Technology Security Assessment for Capabilities and Applicability in Energy Sector Industrial Control Systems:

McAfee®
Application Control
Change Control
Integrity Control

Philip A Craig Jr
Thomas P McKenna Jr

March 2012
DISCLAIMER

Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.
Technology Security Assessment for Capabilities and Applicability in Energy Sector Industrial Control Systems:

**McAfee®**
Application Control
Change Control
Integrity Control

**Authors:**

Philip A Craig Jr
Thomas P McKenna Jr

March 2012

Prepared for
**McAfee®, Inc.**
Under a Related Services Agreement
With the U.S. Department of Energy
Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99352
Preface

There are many applicable and effective features of the McAfee® product suite included in this technical security assessment. Through the engagement with the McAfee® management and technical teams we fully recognize that McAfee® is committed to provide significant improvements for cyber security capabilities that will enable energy sector owners and operators to provide highly defensible security postures for their control system environments. Highlighting where legacy and next generation security opportunities await, vendors such as McAfee® are incumbent to provide security solutions that are effective and can be dynamically upgradable in response to a very active and capable advanced persistent threat environment. As our assessment indicates, our energy domain engineers and computational sciences experts conclude that McAfee® can provide many critical answers to confidentiality, integrity, and availability concerns that are currently shattering cyber security postures throughout critical infrastructure. Outdated security methods that use a maze of disparate, multi-vendor bolted-on, and stacked security tools will only delay an attack while providing multiple opportunities for a modern cyber adversary to attack this fragmented security posture. The McAfee® approach of total security Solidification™ provides new paradigms for defense-in-depth where a highly integrated suite of capabilities can overwhelm today’s cyber adversary by enabling security experts with a tightly integrated and effective solution.

Many thanks to the tireless efforts and air miles of those committed to secure our nations digital infrastructure. A special thank you to Mr. Todd Gebhart (Co-President, McAfee®) who openly shares his vision of value needed to deliver high-impact products specifically adapted to critical infrastructure, to Dr. Phyllis Schneck (Vice-President & Chief Technology Officer, Global Public Sector) who continually enables partnerships across public-private entities that share the battle against cyber-threats on a daily basis. And, with our sincere gratitude, to the management and technical experts at McAfee® and Pacific Northwest National Laboratory that work diligently to provide world-class security innovations into our ever-evolving digital world.

Philip A Craig Jr
Senior Cyber Security Research Scientist
National Security Directorate
Control Systems and Critical Infrastructure
Pacific Northwest National Laboratory

Thomas P McKenna Jr
Senior Project Manager
Fundamental Computing and Sciences Directorate
High Performance Computing
Pacific Northwest National Laboratory
Executive Summary

The Pacific Northwest National Laboratory (PNNL) and its’ energy security technical subject matter experts were commissioned by McAfee® to provide assessments of selected technologies. PNNL provides cyber security research activities that determine the applicability and effectiveness of cyber technologies for use in industrial control system (ICS) environments for many commercial partners. These environments range across the Department of Homeland Security (DHS) multi-sector defined critical infrastructure and key resource (CI/KR) domains as well as the significant CI/KR for the Department of Energy electricity delivery and oil and gas sectors. The grand challenge for CI/KR sector owners and operators is “how” they secure ICS devices and systems that are used in the automated processes and controls within their governance and technical domains. There are particular cyber security management, operational, and technical controls that have been well crafted into governance and oversight expectations that asset owners unilaterally struggle to implement with measurable effectiveness. With the implementation of the Application Control, Change Control, and Integrity Control product suite McAfee® intends to provide a strong commitment and vision in this space and maintains a technology roadmap enabling both current and future cyber security solutions for CI/KR. To challenge and improve the McAfee® approach, PNNL provided an in-depth cyber security assessment of these technologies that evaluated claims and capabilities related to control system components, environments, and functionality that is utilized throughout the DHS multi-sector domain and specifically within the energy sector. As the sector specific agency (SSA) for the energy sector, the U.S. Department of Energy has specific cyber security objectives for protecting critical energy environments (including the bulk electric grid, and oil & gas resources). The outcome of this assessment is intended to enable vendors to evaluate and improve highly effective solutions to industry that will enable them to structure protective measures that will provide more impactful and effective solutions while realizing such investments must be carefully weighed to ensure long-term value. We sincerely hope that the results favor furthering work of this nature that will execute functional testing to prove effectiveness and provide successful outcomes that will serve to better protect critical infrastructure worldwide.

PNNL has explored the McAfee® technology roadmaps and strategic vision that represents an inclusive set of security technologies and solutions intended to target the cyber security barriers such as those identified in the DOE-OE ieRoadmap. The programmatic approach that the energy industry has created that is represented in the ieRoadmap is highly matched to the cyber security acquisitions and solutions assembled by McAfee®. The assessment results were presented from the perspectives of policy & governance, technology, threat landscapes, implementation scenarios, and vulnerability identification and mitigation discussions. In each area PNNL found the applicability of the Solidification™ process to have plausible impacts on the ICS and SCADA platforms as well as a high potential for solving significant
process integrity security challenges on distributed devices. In addition, the national laboratories, and private cyber security researchers have published documents related to common vulnerabilities in critical infrastructure. These vulnerabilities remain valid concerns to control systems environments that have all leveraged a wide range of information technologies to enable functionality and convenience. As such, the “Top 10 Vulnerabilities Of Control Systems And Their Associated Mitigations” 2006¹ as publishd by the Department of Energy’s National SCADA Test Bed Program is a very relevant set of criterion that is constantly and currently evaluated during assessments and audits of CI/KR. The McAfee® technology assessed in this report provides a significant paradigm to classic information technology cyber security approaches by providing a new vertical penetration of application, change, and integrity controls that can be embedded, built-in, or layered within ICS process control software, hardware, and even down to single-purposed endpoint devices. As an enterprise solution PNNL found many new and effective opportunities for these cyber security paradigms that should allow McAfee® to proceed with confidence as they continue to integrate and offer deployments of these solutions to CI/KR owners and operators.

Background and Project Objective

McAfee® realizes the positive impacts that a convergence of both development and strategic deployment roadmaps will provide future cyber security postures within energy infrastructure. Together, the Pacific Northwest National Laboratory and McAfee® will continue to challenge the cyber security threat landscape by diligently assessing the applicability, value, and effectiveness of the security solutions necessary to support the national security mission to secure critical energy resources.

The Department of Energy’s key objective to secure the critical infrastructure and key resources (CI/KR) includes our Nation’s electric generation, transmission, distribution resources, as well as key oil and natural gas assets. Through Battelle’s partnerships, the Pacific Northwest National Laboratory seeks to continue to improve the value of security technologies as they are implemented in these CI/KR areas. Strategic partnerships are of high importance to those that supply our energy needs. Key relationships with McAfee®, Inc. have provided a strong interface to the resources available at the Pacific Northwest National Laboratory for public/private collaboration. Early McAfee® acquisitions of security technologies, such as the Secure Elements’ Sidewinder™ Firewall and subsequent assessment activities are allowing open and effective collaboration between the National Laboratories, vendors, and industry that are addressing rapidly emerging cyber security requirements.

The DOE’s Office of Electricity Delivery and Energy Reliability (DOE-OE)² in 2006 initiated the Roadmap to Secure Control Systems in the Energy Sector. It marks a continued effort by public and private stakeholders to identify steps for resilient energy delivery systems in the electric, oil, and natural gas industries. In 2011, an effort provided by Energy Sector Control Systems Working Group (ESCSWG)³, allowed industry stakeholders to provide some necessary updates to this roadmap in order to address a constantly evolving cyber security threat environment. Security solutions provided by security vendors such as McAfee®, allow industry stakeholders to leverage their published roadmap plan while adding long-term programmatic value supported by the DOE-OE. McAfee® also considers the use of technology development roadmaps of high programmatic value to steer investment decisions that match industry needs. Matching roadmaps will allow a more tightly integrated response to cyber threats of today and in the future. This project will provide an independent assessment of the McAfee® Application Control (MAC), Change Control, and Solidification™ (SolidCore⁴) solutions that are understood to be a comprehensive approach that utilizes dynamic white listing, memory protection, and image comparison, file integrity monitoring, and read and write security principles. This approach is augmented by a through integration into the centralized McAfee® ePO enterprise security management platform. This provides an enterprise-based wide-area management tool capable of full command and

---

³ https://www.controlsystemsroadmap.net/aboutus/Pages/Working-Group.aspx
⁴ SolidCore has transitioned to McAfee® Integrity Control (MIC)
control responses, as well as auditing and reporting functionality intended to add a much higher level of integration of these tools over the entire enterprise cyber security posture.

PNNL will focus on assessing the features and functions of the MAC solution using the technical domain experience of subject matter experts and their professional positions as to the potential effectiveness of the McAfee® solution with specific regard to energy infrastructure systems and networks. The SME’s will also exercise a feature mapping of how the McAfee® MAC solution addresses specific industry governance and requirements (specifically NERC Critical Infrastructure Protection – CIP guidelines and requirements, and related NIST IR 7628 Guidelines for Smart Grid Security). Lastly, PNNL will provide use-cases that describe the potential value of strategic deployment within ICS sample environments describing opportunities for effective deployment.
1 The Future Power Grid

PNNL is known as a leader in providing power grid solutions related to the challenges of efficiency, reliability, and resilience of the bulk power system or more commonly referred to as the “power grid”. As such, we have invested in a significant effort to ensure that power grid modernization efforts are researched and tested on very large scales. Our industry advisors supply endless value to the process through their specific energy domain expertise. The PNNL Future Power Grid Initiative (FPGI) will deliver next-generation concepts and tools for grid operation and planning and ensure a more secure, efficient and reliable future grid. Building on our Electricity Infrastructure Operations Center (EIOC), the Pacific Northwest National Laboratory’s (PNNL) national electric grid research facility, FPGI will advance the science and develop the technologies necessary for meeting the nation’s expectations for a highly reliable and efficient electric grid, reducing carbon emissions and our dependence on foreign oil.

