate or compensating controls or Technical Feasibility Exceptions (TFEs). NERC is in the process of formalizing the procedure to allow entities to submit TFEs for cyber assets that cannot comply with the requirements set forth in its CIP reliability standards.

To bring these cyber assets under the risk management plan, consider the following strategies:

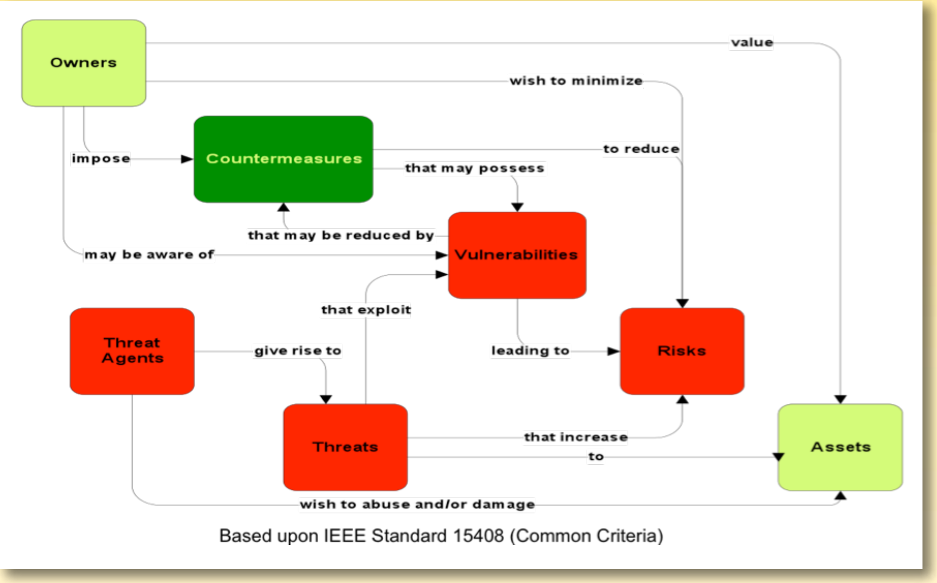
1. **Understand the risk** across all participants, particularly across interconnected supply and delivery partners.
2. **Know yourself and build walls.** Control networks must be well-understood, managed and changed, with limited interactions (e.g., one-way) with any system of less trust.
3. **Be aware and respond swiftly.** Personnel must have access to accurate situational awareness of cyber, physical and operational data so they can detect, isolate and respond appropriately to threats and infrastructure events.
4. **Sustain your security posture.** Ensure the ongoing integration of security activities across people, processes and technology.

[2] www.nerc.com/page.php?cid=2%7C20

[3] www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf

The Risk

Risk management is about discovering your critical assets and understanding their weaknesses, loss expectancy, and the appropriate risk mitigation tactics for ensuring their sustained value. The IEEE Standard 15408 (Common Criteria—Figure 1) includes a fact model depicting the value relationship of owners to their assets. Ultimately our challenge is to introduce countermeasures that restrict a threat agent from successfully exploiting a known threat against an asset's vulnerabilities.



Based upon IEEE Standard 15408 (Common Criteria)

Figure 1. Value Relationship of Owners to Their Assets

Discovering Cyber Assets, Their Capabilities and Weaknesses

Control networks typically are well-engineered and thoroughly documented. However, over time, hardware and systems are upgraded and replaced, personnel changes, and documentation becomes inaccurate. Therefore, ensuring proper cyber asset identification and functionality is paramount.

Asset identification typically involves a combination of documentation review, physical site inspections, configuration analysis, and personnel interviews. The goal is full discovery of all assets comprising the current control network architecture. This process must take into account the direct cyber assets providing critical functionality for the physical critical asset, as well as supporting assets within the system. These supporting assts include Heating, Venting and Air Conditioning (HVAC) systems, uninterruptible power supplies (UPS), physical security systems, and fire alarm and suppression systems. These supporting systems often are controlled via TCP/IP and run on common operating systems such as Linux and Microsoft Windows in varying degrees of update and patching.