We anticipate that our research will allow operators to see grid performance in near real time across a wide service area and under emerging contingency situations. Planners will have the ability to view configurations of the grid and adjust those options against national goals and performance objective. In doing so, our approach is to combine PNNL’s distinctive capabilities in power systems, data intensive computing, high performance computing, and visual analytics to address the complex problems from real-time and large-scale challenges in three Focus areas: Networking and Data Management; Modeling, Simulation, and Analysis; and Visualization and Decision Support.

The future power grid is expected to deploy 100 million smart sensors and meters with various data transfer speeds. The resulting data volume can be at peta scale \(10^{15}\) over a one-year time period. Power grid planners and policy makers need to have tools to quickly retrieve and analyze these volumes of data to make real-time decisions. With the anticipated advancements, the Initiative’s core product is GridOPTICS™ – Grid Operation and Planning Technology Integrated Capabilities Suite, a tool suite that is able to securely collect data in real time, use data to drive modeling and simulation, and convert large volumes of data to actionable information. These concepts and tools will show and analyze grid performance at an unprecedented speed, scale, and resolution and will support operational and policy decision making for the grid of the future.
These, and many more innovative approaches, will shape power generation, transmission, distribution, and consumption in ways that require highly integrated and interoperable systems, devices, and data. Methods to secure these environments need to be better utilized today, and more effective tomorrow. These advancements won’t come at costs network security, application stability, and interoperability. A total data explosion augmented by new high performance computing requirements, data locality (while at rest and in motion), and significant integration challenges will create many new cyber security requirements.

Future Grid (by the number):
- 10-100 millions measurement & communication devices across entire infrastructure
- $10^6$ times more data (petabytes/year) with subsecond speed from two-way communication across entire interconnections (Distribution to Transmission)
- >15%, high penetration of renewable generation (centralized & distributed)
- >15% demand response, + energy efficient loads, PHEV, distributed generation
- Multiple technologies exist, potentially leading to vastly different future grid scenarios and energy policies beyond 2050

Our Vision for Future Grid Operation and Planning
- View and analyze grid performance at an unprecedented speed, scale, and resolution
- Increase grid reliability and security
- Accommodate complexity
- Enable market transformation
- Enable policy assessment with integrated modeling and analysis
2 Cyber Security and the Electric Power Grid

As information and communication technology advances, this technology is being integrated into power system operations and planning functions, yielding greater visibility into the state of the system and advancements in control to enhance system efficiency and maintain high levels of reliability. Supervisory Control and Data Acquisition (SCADA) systems are now prevalent throughout the nation’s transmission system and cover a significant portion of the distribution system as well. SCADA systems and their associated field monitoring and control equipment provide transmission and distribution operators with a real-time view of the operating state of the system, warn them of system events or disturbances, and enable them to adapt to changing operating conditions. Similarly, substation automation technology advances the state of the art in balancing load locally or across the electric grid, maintaining proper voltage levels, and responding to disruptions or attacks. Almost all discussions in the energy sector related to the electric grid start and end with the term “Smart grid”. For semantics purposes we will use the term, but it should be commonly understood that PNNL considers the grid to have a future state consisting of highly connected, and highly capable devices and platforms that will be distributed throughout the generation, transmission, distribution, and load (consumption) segments that comprehensively make up the bulk electric grid.

To accomplish this higher degree of coordination, a layer of information and communications technology now permeates the power grid and parallels the extent of its reach: from generators, through the delivery system, and to the end-use systems. As the extent and capabilities associated with information and communications technology advance throughout the power system, similar advancements are taking place in the monitoring and control of distributed generation, storage, and end-use systems. These domains of automation are maturing to the extent that their boundaries touch
Emerging Vulnerabilities

Despite the significant benefits of future power grid technologies, the increased communication and control capabilities from these technologies introduce many new and significant cyber vulnerabilities. First, the communication systems will be more extensive, with many more access points and additional exposure to possible attacks. Second, these communication systems will be more interconnected, exposing the system to more potentially extensive failures and attacks. Third, systems will be significantly more complex than the current grid. Fourth, these systems will increasingly use commonly available commercial computing technologies and will be subject to their weaknesses. Finally, the communication systems will generate, gather and use data in new ways. Improper use of this data presents new vulnerabilities to national security, our economy, and our society. The following sections address each of these concerns in more detail.

**Increased Exposure:** Full deployment of new technologies, including smart meters, intelligent appliances, and other sensors, increases the number of devices that must be managed by a factor of at least ten, and perhaps by a hundred or more. The number of access points to this infrastructure and these devices will increase accordingly. A large utility today has hundreds to thousands of substations to manage. After a full deployment of advanced metering infrastructure (AMI) the number of endpoints would grow to the millions. With their two-way communication capabilities, smart meters installed at customers’ premises become access points into the smart grid network. To manage these components cost effectively, they must be remotely upgradable, creating new exposure and vulnerability. Of additional concern is the fact that, unlike substations, meters are located outside the physical control of the electricity service provider.

The increased exposure applies not only to external threats, but also to those people with inside knowledge of automation equipment and service providers’ organizations. People will require access to smart-grid-related devices and systems for maintenance and replacement at all levels of the electric system. The insider may have the appropriate security clearance and process knowledge to thwart reasonable defenses. As smart grid capabilities interconnect multiple systems, the reach of an insider threat is likely to grow unless defensive mechanisms are carefully designed to constrain the extent of the reach at each access point and each layer of the system.

**Interconnectivity:** The smart grid will bridge together heterogeneous networks, making the system susceptible to the vulnerabilities of each network. Interconnectivity also brings the threat of network-propagating malware (e.g., worms, viruses). In addition, utilities that host smart grid connected networks are subject to different regulatory requirements that result in vastly different security measures. Figure-1 below illustrates the interconnected nature of the smart grid and shows that there are a significantly higher number of potential communication paths between various areas of the electric system than existed in past systems. Without proper controls, a problem in one area could cause problems in another. For instance a virus on your personal computer used for surfing the web as

---


7 “Insider” as a person having privileged or at a minimum escalated access to locations, devices, information that an outside entity would not.
well as managing your home area network (HAN) might propagate to an electric vehicle, which in turn might spread to an electric charging station and then to other electric vehicles. The payload of this malware could cause your car’s computer systems to crash or possibly attempt to destabilize the grid by using a time synchronized attack to charge or discharge many grid-connected vehicles’ batteries at once.

**Complexity:** The present electric power grid is large and complex; the smart grid will add additional complexity by integrating distributed generation and storage, demand-response programs, and eventually electric vehicles. All these features will add significant challenges to managing the power system. While the diversity of resources can bring greater flexibility in managing the system, this complexity can increase the likelihood of operator error, create more opportunities for failure particularly during the transition from existing technology to next-generation technologies, and create a large attack space for exposing and exploiting vulnerabilities. Other factors also affect the complexity of this system: IEEE Security and Privacy magazine recently published an article titled “Smart-Grid Security Issues,” which points out that “human behavior, commercial interests, regulatory policy, and even political elements” will all contribute to the complexity of the smart grid.9

---


Common Computing Technologies: Enabling the smart grid will require the capabilities and economics of commonly available commercial computing technologies. Multipurpose operating systems and routable network protocols will be used to provide the necessary communication and computing capabilities. Many of the problems that now exist in the office-computing environment (e.g., viruses, worms, Trojans, rootkits, etc.) will affect the smart grid. Appendix C of the NIST Interagency Report 7628 lists and describes the types of vulnerabilities that will arise from using common computing technologies and that will need to be addressed.10

Increased Automation: Smart grid technologies will automate many functions that are done manually today. With the aid of computers, human error is greatly compounded. Many new smart meters can remotely connect and disconnect power to homes.11 This ability to control electricity to large numbers of consumers remotely has been described as the nuclear option or the “cyber equivalent of a nuclear strike – a completely disabling strategic attack that would reduce the enemy population to nineteenth-century standards of living.”12 Without proper mitigations, an operator error or a malicious actor could quickly cause much more damage than previously possible.

Smart Grid Can Make the Electricity System Less Operationally Vulnerable

Smart grid capabilities provide new tools to enable electric system operators to meet changing power needs and add new functionality. These capabilities can improve the resilience of the electricity system in three important ways:

- **Advanced sensor technology and decision support tools** provide system operators with more accurate and timely information about system stresses and security risks from potential problems.
- **Automation of transmission and distribution systems** allows coordinated switching and protective relaying during system disturbances. These capabilities contain the effects of disturbances and support restoration after the force of an event has subsided.
- **Distributed energy resources** (DER) provide responsive generation, storage, and load within local electric distribution and end-use systems that can be combined in multiple ways to strengthen system operations.

There is a potential for future smart grid devices to increase operational security of a device or overall system. The current challenge however, is that vendors already struggle to meet customer demands related to desired features where security hasn’t been made a priority. Advanced sensor technology installed at the bulk transmission level can enhance situational awareness and decrease the vulnerability of the system to disruption from intentional or natural acts. Communication networks help to share sensor data across operating areas and regional interconnections quickly. Computer systems can analyze, organize, and summarize the data in tables, pictures, and trending visualizations to help system operators understand the state of the system and the level of system stress (a degree of vulnerability).

---


When used with sophisticated decision support systems, this data can help operators reduce security risks from impending problems, or mitigate the extent of damage done to the system from a disruption. At the distribution level, measurements from distribution automation systems can be relayed to distribution operators to help them understand which areas are affected by a local disturbance, diagnose problems, and reconfigure the system to mitigate impacts of such events. The gap remains where security has not been built-in as a defined capability based on area or domain requirements. The advancements of technology need to include these capabilities, but will remain challenged by regulation and/or auditing security requirements instead of strong use-cases for proper development and deployment.

The Dynamic Nature of the Smart Grid Introduces Vulnerabilities

Although the benefits of smart grid technologies are significant, the increased communication and control capabilities of these technologies will introduce new cyber vulnerabilities. Vulnerabilities include the following:

- Communication networks linking smart grid devices and systems will create many more access points to these devices, resulting in an increased exposure to potential attacks.
- Communication networks will be more interconnected, further exposing the system to possible failures and attacks.
- The electric system will become significantly more complex as more subsystems are linked together.
- Smart grid systems will increasingly use common, commercially available computing technologies and will be subject to their weaknesses.
- Communication networks will generate, gather and use data in new and innovative ways. Improper use of this data presents new risks to national security and our economy.

Mitigating Smart Grid Vulnerabilities

The smart grid functions derived from the use of distributed energy resources and transmission and distribution automation contribute to mitigating cyber attacks on the system. While cyber criminals or cyber warfare can compromise parts of the system, the resulting abnormal system behavior from such attacks can result in the separation of parts of the system. With DER and automation resources in the delivery infrastructure, the extent of the detrimental impact from the attack may be contained. The ability to create electrical islands in the distribution or transmission system can continue to service end-users in a priority manner. In addition, detection of cyber disturbances can provide input to operators
of the communications systems to segment the information traffic and thereby limit the spread of malware or cyber espionage. By having a system whose components are prepared to change their state to safe operating positions in the event of lost communication, electricity delivery may be able to continue, even though operational efficiency may be reduced due to the deliberate isolation of communications links.

Physical and cyber security best practices throughout the design, implementation, maintenance, and decommissioning lifecycle will help mitigate potential disruptions caused by deliberate attacks or inadvertent actions. This requires an engineering and operations culture that embraces security when developing and deploying information and communications technology into the electric system. Smart grid deployments need to be designed with predictive and adaptive cyber and physical defense-in-depth systems using layered security techniques. Using this approach, if one layer is breached the other layers can still mitigate a disruption.
3 Energy Sector Cyber Security Research Programs, Policy, and Requirements

The current state of policy and governance for cyber security in general contains a wide range of codified regulation, highly detailed standards, and self-adopted program or frameworks. Many use the same philosophy or approach, but few have commonly identified semantic structures that allow a contextual framework. In this section, PNNL will present the DOE-OE Roadmap to Achieve Energy Delivery Systems Cybersecurity, while coupling significant efforts by the National Institute of Standards and Technology guidance to should provide a strong semantic framework for the discussion of cyber security in the energy sector.

Research and Development - DOE-OE ieRoadmap

Cyber security has historically, and is currently, part of the fundamental DOE mission to secure our energy infrastructure. Through effective interaction with energy-infrastructure owners and operators, vendors, and the national laboratories, DOE-OE has programmatically committed to providing a forum populated with active working groups that are diligently working to solve cyber security challenges for energy delivery systems. To chart the course for this effort an interactive roadmap (the ieRoadmap) was created to enable energy sector stakeholders to map their energy delivery system cybersecurity efforts to specific milestones identified in the Roadmap to Achieve Energy Delivery Systems Cybersecurity. The ieRoadmap, managed by the Energy Sector Control Systems Working Group, provides a platform for pursuing innovative and practical activities that will improve the cybersecurity of our nation's energy infrastructure.

The ieRoadmap:

- Informs the sector of new and ongoing energy delivery systems cybersecurity efforts
- Helps the sector to identify gaps in the energy sector’s cybersecurity efforts and minimize unnecessary, overlapping, or redundant efforts
- Provides a forum to encourage and stimulate collaboration within the energy sector
- Helps energy stakeholders align their resources to develop and implement the strategic and tactical approaches needed to achieve the Roadmap milestones

---

13 Roadmap to Achieve Energy Delivery Systems Cybersecurity (http://www.controlsystemsroadmap.net)
14 Energy Sector Control Systems working Group (https://www.controlsystemsroadmap.net/aboutus/Pages/Working-Group.aspx)
PNNL Technology Assessment for McAfee®, Inc.

- Aids the sector in measuring progress toward meeting the Roadmap milestones

During the initial ieRoadmap rollout in 2006, several barriers were identified by industry. These barriers define a high-level set of challenges that the ieRoadmap intends to solve. The barriers identified are:

- Cyber threats are unpredictable and evolve faster than the sector’s ability to develop and deploy countermeasures
- Security upgrades to legacy systems are limited by inherent limitations of the equipment and architectures
- Performance/acceptance testing of new control and communication solutions is difficult without disrupting operations
- Threat, vulnerability, incident, and mitigation information sharing is insufficient among government and industry
- Weak business case for cyber security investment by industry
- Regulatory uncertainty in energy sector cyber security

Research, industry, and vendor teams have provided specific solutions towards breaking down these barriers. The efforts to date are listed on the ControlSystemsRoadmap.net website. The efforts that support the core ieRoadmap strategies intended to be addressed by 2020 are:

- Resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.
- Build a Culture of Security
- Assess and Monitor Risk
- Develop and Implement New Protective Measures to Reduce Risk
- Manage Incidents
- Sustain Security Improvements

As one may imagine the overall task is extensive and the implementation timeline long. As of this report there remains an eight-year window to achieve effective strategy solutions to ensure that barriers are identified and remain mitigated by a sustainable security posture. Often used in the same context with energy delivery systems are SmartGrid systems. It is important to note that these systems are part of the larger energy grid environment. “SmartGrid” may represent those digitally advanced technologies that have more functional intelligence or capability than the bulk of the devices already deployed in the power grid today. Consistent with the DOE-OE Roadmap however, both delivery system and SmartGrid systems are both enabled by highly connected networks and shared computing capabilities that are challenged by a significantly accelerated growth of cyber security vulnerability.

**Cyber Security Guidance for the Smart Grid**

From PNNL’s perspective, and many who in industry share the same opinion, few words can more clearly articulate the need for a comprehensive approach to “Smart Grid cyber security” than does the NIST IR 7628 document itself. “Traditionally, cyber security for Information Technology (IT) focuses on the protection required ensuring the confidentiality, integrity, and availability of the electronic
information communication systems. Cyber security needs to be appropriately applied to the combined power system and IT communication system domains to maintain the reliability of the Smart Grid and privacy of consumer information. Cyber security in the Smart Grid must include a balance of both power and cyber system technologies and processes in IT and power system operations and governance. Poorly applied practices from one domain that are applied into another may degrade reliability.\(^{15}\)

The nineteen categories of high-level security requirements represented in the table below have a number of specific associated security controls. These describe the requirement but do not prescribe the solution.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Individual Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>SG.AC</td>
<td>Access Control</td>
<td>(21)</td>
</tr>
<tr>
<td>SG.AT</td>
<td>Awareness Training</td>
<td>(6)</td>
</tr>
<tr>
<td>SG.AU</td>
<td>Audit and Accountability</td>
<td>(16)</td>
</tr>
<tr>
<td>SG.CA</td>
<td>Security Assessment and Authorization</td>
<td>(6)</td>
</tr>
<tr>
<td>SG.CM</td>
<td>Configuration Management</td>
<td>(11)</td>
</tr>
<tr>
<td>SG.CP</td>
<td>Continuity of Operations</td>
<td>(11)</td>
</tr>
<tr>
<td>SG.IA</td>
<td>Identification and Authentication</td>
<td>(6)</td>
</tr>
<tr>
<td>SG.ID</td>
<td>Information and Document Management</td>
<td>(5)</td>
</tr>
<tr>
<td>SG.IR</td>
<td>Incident Response</td>
<td>(11)</td>
</tr>
<tr>
<td>SG.MA</td>
<td>Smart Grid Information System Development and Maintenance</td>
<td>(7)</td>
</tr>
<tr>
<td>SG.MP</td>
<td>Media Protection</td>
<td>(6)</td>
</tr>
<tr>
<td>SG.PE</td>
<td>Physical and Environmental Security</td>
<td>(11)</td>
</tr>
<tr>
<td>SG.PL</td>
<td>Planning</td>
<td>(5)</td>
</tr>
<tr>
<td>SG.PM</td>
<td>Security Program management</td>
<td>(8)</td>
</tr>
<tr>
<td>SG.PS</td>
<td>Personnel Security</td>
<td>(9)</td>
</tr>
<tr>
<td>SG.RA</td>
<td>Risk Management and Assessment</td>
<td>(6)</td>
</tr>
<tr>
<td>SG.SA</td>
<td>Smart Grid Information System and Services Acquisition</td>
<td>(11)</td>
</tr>
<tr>
<td>SG.SC</td>
<td>Smart Grid Information System and Communication Protection</td>
<td>(30)</td>
</tr>
<tr>
<td>SG.SI</td>
<td>Smart Grid Information System and Information Integrity</td>
<td>(9)</td>
</tr>
</tbody>
</table>