After properly inventorying all cyber assets within the control network, the next step is identifying a cyber asset's functionality and criticality, as well as how cyber assets within the control network communicate with each other. For help, NERC and industry representatives created a draft document titled "Identifying Critical Cyber Assets."[4]

Performing Vulnerability Assessments

Traditional corporate IT vulnerability assessments employ commercial and open-source tools to analyze the cyber-security state of their systems and networks. Because these tools are not tuned for the control network environment, running them on a production network could do more harm than good. In order to avoid a self-imposed denial-of-service attack, these analysis tools should run against an emulated network test environment—not the actual systems. You might emulate the network using virtualization technology; however, you must ensure that the virtual system successfully represents the production environment with all its unpatched systems and services running. Organizations conducting manual reviews of Unix- or Windows-based systems can leverage command sets available in SANS Institute cheat sheets to identify potential vulnerabilities.

The following table describes several recently identified control system Cyber asset vulnerabilities.[5]

Vulnerable Cyber Asset	Description	Released
Energy Management System (EMS)	Multiple high-risk vulnerabilities identified in AREVA **e-terra***habitat*	February, 2009
Historian	OSIsoft PI Server authentication weakness[6]	September, 2009
Remote Telemetry Unit (RTU)	Bluetooth-accessible power pole RTU[7]	March, 2005
Advanced Metering Infrastructure (AMI) / Smart Meter	Idaho National Laboratory researches vulnerabilities associated with the smarter grid, specifically AMI and smart household devices.[8]	April, 2009
Programmable Logic Controller (PLC)	Omron PLCs are now remotely accessible via the Apple iPhone ScadaMobile application.[9]	Summer, 2009
OLE for Process Control (OPC)	MatrikonOPC dependency on Microsoft Windows Object Linking and Embedding (OLE).[10]	February, 2008

Continued on next page.

[4] www.nerc.com/docs/cip/sgwg/Critcal%20Cyber%20Asset%20ID%20V0%20R902%20for%20CIPC%20Review.pdf
[5] www.sans.org/resources/linsacheatsheet.pdf and www.sans.org/resources/winsacheatsheet.pdf
[6] http://seclists.org/bugtraq/2009/Sep/240
[7] www.nulec.com/pdfs/e2005-1.pdf
[8] www.inl.gov/scada/publications/d/securing_the_smart_grid_current_issues.pdf
[9] www.sweetwilliamautomation.com/
[10] http://blog.matrikonopc.com/index.php/opc-and-the-ole-automation-vulnerability/

Vulnerable Cyber Asset	Description	Released
Human Machine Interface	1. CitectSCADA buffer overflow.[11]	June, 2008
	2. Digital camera causes Indian Point power plant to shut down. [12]	March, 2008
Industrial Communications Hardware	1. Rockwell Automation ControlLogix 1756-ENBT/A bridge default settings. [13]	February, 2009
	2. ABB Process Communication Unit 400 stack overflow. [14]	September, 2008
All	Flooded communications network restricts communications of critical hardware across Ethernet network. [15]	August, 2006
All	Insider/partner risk: IT contractor does not receive permanent employment and turns on employer. [16]	Summer, 2008
Several (traditional corporate cyber assets)	1. Vulnerabilities associated with commercial applications and platforms (e.g. Linux, Unix, AIX, Windows, Cisco IOS).	1980s-present
	2. Undocumented changes to or addition of cyber assets or communications channels.	
	3. Unnecessary applications, default services and default, administrative and shared user accounts.	
	4. Multi-homed devices spanning the control and corporate networks.	

Table 1: Threats to Control System Cyber Assets

The real challenge comes in assessing current configurations for IEDs such as remote terminal units (RTUs), programmable logic controllers (PLCs), relays and other control network devices. The only way to understand how utility-specific devices like these have been configured and modified is to work closely with skilled cyber security professionals and the control system and IED vendors. In many situations, removing vulnerabilities requires system firmware or software updates. Before updating any system, manually validate that it hasn't been updated itself. For this, you can check its authenticity via integrity checks like SHA(2)-256 and authenticated vendor interaction.