Table 1, NIST IR 7628 – High-Level Smart Grid Security Requirements

The NIST IR 7628 document also contains a very valuable piece of work in Appendix-A. This appendix, “Crosswalk of Cyber Security Documents\(^{16}\)” provides a mapping across the NIST IR 7628, NIST SP 800-53 (Rev-3)\(^{17}\), DHS Catalog of Control Systems Security: Recommendations for Standards Developers\(^{18}\), and the NERC CIPs (1-9) dtd. May 2009\(^{19}\). While multiple governance entities sort out an absolute set of requirements, and while critical infrastructure owner/operators may own and operate multiple assets within multiple governance areas, this appendix provides an excellent navigational capability across

\(^{15}\) NIST IR 7628, “Guidelines for Smart Grid Cyber Security”, pg.4-Scope and Definitions
\(^{16}\) NIST IR 7628, “Guidelines for Smart Grid Cyber Security” – Aug 2010
\(^{17}\) NIST SP 800-53 (Rev-3)
\(^{18}\) DHS Catalog of Control Systems Security: Recommendations for Standards Developers
\(^{19}\) NERC CIPs (1-9) dtd. May 2009
these concerns. This assessment, and any subsequent assessments, should utilize this resource as it expedites the ability to apply a common set of security controls across an energy enterprise.
Industry Policy and Cyber Security Requirements

The highest impact affecting the security of the Bulk Power System (BPS) are the strict audit requirements of the North American Energy Reliability Corporation (NERC) reliability standards, most specifically the Critical Infrastructure Protection (CIP) 001-009 requirements documents. The complete CIP catalog represents the following ten separate subject areas:

- Sabotage Reporting (001)
- Cyber Security – Critical Cyber Asset Identification (002)
- Cyber Security – Security Management Controls (003)
- Cyber Security – Personnel & Training (004)
- Cyber Security – Electronic Security Perimeters (005)
- Cyber Security – Systems Security Management (007)
- Cyber Security – Incident Reporting and Response Planning (008)
- Cyber Security – Recovery Plans for Critical Cyber Assets (009)

The fully articulated definitions reside on the NERC website (Standards, Reliability Standards, Critical Infrastructure Protection-CIP). In this section the technical focus will be around the CIP-005-3a, and CIP-005-3b standards. Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3. The two key concepts that need to be fully understood are; 1) Electronic Security Perimeters (ESP), and 2) Critical Cyber Assets (CCAs). The NERC CIP-002-4, Attachment-1, defines “Critical Asset” (CA) by currently listing 17 technical attributes. The “cyber” component would be the function provided to operate the CA (i.e., hardware, software, firmware, network connections, serial (or other) connections). The NERC guidance does not allow an asset owner to discriminate with regard to the risk of vulnerability associated with a specific function, only that it is a functional part of the CA. Once the CAs and CCAs are identified the ESP will begin to be defined. Specific guidance for establishing the ESP is provided in CIP-005-4. Also, the requirements section of this guidance further specify not only the CCAs that are defined to be within the ESP, but those that provide an interface to the ESP. All other uncontrolled (not under the purview of the asset owner) devices are exempt from the ESP, (e.g. uncontrolled data/telecommunications equipment that transports data between ESPs).

To this point in the document you should understand that there is significantly funded research and development around cyber security for the energy sector by the U.S. Department of Energy, that specific guidance does exist from NIST in the form of the NIST IR 7628 as well as Special Publications in Series 800 of the NIST technical library, and that industry is significantly challenged by strict policy requirements provided by the NERC. The next section will break down the system view to provide an easier understanding of what we’re presenting.

---

[NERC website (Standards, Reliability Standards, Critical Infrastructure Protection-CIP)]
Industrial Control Systems Cyber Security

The functional technology layers represented in the figure below in many cases have significant connectivity from a network and system perspective. A fundamental challenge is commonly discussed as the *convergence* of the business, operations, and industrial control system areas. Common enterprise-based information technology methods are the culprit. Highly purposed ICS systems have leveraged common networking, protocol, and practice in where now, real-world cyber-physical systems are controlled by centralized SCADA platforms. The legacy systems that remain are signficant, and those systems may rely on their very dated communications interfaces and single-purpose capabilities. However, many have been provided with augmented capabilities that integrate their functions into current and common computer and network infrastructure netting both very good and very bad results. Very good in integrating a common view where command and control are usually very centralized and highly capable and very bad where security has yet to even be an after-thought. Since these environments have grown to be very functionally integrated through highly connected infrastructure, one would be predisposed to think of using a security posture that could be applied in the same manner. Once very important difference, in that such a security system would need to consider interoperable security controls leveraged through a well orchestrasted hierarchy rather than layer after layer of bolted-on devices and software. In this assessment consider the figure below to depict virtually any CI/KR real world cyber-physical domain such as transportation, oil & gas, water, etc.

The power grid contains many different types of devices that contain critical measurements. These intelligent devices generate a huge amount of data that is be capture, analyzed, visualized, and protected. This data may be binned into the following categories:

**Operational data**—Represents the electrical behavior of the grid. It includes data such as voltage and current phasors, real and reactive power flows, demand response capacity, distributed energy capacity and power flows, and forecasts for any of these data items.

**Non-operational data**—Represents the condition, health and behavior of assets. It includes master data, data on power quality and reliability, asset stressors, utilization, and telemetry from instruments not directly associated with grid power delivery.

**Meter usage data**—Includes data on total power usage and demand values such as average, peak and time of day. It does not include data items such as voltages, power flows, power factor or power quality data, which are sourced at meters but fail into other data classes.

**Event message data**—Consists of asynchronous event messages from smart grid devices. It includes meter voltage loss/restoration messages, fault detection event messages and event outputs from various technical analytics. As this data is triggered by events, it tends to come in big bursts.

**Metadata**—Is the overarchng data needed to organize and interpret all the other data classes. It includes data on grid connectivity, network addresses, point lists, calibration constants, normalizing factors, element naming and network parameters and protocols. Given this scope, managing metadata for the power grid is a highly challenging task. This data then could traverse many complex and highly interconnected networks as described in Figure-2. The three main layers that are depicted represent a commonly adopted view of where CCAs may reside within the defined ESPs. These layers are; 1) Grid

---

21 Cyber-Physical Systems; Devices, platforms, equipment that can be manipulated using computing capabilities (i.e., software and hardware).

---

27 PNNL-21313
Power System, 2) Control System, 3) Communications. These physical boundaries contain many interconnected networks.

The Grid Power System represents the highest layer of the overall combined technologies that support generation, transmission, distribution of power. It will contain many computing environments spanning multiple organizations each with certain business and operational responsibilities.

The Control System layer provides the real-time control of power flow. As a highly coordinated system in itself, it is also very highly connected. In this layer, the CCAs are identified. Due to the overall coordination required between systems and devices, it is most difficult to define any associated CCA components. A failure of any component in the overall system may or may not represent a failure of a particular CCA function. However, should an associated component be required to be fully functional to ensure full function of a CCA, then that component itself becomes a CCA.

The Communications layer enables the enterprise’s ability to integrate business process with operational demands. This layer provides that largest vulnerability to the operational integrity of the enterprise. Once this layer is compromised, it is very difficult to fully mitigate the spread or effect of an intrusion.
A typical system breakdown may be represented as in Figure-3. This architecture looks fairly neat and clean, however, the complexity of the network topology, protocols enabled on it, resident devices, and the overall combination of software and firmware that enables all of the associated functionality is very complex.

As indicated while completing a systematic breakdown of the SCADA diagram, a cyber security specialist will discover that the entire network is protected by a single firewall. Given the benefit of a good IT security deployment, you may assume that the personal computers and servers are protected by a domain controller, anti-virus, a corporate intrusion detection/prevention system, and a set of well defined corporate computer security policies. From a cyber security perspective how would the cyber security specialist provide security to ensure that the system(s) were “trusted”. Referring to our previous discussion, “What are the Threats of a Cyber Security Attack on the Power Grid” our specialist needs to:

- Trust configurations
- Trust applications
- Trust sources
- Trust execution
- Dynamically trust what is good, deny what is bad, and control what is neither
- Recover quickly from anything
• Continually report status (Assess, audit, comply)

Our system in figure-5 has not;
  ✔ baselined configurations
  ✔ authenticated applications
  ✔ mapped trusted sources
  ✔ interrogated execution
  ✔ determined good/bad or other
  ✔ provided a recovery method
  ✔ reestablished a trusted operational environment

With some assumption you could;
  • Ascertain that backups are current and clean
  • You have all the production and engineering skills necessary to fully recover
  • Methodically test your endpoints for integrity
  • Reload backups
  • Reconfigure software OS and Applications
  • Test system functionality
  • Restart production environments after forensic efforts have assured Sr. management that the problem won’t reoccur and you won’t have to start from the beginning

Complicating the problem is current electric industry oversight and auditing which is providing significant challenges to asset owners with regard to the establishment ESP’s and ‘what’ constitutes a CCA. More specifically, there have been many inconsistencies reported during NERC CIP audits that include certain hardware and software processes within general information technology (IT) infrastructure that are used to connect and protect industrial control system (ICS) hardware and software are themselves considered within both the CCA and ESP purview. To fully identify and mitigate cyber security risks associated with these realms is, at a minimum, a very difficult and costly challenge for the industry. It is safe to say, however, that most security solutions are added to this operational infrastructure (bolted on) and provide specific security controls that address network and platform security. In fact, where very high performance data acquisition or energy management systems (EMS) exist many current anti-virus, firewall, and proxy protection technologies aren’t utilized because those types of operational systems and subsystems often experience performance degradation which may present inadvertent software or data collection errors during real-time execution.
PNNL Technology Assessment for McAfee®, Inc.
4 Threats of a Cyber Attack on the Power Grid

Driving our need to secure our energy delivery environments is the threat of a cyber attack that could impose significant damage to physical infrastructure, and thus challenge public safety. Impacts are physical, psychological, political, emotional, and reactive. These attributes are all multipliers of the effects that a successful cyber attack could have if not identified and mitigated. Why a cyber attack? This isn’t a simple question to answer. The approach to understanding motive, opportunity, and intent (MOI) will help the viewpoint of why, but more importantly those characteristics are used to define and design the defensive techniques that will be effective against such an attack. Detect, deter, delay, deny, respond, and recover are the core attributes used in a well-constructed defensive posture. This is true of the cyber defensive posture. Physical security professionals swap “detect” and “deter”, because they typically deploy physical security measures to first deter and attacker. Cyber security professionals don’t have that luxury. The technique most afforded cyber security professionals is the ability to detect that an adversary is has visited, is lurking, is inside, or is active. The adversary has many characteristics, many of which from an MOI perspective can be represented by a Low, Medium, and High threat perspective. This approach is accepted in many risk management programs. For our shortened cyber security threat discussion a; “Low” level threat is an adversary that is typically a common hacker, hacktivist (politically motivated, or sympathetic hacker); a “Medium” threat which represents a more coordinated or structured capability such as having more financial means and significant hacking experience; and a “High” level threat typically involves organized criminals enabled possibly through a nation state.

Now we know “what” a threat may be build from, why the power grid? For arguments sake, on broader terms why critical infrastructure? Impact. The adverse effects from a successful cyber attack can not only potentially cause physical damage, but the reaction to such an attack (depending on the target) can have long-term financial and reputation implications. Our power grid owners and operators are very good at generating, transmission, and distribution of power. This is true worldwide. However, they are very dependent on the digital/electronic means to accomplish this task. When such a complicated digital environment is challenged the operators are busy reacting to protective mechanisms, planning requirements, and delivery priorities. With a well-placed cyber tools, the attacker can feign and fake operators into doing the damage themselves, or override any centralized capability to command and control the system into orderly operations or recovery.
So what are the threats of a cyber attack on the power grid with respect to cyber security?

- Connectivity and Network traffic (manipulation, man-in-the-middle, intrusion, interception)
- The OSI layer model; (Physical layer, Data link layer, Network layer, Transport layer, Session layer, Presentation layer, Application layer, System layer)
- Buffer Overflows
- String Injection/Manipulation
- Denial of Service
- Operating System (patches, bug fixes, inefficiencies, programming errors)

Why the whole OSI model? Control systems were not originally conceived on the OSI model. Vendor proprietary approaches provided a huge competitive advantage for those vendors that could very efficiently integrate their system capabilities. Routable technologies via Ethernet have allowed new cost-effective and efficient connectivity to control systems. During the transition to the Ethernet many employed simple encapsulated protocols *glued* to the Ethernet environment. The older protocols were simply wrapped into TCP/IP protocol and unwrapped at the destination.

Social/Behavioral Engineer and Exploitation puts the attacker at either the insider or close to an insider that may have access to the target systems. The OSI model can be directly challenged with air gap (USB, portable media, wireless), via a trusted source. Many exploits have been successful this way. Another behavioral manipulation is to draw the trusted source to the attacker. Websites, such as discussion forums, professional group websites, Facebook, etc., provide an attacker an endless supply of unwitting participants. What do we know about cyber threats to the energy sector?

The cyber attacker will:
- Pollute the supply chain
- Infect operating systems and embedded systems
- Use the network to listen and mimic digital transmissions
- Replace known/good software with bad
- Challenge the integrity of system endpoints and centralized command and control
- Challenge authentication and authority
- Combine, confuse, and overwhelm a target set

The cyber defender will *need* to:
- Trust configurations
- Trust applications
- Trust sources
- Trust execution
- Dynamically trust what is good, deny what is bad, and control what is neither
- Recover quickly from anything
- Continually report status (Assess, audit, comply)
PNNL Technology Assessment for McAfee®, Inc.

Top 10 Vulnerabilities of Control Systems and the Newest Threat

The following Top-10 vulnerabilities of control systems were presented as a result of the efforts from the Control Systems Security Working Group made up of government, academic, industry, and researchers. Although circa 2006 this list stands as the comprehensive list of concerns, recently augmented by the “Stuxnet” and subsequent “Duqu” variants of 2011-2012. At a high level our assessment shows that the features and functionality of the McAfee® Application, Change, and Integrity Controls would offer preventative measures that could mitigate these concerns. At a detailed level, as these vulnerabilities and mitigations are discussed in the document, we believe that the McAfee® technology would match well with properly configured and processed Solidification™.

Top Ten Vulnerabilities of Control Systems

TOP 10 VULNERABILITIES OF CONTROL SYSTEMS AND THEIR ASSOCIATED MITIGATIONS – 2006

National SCADA Test Bed Program

March 16, 2006

• Inadequate Policies, Procedures, and Culture Governing Control System Security
• Inadequately Designed Control System Networks That Lack Sufficient Defense-In-Depth Mechanisms
  *McAfee® solution addresses through Layering of Application Control, Change Control, Solidification™, and integration of ePO.
• Remote Access to the Control System without Appropriate Access Control
  *McAfee® Integrity Control for endpoint protection.
• Auditable System Administration Mechanisms (System Updates, User Metrics, etc.) are Not Part of Control System Implementation
  *McAfee® solution addresses through Layering of Application Control, Change Control, Solidification™, and integration of ePO.
• Inadequately Secured Wireless Communication
  *McAfee® Integrity Control for endpoint protection.
• Use of a Non-Dedicated Communications Channel for Command and Control, such as Internet Based SCADA, and/or Inappropriate Use of Control System Network Bandwidth for Non-Control Purposes (e.g., VOIP)
  *McAfee® Integrity Control for endpoint protection.
• Lack of Quick and Easy Tools to Detect And Report on Anomalous or Inappropriate Activity. Inadequate or Non-Existent Forensic and Audit Methods
  *McAfee® solution addresses through Layering of Application Control, Change Control, Solidification™, and integration of ePO.

PNNL Technology Assessment for McAfee®, Inc.

- Installation of Inappropriate Applications on Critical Control System Host Computers
  *McAfee® solution addresses through Layering of Application Control, Change Control, Solidification™, and integration of ePO.*

- Software Used in Control Systems is Not Adequately Scrutinized
  *McAfee® solution addresses through Layering of Application Control, Change Control, Solidification™, and integration of ePO.*

- Control Systems Command and Control Data Not Authenticated
  *McAfee® Integrity Control for endpoint protection.*

**Stuxnet and Duqu**

Most discussion regarding malware or other computer virus infections has been summarily dismissed by those who believe that the legacy characteristics of ICS environments makes them invulnerable because of protocol, dated communications mediums, or unsupported platforms that use RISC based structured logic, very unlike a personal computer. This is an age-old story. The simple fact is that today, we have this new threat which isn’t really the brawler a botnet is, or the bully that malware can be. This new threat is seems to have the disposition of a cyber-sniper. A carefully designed tool tasked for a specific intent. This is proud and highly skilled work. The Stuxnet malware attacked Windows systems using an unprecedented four zero-day attacks. It deployed via infected removable media, and then uses other exploits and techniques to infect and update other computers inside private networks that are not directly connected to the Internet. A zero-day Windows exploit is a highly marketable kit and not normally deployed in numbers. Stuxnet used advanced syntax (including C and C++). It has two modes of rootkit capability under Windows, and also used device drivers that had valid digital signatures. The malware had help from two different command and control servers.

Duqu has much speculation. Same tool different purpose. With such a monumental effort to assemble such a well-crafted piece of malware why wouldn’t it be picked up and used again…and again. Two cyber snipers are in the wild. The days are gone where we can claim that our control systems are safe because they’re not really a hearty target.
Vulnerability and Attack Prevention Using McAfee® Application Control and Change Control and the Solidification™ Process

This section will apply the known industry applied security requirements to the electronic features available in the McAfee® Application, Change, and Integrity Control product set using McAfee® Solidifier. As we discussed in Section-3, certain stringent and audited security requirements are challenging industry to apply a plethora of technologies, many siloed into tightly controlled and disparate capabilities. Worse, the best combination of these may present overlapping controls that will have to be disabled to alleviate potential conflicts in the security posture. A careful assessment and mapping of requirements to the McAfee® solution feature set will allow us to focus on prevention and mitigation strategies without overprescribing unnecessary or irrelevant security controls. Next, we studied a current threat exercise where we will present discussion for the significant effectiveness towards discovery, configuration, control, reporting, and maintenance of ICS platforms using the McAfee products.