Control system vulnerability assessments require highly specialized professionals. Sandia National Laboratory's "Guide to Critical Infrastructure Protection Cyber Vulnerability Assessment" can serve as a starting point.[17]

[11] www.kb.cert.org/vuls/id/476345
[12] DOE Operating Experiences, July 18, 2008 - www.hss.energy.gov/csa/analysis/oesummary/oesummary2008/OES_2008-06.pdf
[13] www.nerc.com/fileUploads/File/Events%20Analysis/A-2009-02-13-01.pdf
[14] www.kb.cert.org/vuls/id/343971
[15] www.nrc.gov/reading-rm/doc-collections/gen-comm/info-notices/2007/in200715.pdf
[16] www.networkworld.com/news/2009/092309-contractor-pleads-guilty-to-scada.html
[17] www.oe.energy.gov/DocumentsandMedia/26-CIP_CyberAssessmentGuide.pdf

Build Walls and Know Yourself

Ensuring appropriate risk mitigation across numerous vulnerabilities and threat vectors requires systematic layering of security controls. These controls range from typical corporate IT solutions—network firewalls, user account management, anti-virus and/or application whitelisting, and system event analysis—to more unconventional solutions such as:

- Unique, operator-monitored Distributed Control System/ Supervisory Control and Data Acquisition (DCS/SCADA) monitoring and control points,
- Deterministic communications monitoring and filtering, and
- Uniquely-defined interactions among primary and compensating controls.

Build Enclaves

To limit the success of man-in-the-middle attacks, define strong electronic security perimeters (ESPs), and baseline cyber asset configurations and appropriate information flows within them. Two excellent resources are NIST's Special Publication 800-82 v2,[18] Industrial Control Systems Security (soon to update to version 3), and the Department of Homeland Security's "Cyber Security Procurement Language for Control Systems."[19]

An ESP serves as the boundary between critical and non-critical cyber assets. In addition, this boundary often serves as the electronic egress point for data flow to remote systems as well as external interactive access for remote support. ESPs must be well defined, maintained and documented similar to the U.S. Department of Defense's definition of a security enclave. A security enclave, as defined in DoD Directive 8500.1 E2.1.16.2, is:

> *"… the collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the automated information system (AIS) applications or outsourced IT-based processes they support, and derive their security needs from those systems."*

Ultimately an enclave operates as a trusted collection of cyber assets that requires a model of mutual distrust for any and all interactions outside of the enclave. Once you've established the enclave, preventing intrusion becomes easier.

[18] http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-82
[19] www.us-cert.gov/control_systems/pdf/SCADA_Procurement_DHS_Final_to_Issue_08-19-08.pdf

Know the Flow

Organizations also must understand the bi-directional information flow between cyber assets, especially in cases where user interaction and partner connectivity conjoin. On the control network, this includes the data flow for operations such as Inter-Control Center Communications Protocol (ICCP), Automatic Generation Control (AGC), and Phasor (energy wave) Concentrator Units (PCUs). Understanding other flows, such as user interaction and authentication into a control network interface, or a partner connection, also is important. This means knowing how transactions flow to and from every edge point in the network and to each internal system with authorized access.

Organizations should architect information flow based on application requirement. For example, if an application enables an executive to view data about an asset's operational status, then it calls for a physically limited, one-way view only data flow. Another way of controlling information flow is to provide remote state estimation and control capabilities via ICCP. In this instance, establish a dedicated physical communication pathway with logical firewall partitions and set application thresholds. Some additional examples (see Figure 2) of ESP boundaries/enclaves include:

1. **Executive dashboard:** One-way fiber optic communications using Waterfall Technology agents or similar tool for data replication.
2. **SSL- or IPsec-protected ICCP:** Users are authenticated and data encrypted and its integrity validated.
3. **AGC:** Dedicated pathway with application thresholds.
4. **Application proxies** for static communication pathways.
5. **Jump hosts**/isolation stations for remote support.
6. **Cyber security monitoring.**
7. **Physical security monitoring.**
8. **Authentication and identity management systems.**
9. **Operational data repository.**
10. **Backup data repository.**
11. **Test systems and networks.**