Requirements Mapping

The following discussion is centered on providing a mapping of features to the specific guidance and audit criteria that is used in the electric sector. As presented in the previous Cyber Security Policy section above, the two programs driving security requirements for the bulk power system and Smart Grid ICS environments are the NERC CIP 002-009 for the Bulk Power System, and NIST IR 7628 for Smart Grid cyber security. Additional, and very relevant, guidance is found within NIST Special Publication 800-53-Guide for Assessing the Security Controls in Federal Information Systems and Organizations23, and NIST Special Publication 800-82-Guide to Industrial Control Systems (ICS) Security24. While the NERC governance provides specific guidance to more of a higher-level programmatic concern, the NIST guidance and reports provide a detailed description of the security controls necessary to meet NERC requirements as well as providing an extensible resource for best-practice applications of such controls. The McAfee® Solidifier features25 in the following table provide extensive tailorable control within a platform in which it is deployed.

---

25 McAfee® Solidifier Product Guide (For Application Control)
The core features of the McAfee’s Application Control, Change Control, and Integrity Control are:

- **Dynamic Whitelisting**
  
  Authorized code execution through Solidifier. A whitelisting approach provides the ability to deny all others with only the absolute exception of the validated and signed code.

- **Memory Protection**
  
  Unauthorized execution is denied, vulnerabilities blocked and reported.

- **File Integrity Monitoring**
  
  Any file change, addition, deletion, renaming, attribute changes, ACL modification, Owner modification is reported. This includes network shares.

- **Write Protection**
  
  Authorized writes only to Operating System, Application Configuration, and Log Files. All others denied.

- **Read Protection**
  
  Authorized reads only, for specified files, directories, volumes and scripts. All others denied.

Through the Solidification™ process, an inventory of the initial clean software configuration is taken. This manifest serves as the basis for all of the McAfee Solidifier protection mechanisms. Each “solidified” system maintains and protects this configuration through the Application Control and Change Control modules.

The McAfee Application Control module provides:

- Execution control (only authorized code can run)
- Memory control (vulnerabilities in authorized code that is running cannot be exploited)
- Tamper-proofing (prevent deletion, renaming, overwriting of authorized code)

The McAfee Change Control module provides:

- Real-time monitoring for file and registry changes (no scanning)
- Visibility of ad-hoc changes (who-user, what-program, when-log made changes)
- Write protection (no new or modified files or registry allowed by rule)
- Enforcement for compliance (logging and reporting)
- Process execution monitoring
- User account tracking
Applicable NIST Guidance and NERC Requirements

<table>
<thead>
<tr>
<th></th>
<th>Application Control</th>
<th>Change Control</th>
<th>ePolicy Orchestrator</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NIST GUIDANCE</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network IDS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User access controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-virus protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Awareness Training</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Assessment and Authorization</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information and Document Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Response</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Protection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical and Environmental Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Program management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personnel Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>NERC REQUIREMENTS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change control and config. Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Security Perimeter</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electronic Access Controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring Electronic Access</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cyber Vulnerability Assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Document Review and Maintenance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test Procedures</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ports and Services</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Patch Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Malicious Software Prevention</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Status Monitoring</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disposal or Redeployment</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2 – Guidance and Requirements Matrix
The Solidifier, Application Control, Change Control product guides also presented additional features and advanced configuration parameters, which are extensive. This advanced customization capability allows some very important parameter customization that would be used extensively in both legacy and advanced (new) industrial control system environments.

**Secure Signed Updates Reference**

The McAfee® solution also contains digital signature features needed to support integrity requirements. This feature applied at the level designed into an ICS environment provides the highest available path to determine absolute integrity control throughout the platform. The industry today utilizes this capability generally for enabling protected communications pathways. However, rarely in field assessment that PNNL has participated in have these feature been applied deeply into the ICS environment. The *Solidifier product guide* describes the following:

- An administrator can install new software, or patches/updates on a solidified system without entering Update Mode provided the installer is a digitally signed file and its certificate is present in Solidifier Certificates store.

- The primary consumers for this method of performing updates are the manufacturers who embed the Solidifier in their system, e.g., ATM manufacturers, storage system manufacturers, Point-Of-Sale systems manufacturers, etc. However, this method for performing updates can also be used within a commercial Enterprise also. Effectively, the administrator can execute an unsolidified program code on a solidified system provided that it is specially signed.

- The signing process is made secure using the public-private key cryptographic technique for the validation of signed files. A private key is used for signing an executable file. The public key corresponding to that private key must be present on the solidified system in the Certificates directory under the *Solidifier* install directory.

- Any signed file that has a valid public key certificate installed on the system is allowed to execute. The behavior of the validated signed installer is similar to that of an updater on the system.

These are key elements for ICS vendors to consider that would provide significant security improvements in embedded systems, SCADA platforms, Remote Terminal Units (RTUs), and protected communications devices. The breadth of platforms already supported should lend itself an effective path to provide these features.

**Advanced Configuration parameters**

The advanced configuration parameters ads a level of control also not often found in operation today. This level of platform control specifically over the execs and memory on the system would provide a very high-assurance of process and platform integrity. These parameters were not fully assessed in this
mostly because they provide extensive control over processes that need to be fully defined before such an assessment or technical evaluation could prove beneficial.

Table-3 will map the NERC CIP requirements (as selected that are relevant to the technology under assessment to the selected set of features. In this table only the highest impact features for ICS have been mapped. This should provide a strong case for use in this compliance space realizing that the opportunity to provide a significant number of additional credits depending on the system being audited could be achieved.

**Table 3, McAfee® - NERC Feature Mapping**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CIP-003 R6, Change Control &amp; Config Mgmt.</td>
<td>+ + +</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-005 R1, Electronic Security Perimeter</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-005 R2, Electronic Access Controls</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-005 R3, Monitoring Electronic Access</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-005 R4, Cyber Vulnerability Assessment</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-005 R5, Doc Review and Maintenance</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-007 R1, Test Procedures</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-007 R2, Ports and Services</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-007 R3, Security Patch Management</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-007 R4, Malicious Software Prevention</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-007 R5, Account Management</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-007 R6, Security Status Monitoring</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-007 R7, Disposal or Redeployment</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-007 R8, Cyber Vulnerability Assessment</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIP-007 R9, Doc Review and Maintenance</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
After an evaluation of the Solidifier features cursory look at the NERC CIP table above reveals that there are multiple features that may be applied as security controls to the governance requirements. This evaluation is a higher-level view that would be if a specific environment were used. Should the technical details of a platform used fully documented (e.g. processes needed/not needed, port requirements, communication protocols, inter-process communications, and connectivity requirements) the security design would be able to fully leverage the full Solidifier feature set. In addition, the advanced configuration parameters could be strongly tailored to provide a maximum benefit to the operational integrity of the platform and processes it serves.

Table-4 contains a mapping commensurate to Table-3. This mapping however represents how the Solidifier features could be applied to certain high-level security controls for the Smart Grid. Keep in mind, although the NIST IR 7628 report carefully documented the definition and best use of 19 high-level requirements, they are easily mapped and related to the three classes of (Management, Operational, Technical), eighteen families (i.e., access control, audit and accountability, identification and authentication, system and communications protection), and +200 individual security controls. In this evaluation, again, not all of the individual security controls were selected. Only those with a technical application potential were selected in order to quantify the saturation of the Solidifier feature set into the NIST guidance. As this guidance is very detailed it would require an in-depth understanding of the system being evaluated for this application. Preliminary white board exercises netted a high saturation of possibilities, again identifying a significant opportunity to utilize this technology to satisfy the implementation of selected NIST security controls. In this table, the assessors pared-down the mapping to and identified which module would provide the best result, and in some cases (denoted by the “+” a highly applicable feature. This table could be used by asset owners to tailor their set of selected security controls for a specific digital asset, thus providing potential auditors a strong position for its use.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SG.AC-1 Access Control Policy and Procedures</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AC-2 Remote Access Policy and Procedures</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AC-3 Account Management</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AC-4 Access Enforcement</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AC-5 Information Flow Enforcement</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AC-6 Separation of Duties</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AC-7 Least Privilege</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AU-2 Auditable Events</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AU-3 Content of Audit Records</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AU-6 Audit Monitoring, Analysis, and Reporting</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AU-7 Audit Reduction and Report Generation</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AU-8 Time Stamps</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AU-9 Protection of Audit Information</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AU-13 Audit Tools</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AU-15 Audit Generation</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.AU-16 Non-Repudiation</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.CA-5 Security Authorization to Operate</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.CA-6 Continuous Monitoring</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.CM-2 Baseline Configuration</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.CM-3 Configuration Change Control</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.CM-4 Monitoring Configuration Changes</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.CM-5 Access Restrictions for Config Change</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.CM-6 Configuration Settings</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.CM-7 Configuration for Least Functionality</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.CM-8 Component Inventory</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.CM-10 Factory Default Settings Management</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.CP-9 Alternate Control Center</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.CP-10 Information Sys Recovery/Reconstitution</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.IA-2 Identifier Management</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.IA-3 Authenticator Management</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.IA-4 User Identification and Authentication</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.IA-5 Device Identification and Authentication</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.IA-6 Authenticator Feedback</td>
<td>+</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 4, McAfee® - NIST IR 7628 Feature Mapping

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SG.IR-6 Incident Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.IR-7 Incident Reporting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.IR-8 Incident Response Investigation &amp; Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.IR-9 Corrective Action</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.IR-10 Smart Grid Information System Backup</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.MA-2 Legacy Information Sys Upgrades</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.MA-3 Information System Maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.MA-4 Maintenance Tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.MA-6 Remote Maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SA-7 User-Installed Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SA-9 Developer Configuration Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SA-10 Developer Security Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-3 Security Function Isolation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-5 Denial-of-Service Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-6 Resource Priority</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-7 Boundary Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-8 Communication Integrity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-10 Trusted Path</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-12 Use of Validated Cryptography</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-13 Collaborative Computing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-14 Transmission of Security Parameters</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-15 Public Key Infrastructure Certificates</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-16 Mobile Code</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-17 Voice-Over Internet Protocol</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-18 System Connections</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-20 Message Authenticity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-21 Secure Name/Address Resolution Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-22 Fail in Known State</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-23 Thin Nodes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-25 Operating Sys-Independent Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-28 Virtualization Techniques</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SC-29 Application Partitioning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SI-3 Malicious Code and Spam Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SI-4 Information Sys Mon Tools and Techniques</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SI-5 Security Alerts and Advisories</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SI-6 Security Functionality Verification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SG.SI-7 Software and Information Integrity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**
- **Solidification – Application Control:**
  - Execution Control
  - Tamper-Proofing
  - File and Directory Change Control
- **Tamper-Proofing:**
  - Process Execution Monitoring
  - User Account Tracking
- **File and Directory Change Control:**
  - Registry Management
  - Solidifier Management
- **Registry Monitoring:**
  - Dynamic Audit Control
  - Event and Activity Reporting
- **Protected Security Posture:**
  - Protected Security Posture
- **ePolicy Orchestrator:**
  - ePolicy Orchestrator
- **Enterprise Security Visibility:**
  - Enterprise Security Visibility
- **Full Response Command and Control:**
  - Full Response Command and Control
- **Global Threat Intelligence:**
  - Global Threat Intelligence

- **Applicable NIST IR 7628 Requirement**
  - **= Applicable**
  - + = “High value to ICS”
Table Top Exercise in Requirements Mapping and Effectiveness Study

Referring back to Section-3, Figure-3 – “Example SCADA Architecture”, which represented a simple IT approach to securing an ICS system, we now look to a opportunity to apply the McAfee® solution to the same picture. This is a tabletop exercise intended to identify a security posture consistent with the necessary security controls that could be deployed within an ICS environment. The relevant improvements of the Example SCADA Architecture (Figure-4) that could be implemented are seemingly extensive as represented by the green dots littered throughout the diagram.

While we were able to represent quite a bit capability to secure endpoints, client/server platforms, and communications relationships, we ran out of room to show the individual capabilities of the MAC and Solidification™ products. More descriptively many of the example architecture platforms could have these security tools applied in the following manner.
Referring again back to our trust requirements the McAfee® solution provided:

- **Trust configurations**
  - ✔ Image Comparison
  - ✔ Change Configuration Control and Auditing
  - ✔ File Integrity Monitoring and Change Prevention
  - ✔ Endpoint communications configurations
  - ✔ Diagnostic Tool – ScAnalyzer baseline management

- **Trust applications**
  - ✔ Application Integrity Checking
  - ✔ Automatic Application discovery
  - ✔ File Integrity Monitoring and Change Prevention

- **Trust sources**
  - ✔ Change Control
  - ✔ Read/Write Control

- **Trust execution**
  - ✔ Protected Memory Execution
  - ✔ White listed/memory protected application execution

- **Dynamically trust what is good, deny what is bad, and control what is neither**
  - ✔ Dynamic Whitelisting
  - ✔ Global Threat Intelligence (reputation controls)

- **Recover quickly from anything**
  - ✔ Application Audit and Integrity
  - ✔ File Integrity Monitoring and Change Prevention

- **Continually report status (Assess, audit, comply)**
  - ✔ No Updates, ensures no changes from initial configuration
  - ✔ Solidifier, real-time change monitoring and auditing for configuration, code, files, directories, processes and registry (Windows)

The level of protection and configuration will depend on the complexity of the platform being secured. Our initial exercise even in this simple illustration found the set of McAfee® Access and Change Control features to be extensively available to the Windows host operating systems, as well as a significant number of endpoints (especially considering the computing capabilities of the more intelligent single-purpose devices available today). A detailed system evaluation would most likely result in multiple features being applied with the opportunity to customize each deployment.
Detailed Capabilities Table-Top Assessment Using the 2011 NERC Grid Security Exercise as a Realistic Backdrop

More current activities from NERC have resulted in a report titled, “2011 NERC Grid Security Exercise”, After Action Report (dtd. March 2012)\(^\text{26}\). Refer to the original publication for full attribution to the effort and participation. Provided for discussion related to the McAfee®, Inc. approach we thought it valuable to consider what the consortium of participants ranging from multiple private utilities to federal agencies (FBI, DHS, DoD) thought in terms of a valid cyber attack scenario and how responses may have been beneficial in such an attack should the McAfee®, Inc. solution have been deployed in this exercise.

The Exercise Objective

Prior to Move One of exercise play, a motivated adversary with a desire to cause disruption to the power grid had devoted significant resources to developing malware that attacked grid functions. The code leverages communications protocols as an intermediate attack vector to deliver malicious code across the North American bulk power system. Once delivered, the malware corrupted core systems and their functions. The malware required two vital pieces of information to work – network address information and operator credentials. The attacker gained unauthorized access to several substations and back-up control centers (BUCC) and inserted a low profile data device between the keyboard and the computing workstations in these locations to capture administrative credentials and other sensitive data for later use in crafting malware.

As discussed earlier in the document, Motive, Opportunity, and Intent are established, a Medium-Level Adversary with commensurate tools and tactic is engaged, a target set has been identified, and an attack vector has been selected for execution. The attack package is now viable.

Upon introduction, the sophisticated malware sensed anti-virus/anti-malware products in use, maintained a small footprint, and supported numerous operating system-based payloads that could be launched from within the master payload located at one of the drop locations. The malware communicated with other copies to share information in a ‘mesh’-based methodology so that if any one node was discovered, the communications of that node did not reveal nodes belonging to other cells. The malware was designed to run adjacent to main reporting processes and opened ports usually assigned to permitted functions (so that intrusion detection was not triggered), transferred the binary or mapping information, and shut down. A number of hidden binaries were included in the master binary. These additional binaries were small applications designed to run inside existing critical systems. The malware also had the ability to travel from the ICS environments to the corporate network through trusted links. Once there, the worm sought to find egress points out of the network.

Progression of the attack. Anti-virus bypassed, numerous operating systems within the nefarious payload, inter-malware communications enabled, IDS ineffective, hidden binaries running “inside” critical systems, traversal within ICS networks and corporate networks via “trusted” links. The last point of the “worm” working egress isn’t really our concern because the assumption is that it’s already in the deepest most sensitive layer of the ICS network and devices...could it get any worse?

Exercise Phases/Moves
The exercise was structured around three phases or “moves” that simulated three discrete blocks of time. To simulate the passage of time, a notional 24 hours passed between Move One and Move Two, and 48 hours passed between Move Two and Move Three. Each move was initiated by new information that updated players’ situational awareness and understanding of the current environment. The moves are presented in Figure-5.

Move One (T-Zero): Detection and Information Sharing
In Move One, sector entities and organizations began observing abnormal activity in their operational environment. Network operations were sluggish and an overall system slow-down was detected. Operators observe traffic resets and remote terminal unit (RTU) scans fail to complete. It appears that timing relationships and signals are corrupted, endangering the electricity sector’s remote assets. The malware has created plausible changes in unit outputs that remain within the unit’s operating limits. Impacted entities begin to identify alternative means of relaying data, including verbal
Communications and other manual approaches. Entities also consider deploying manpower to substations to address reliability concerns with remote assets. While the source of the issues is not yet understood, IT staff begins forensics measures and attempt to clean systems. Utilities, BAs and RCs share information on the conditions and validate a common pattern of suspicious conditions across the BPS. Players become suspicious of communications protocol traffic and begin to focus on this channel as a source of abnormalities. Meanwhile, market dispatch issues arise due to data anomalies complicating the arrangement of imported power (interchange). The disturbance and current conditions necessitate entities to issue Electric Emergency Incident and Disturbance Reports (OE-417) to the appropriate authorities. As Move One concluded, entities continued to lose visibility and experienced difficulty managing load. An RCIS bulletin revealed that cyber tampering at major utilities’ key locations had been detected.

“Observation” of abnormal activity, network operations challenged, remote devices affected, signals are corrupted, manpower is deployed ($$$), IT executes “forensics” and attempts to “clean” systems (from?). “Suspicious” conditions evident, participants become “suspicious”, reporting initiated so others can plan for response, loss of system visibility, cyber “tampering” detected. All seems to be unfolding for the attacker, multi-resource responses necessary costing resource budgets critical funding to be drained, the network has been fully penetrated, “suspicion” seems to be the tool of choice at this point. The attacker is in the lead.