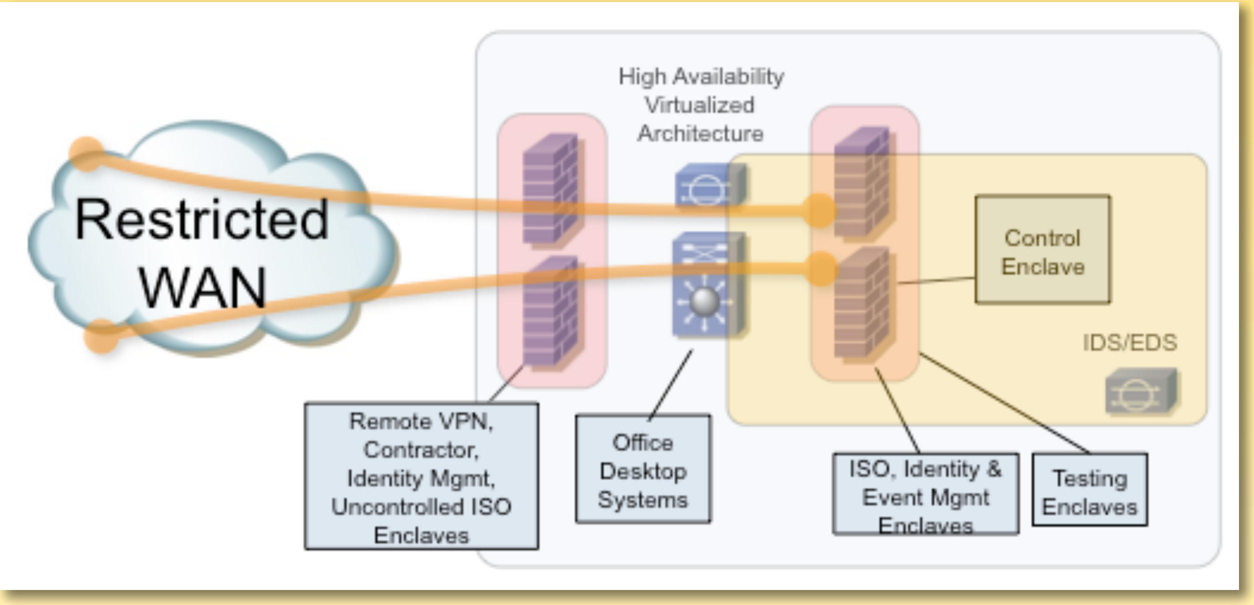

Restricted WAN
High Availability Virtualized Architecture
Control Enclave
IDS/EDS
Remote VPN, Contractor, Identity Mgmt, Uncontrolled ISO Enclaves
Office Desktop Systems
ISO, Identity & Event Mgmt Enclaves
Testing Enclaves

Figure 2: Flow Architecture Control Points

Ultimately, utility companies need to architect security perimeters into physical building and access controls. As they develop security policies, utility companies also will need to consider response mechanisms to pre-determined indicators of trouble. For instance, the ability to physically disconnect a cable—and thereby remove Internet access for the control network—would be invaluable during a threat event. Likewise for the ability to remove a corporate network connection should an internal threat arise. This would not affect connections to secondary control centers or regional authorities requiring a view or control capabilities of current operations.

Develop Baselines

System baselines are necessary for a number of purposes, including change detection, troubleshooting and forensics. An organization must routinely compare a cyber asset against its baseline and analyze system changes. The baseline automated or manual script depends on the individual control system vendor or typical operating systems. For examples of information required for profiling specific hardware types, see below:

End Host Configuration and Activity Analysis (Windows)

- **Local Audit Policy**
  - auditpol
- **Network Settings**
  - ipconfig
- **Listening Service Ports**
  - netstat
- **Environmental Settings**
  - set
- **Registry Settings**
  - regdmp
- **NTFS DACLs**
  - showacls
- **IIS Metabase**
  - cscript metaback
- **User Accounts and Group Memberships**
  - addusers
- **Shared Folders and Byte Counts**
  - diruse
- **Active Processes and System Drivers**
  - wmic
- **Service Settings**
  - net / sc

End Host Configuration and Activity Analysis (*nix)

- **Network Settings**
  - /etc/sysconfig/network
- **Listening Service Ports**
  - Netstat; ntop
- **Environmental Settings**
  - env
- **Configuration Values**
  - Varied locations dependent upon applications installed (/etc; /opt)
- **FS DACLs (SUID/SGID)**
  - Find -perm -4000
  - Find -perm -2000
- **Drivers**
  - /dev
- **User Accounts and Group Memberships**
  - /etc/group; /etc/passwd and associated shadows
- **Folders and Byte Counts**
  - ls
- **Running Processes**
  - lsof / ps; top
- **Run Level Settings**
  - Chkconfig – list

Monitor Everything

Once an organization has established information flows, it's important to deploy an intrusion detection system (IDS) tuned to detect power industry-specific attack signatures. For example, the system should be highly sensitive to alerting upon unapproved information flows within the control network. Along with looking for the attack signatures and behavior algorithms unique to power grids, the IDS should work in conjunction with vulnerability management and a security information event management (SIEM) platform to aggregate and correlate data from across multiple applications and security controls.

Because control networks are running over commercial protocols and systems, they require hardening against thousands of vulnerabilities and uncountable number of exploits. The Idaho National Laboratory and other entities have identified the man-in-the-middle attack as a primary concern for smarter grid operations. Man-in-the-middle occurs when a "hijacker" interrupts the flow or takes over the flow channel itself. The following table depicts several examples of man-in-the-middle attacks that could apply to IP-enabled SCADA systems.

Vector	Threat	Control
OSI Physical	Physically become in line to the data communication stream with a wiretap.	Six wall border and emissions shielded network cable.
	Wireless interception, transmission and alteration of emissions.	Physically limited unidirectional data flow. Monitor physical link endpoint connectivity. Tempest shielding (Faraday cage).[20]
	Physical cable cut, RF interference.	Redundant and media-independent physical connectivity.
	Gain access to storage media.	Protect data at rest with cryptography.
OSI Datalink	MAC address spoofing.	Enable port security properly and MAC address protection.
	Elect to become the spanning tree protocol (STP) root bridge.	Enable STP root bridge and BPDU protection.
	Enable an unauthorized DHCP server.	Enable DHCP/ARP snooping.
	Enable VLAN trunking using the Dynamic Trunking Protocol (DTP).	Disable DTP.
OSI Network	Inject blackhole or incorrect routing table information.	Use static routes or mutually authenticated routing updates.
	Source route IP packets.	Disable IP source routing.
	Inject arbitrary sources, forged and spoofed IP packets.	Perform IETF RFC 1918/2827 ingress and egress filtering. Filter BOGON and geopolitical IP addresses. Use IPsec-protected payloads with ESP/AHP (S-ICCP)
Application	DNS cache poisoning.	Split DNS within enclaves. Static host tables.
	Data spoofing.	RSA signatures with or without digital certificates; integrity validation.

Table 2: Man-in-the-Middle Attack Matrix

To prevent against man-in-the-middle and other attacks, limit centralized dependencies or common mode failures within the control network and properly authenticate for trusted communications. For more information and to comment on the current draft standard for the next-generation grid's cyber assets, review the NIST's "Smart Grid Cyber Security Strategy and Requirements."[21]

[20] http://en.wikipedia.org/wiki/Faraday_cage

[21] csrc.nist.gov/publications/PubsDrafts.html#NIST-IR-7628

Awareness and Response

One of your greatest challenges is to make sure employees and executives are acutely aware of the potential security implications of any action they take, from badge-point entry to each control interface interaction to their use of everyday business applications. The aging workforce must ensure that new engineers and IT professionals understand how the systems operate in both automatic and manual modes. Essentially, industry needs to create cyber archaeologists for critical infrastructures in general, and for power utilities in specific.

To embed cyber safety practices into the employee mindset, make sure your policies resonate with the utility staffs' daily duties. If not, employees may view the training as frivolous and fail to apply cyber safety practices. For example:

- Field technicians need to understand the importance of protecting sensitive engineering schematics, as well as the appropriate procedures to upgrade field equipment software and configurations with support from centrally-managed/guided IT. They also must understand the importance of properly securing, monitoring, encrypting and password-protecting field equipment (including controls on smart phones).
- Generation control system operators need to be aware of applicable cyber threats so you can maintain the trustworthiness of the operational data of locally controlled IEDs.
- Executives and management must understand the full landscape of risk throughout entire architecture.
- Customers and the general populous need to be aware of what to do in the event of an outage or other event, as prescribed by www.Ready.gov.

Importantly, organizations need to back up this education with a system that can monitor behavior and notify on violations. In addition, every organization must establish an emergency response team that can react to situations and can even cross coordinate with other critical infrastructure sectors in case of an infrastructure event. This calls for planning and identifying emergency response parties, and preparedness training across vectors.

Response

Should a cyber security event occur, your goal is to react appropriately and quickly to limit exposure. So energy companies need to tune their security to be aware of the current state of vulnerabilities, threats and threat agents to their cyber assets. For example, shortly after an external party alerts the utility company to a new threat, corporate IT identifies inbound attacks to the ESP, the control network operator sees a failed login attempt, and later a breaker closes. Being able to coordinate information about events taking place across physical, cyber and operational domains provides invaluable insight to whether or not the utility faces a malicious attack. In this case, a coordinated SIEM program, tuned to the devices, applications and flows represented in a utility environment, can help.

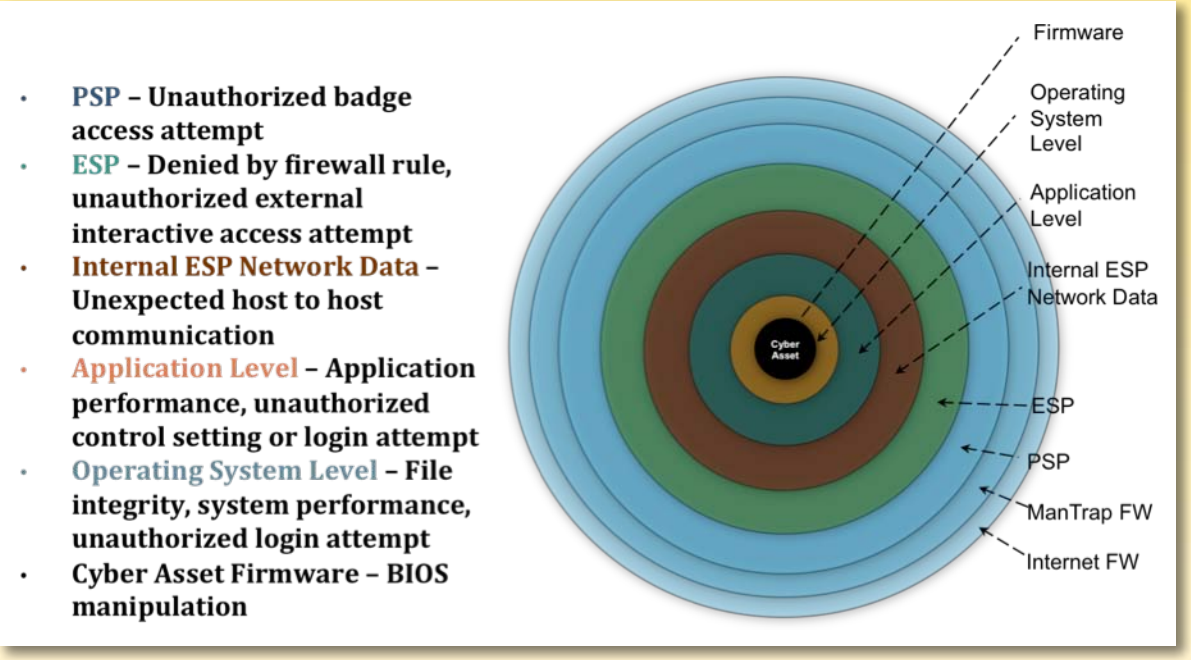
The SIEM system should be able to monitor and correlate events from a variety of cyber assets, their operating systems and associated applications, as well as from other security devices, such as network and end point IDS and firewalls. This also would aid in compliance with NERC CIP-005, R3 and CIP-007, R6. Such a system must properly notify assigned personnel in the event of an actual detected incident. This requires correlation and normalization tuned to the environments at control centers, substations and generating plants.

Specifically within power utilities, SIEM systems should be able to:

- Correlate cyber, operational and physical security events within generation control centers and substations. In many situations, providing individuals with unique user accounts can be difficult or technically infeasible, so correlated cyber and physical events help provide accountability.
- Alarm by default upon vendor-specific IED and control system security events.
- Check for compliancy with industry regulations such as NERC CIP.

Furthermore, if a response is mandated, authorization for that response is required. This part involves a human—two, actually—to keep in rotation. Ensure that at least two cyber security professionals have authorization to modify the operating state of a generating plant, substation or control center based on current threat indicators and known vulnerabilities within the control network's cyber assets. The cyber security professionals need the authority to move, impede or disable operations based on the detected incident. Insuring against abuse of this privilege requires careful coordination between the SIEM and access control systems.

Figure 3 depicts several layered security controls an organization can use to trigger and correlate events in a control network. For example, a detected scan of control network system ports (e.g. DNP/IP using TCP Port 2000 or Modbus/IP using TCP 502) at the Internet firewall may not impede or require a modification of operations at the control network, but may warrant additional monitoring at inner layers. However, events occurring at the man-trap firewall or, closer yet, at the ESP are of higher concern and warrant professional review. For more information, see NIST SP 800-61.



- **PSP – Unauthorized badge access attempt**
- **ESP – Denied by firewall rule, unauthorized external interactive access attempt**
- **Internal ESP Network Data – Unexpected host to host communication**
- **Application Level – Application performance, unauthorized control setting or login attempt**
- **Operating System Level – File integrity, system performance, unauthorized login attempt**
- **Cyber Asset Firmware – BIOS manipulation**

Figure 3: Layered Protection/Correlation

Conclusion: A Sustainable Model

In today's heightened state of terrorist threat, power utility security is more critical than ever. Yet, power utility security and assessment needs are different from most other critical infrastructure sectors, even though some of the protocols and systems our power runs through are no longer proprietary. We cannot just simply upgrade to Power Grid version 2 or Power Utility control system version 2. These systems take years to introduce technically, and considerably more time to educate support personnel.

What you can do now:

- Continue to educate each about control network cyber assets.
- Identify critical cyber assets, and their interrelatedness with cyber and physical security weaknesses.
- Build strong ESPs.
- Limit and monitor intra-ESP communications.
- Enable situational awareness tools for event detection.

In the case of an event, appropriate reporting and remediation are critical, as well. Policies should identify responders and even prepare for the worst by practicing emergency preparedness scenarios that involve multi-tiered cyber and physical attacks. Such tests are required on an on-going basis and necessitate a cultural shift to sustaining your organization's security program.

As Mark Twain once said, "History does not repeat itself, it rhymes."[22] The power industry needs to design the proper security controls into the nation's smart grids before making them even more intelligent and interconnected over public clouds.

[22] http://en.wikiquote.org/wiki/Mark_Twain

About the Author

Matthew E. Luallen is co-founder of Encari, a critical infrastructure information security consulting company. He is a well-respected information security professional, researcher, instructor and author who has written, consulted and trained extensively for several critical infrastructures containing typical corporate Cyber assets as well as industrial control systems security issues. Recently in the United States for NERC CIP, he performed gap analyses and developed and implemented remediation strategies across all of the NERC CIP reliability standards and a wide variety of critical cyber assets. Prior to incorporating Encari, Mr. Luallen provided strategic guidance for Argonne National Laboratory, U.S. Department of Energy, within the Information Architecture and Cyber Security Program Office. Mr. Luallen also serves as adjunct faculty for DePaul University, as a CCIE and certified instructor for Cisco Systems, and as a certified instructor for the SANS Institute.

SANS would like to thank this paper’s sponsor:

nitrosecurity