Move Two (T+24 hours): Validation and Mitigation

In Move Two, entities continued to experience reliability concerns as summer peak demand exacerbated load-balancing issues. ICS-CERT released a bulletin that stated that the imbedded malware was observed attempting to exploit a C2 channel (command and control) within some entities. The egress was detected through analysis of entity network logs. In coordination with ICS-CERT, the FBI announced to the sector the probability of malicious intent to disrupt the power grid. Entities continued to report severe conditions and reliability concerns through RCIS bulletins while coordinating with Regional Entities and authorities. Some failover and back-up systems were inoperable, which forced many entities to initiate manual operations. This process severely taxed resources of RCs, BAs and other Regional Entities. The scenario affected several key calculations and forced some utilities to abandon market activity. Other small utilities that failed to detect the C2 egress experienced intermittent outages in their regions. ICS-CERT, in coordination with the FBI, gathered a flyaway team to engage in further analysis and forensics. Entities also experienced issues with their corporate LAN and other supporting systems, as the malware appeared to have vectored to the corporate network. Network functions were sluggish and DNS resolution was unreliable. Outage management/GIS systems are compromised, corrupting distribution functions among some entities. To conclude Move Two, the ES-ISAC scheduled a sector coordination call to review impacts, provide guidance, and coordinate a response.
At the +24hr mark the malware was detected, command and control compromised, egress successful, FBI is involved (federal resource activation), operations amplify impact by having critical backups in-op, and resources are stressed. Market operations “abandoned”, smaller less capable utilities are suffering power outages, a fly-away team is airborne ($$$), now the corporate LAN is challenged as well as IT resource priorities? The attackers are still in the lead at T+24hrs.

Move Three (T+72): Maintaining Reliability and Initiating Recovery

Move Three began with a media report, chronicling the coordinated attack, grid conditions and response activities. By the start of Move Three, the ES-ISAC, ICS-CERT, FBI, DOE, and FERC shared information frequently. ICS-CERT analyzed malware and published near-term identification and mitigation measures and the NCCIC continued to serve as a coordination point for government agency interaction and information sharing. Entities worked with their anti-virus and control system vendors to obtain patches. A NERC Alert was issued to provide malware information and eradication steps to the community to clean systems and restore functionality. At the conclusion of Move Three, fragile grid reliability was achieved, but with significant inefficiencies.

At +72 hours (three days later!), recognized “coordinated attack”, multiple agencies fully engaged, cyber security experts analyze malware and have a “near-term” mitigation solution, multiple vendors are now engaged ($$$) at multiple levels as they battle the problem and the perception of their reputations, “fragile” grid reliability could cause further stress and failures, operations, support personnel, and the peripheral participants at this point are most likely a few hundred strong. Attackers have achieved their designed objectives.

In summary, The GridEx exercise and report netted the following results:

- **Finding #1**: Entities effectively applied internal security protocols and cyber incident response measures in an effort to maintain grid reliability and mitigate the impacts of a sophisticated cyber attack. Information sharing across business units and departments occurred frequently, but areas for improvement emerged.
- **Finding #2**: Horizontal communication that occurred among utilities was extremely robust but vertical information sharing can be improved. While BPS entities shared information readily, communication with NERC and government agencies, were often not as frequent or comprehensive.
- **Finding #3**: NERC fulfilled its role as the central coordinating body for maintaining reliability across the BPS. By developing alerts and hosting industry coordination calls, NERC promoted information sharing and coordinated mitigation efforts to counter the scenario impacts. Although information sharing mechanisms did promote broader awareness, the exercise identified several areas for refinement and clarification.
- **Finding #4**: NERC’s ES-ISAC and Situational Awareness (SA) teams collaborated closely to support a coordinated BPS response to the GridEx scenario. Despite generally effective coordination, improvements can be made in defining individual roles and responsibilities during a High Impact, Low Frequency events.
Finding #5: Entities responded to initial physical intrusion information with conventional measures but cyber threats should be considered when addressing BPS break-ins.

Finding #6: While the NERC Emergency Standards process could effectively develop binding standards in response to an imminent issue regarding the bulk power system, the process could interfere with core incident response activities at the entity level.

The summary findings are not intended to provide value to the assessment outcome as they represent a coordinated response effort across the entire energy stakeholder domain. Rather, we provided it for an understanding that somewhere in the trenches is cyber security specialist that will be asked, “what the heck is going on and when is it going to be fixed!” The tools being assessed are seemingly answering that very question. The GrixEx Scenario Attack Evolution matrix in Table-5 provides a substantial position that the capabilities offered by the McAfee® solutions are well suited to address an attack scenario as serious as the one in the exercise. In some cases (denote by “!”) the general McAfee® application, change, and integrity control solution could have had a significant opportunity to prevent the malware from entering and executing on the system (a preventative rather than mitigating or forensic measure). The assessors fully understood the attack approach, and the exercised attack vector. However, introducing malware into an environment where the McAfee® solution is deployed would be nearly impossible without detection even if introducing a completely separate device onto the network. If this could be accomplished, such a device wouldn’t have the correct signatures and authority to become part of the operational control system environment especially if a skilled network engineer had properly designed their network. Application, change, and integrity controls are intended to enforce validation and verification of the software and services that provide the functions of the ICS systems. Although the scenario was fictitious it wasn’t that much of a stretch considering the documented and successful attacks on ICS environments today. The level of effort that went into such an exercise was high, the contributors were very skilled, and the outcome worthy of a repeated effort. If, in the next exercise, a security posture such as McAfee’s could be put in tandem with the timeline, it would prove very interesting as to how it may present an appropriate and effective cyber security paradigm.
### GridEx Scenario Attack Evolution (Truncated Activities)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Network addresses and admin credentials</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anti-virus identified and bypassed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Numerous Operating System Payloads</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network “Mesh” malware communications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IDS bypasses, uses approved communications</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hidden binaries and a master binary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Binaries placed on critical plant systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traversal of malware on trusted networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>“Observation” of abnormal activity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network operations challenged</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Remote devices affected, signals are corrupted</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IT executes “forensics” and attempts to “clean” systems, “suspicious” conditions evident, participants become “suspicious” reporting initiated, loss of system visibility**

**Cyber “tampering” detected**

**All seems to be unfolding for the attacker, multi-resource responses necessary challenging resource budgets, the network has been fully penetrated, “suspicion” seems to be the tool of choice at this point.**

**At the +24hr mark the malware was detected**

**Command and control compromised, egress successful**

**FBI is involved, Operations amplify impact by having critical backups in-op, and resources are stressed.**

**Market operations “abandoned”, smaller less capable utilities are suffering power outages**

**Fly-away team is airborne**

**Corporate LAN is affected**

**At +72 hours recognized “coordinated attack”**

**Cyber security experts analyze malware and have a “near-term” mitigation solution.**

**Attack Successful: Multiple vendors are now engaged at multiple levels as they battle the problem and the perception of their reputations, “fragile” grid reliability could cause further stress and failures, operations, support personnel, and the peripheral participants at this point are most likely a few hundred strong. Attackers have achieved their designed objectives.**

---

Table 5 - GridEx Scenario Attack Evolution Matrix
6 Additional Use Cases for the Application of McAfee® Solidifier in Industrial Control System Environments

Use Case #1 – Local Industrial Control System
This first case represents a very typical and dynamically controlled system. It may control mixing equipment in water treatment processes, manufacturing equipment used in production of structural aircraft components, critical processing of petroleum products, and possibly even centrifugal separation or other hazardous environment processes. This system controls a high-speed material separation system. It has been deployed as a stand-alone system only networked within itself. This is to ensure that the system cannot be remotely accessed. In system preliminary system commissioning it was determined that the communications from the PLC containing batch processing data was not getting to the historian in “real-time” as the engineers expected or required by their quality assurance document policies. As such, due to the performance requirements of the Data Historian and the batch processes contained within the Engineering Workstation, no local anti-virus programs are resident.

*Solidifier would be used to determine baselines for the Data Historian, Engineering Workstation, and HMI. The endpoint devices may have single-function processing capabilities but would need to be evaluated for feasibility for the McAfee solution. The PLC would be in the same situation.

Figure 6, Local Industrial Control System
Use Case #2 – NERC Electronic Security Perimeter

The NERC Electronic Security Perimeter (NERC-ESP) allows a site to specify (according to guidance provided by NERC CIP-5) those assets that are included as “critical assets” and “critical cyber assets”. Each has requirements for configuration management, protective mechanisms (cyber/physical) and a host of applied security controls (typically found in such guidance as NIST SP 800-53 and NIST SP 800-82). These controls would be applied in the Control Center and Field Site 1 area depicted below, but the green shaded area is specifically exempt from the NERC CIP-5 requirements, (specifically CIP-5, section 4.2.2, “Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters”).

*Two separated environments, the Control Center and Field sites, pass through an owner controlled communication hub. In this case Solidifier could evaluate the HMI, Engineering Workstations, Data Historian. The field equipment would need to be individually reviewed. Assuming that the target sets may be in the field sites, the owner may wish to deploy edge devices that Solidifier could utilize, but the best solution would be an endpoint resident installation. Depending on criticality of the system and current audit requirements, the owner is most likely to have to make important upgrades. Although the green communications region is not within an “electronic security perimeter”, vulnerability still exists and must be mitigate to the point of protecting any critical assets at the field sites. The Control Center itself “is” a critical asset and within the ESP, so the McAfee® solution would serve a good purpose at that location.*

(NERC Electronic Security Perimeter)
Use Case #3 - Distributed Control System

In this distributed control system (DCS) example, the assets that make up the system are quite diverse. Building on use case #1, the operation would benefit from a Securified implementation of Access and Change Control modules. The connectivity scheme would almost dictate an enterprise solution for full security visibility. Deployment of application control would protect the overall “process” integrity by employing whitelisting and memory protection. Protection from the “enterprise” is also necessary.

*Deploy Securifier and develop a baseline for all client/server platforms. Deploy on HMI, and any feasible endpoints. Evaluate the system for necessary upgrades to ensure critical processes have a high availability. Due to a number of pressure sensors, regulators, and local controllers, this process may have safety concerns related to the proper operation of their ICS. Should a cyber intrusion be successful, the owner must assume any worthy target could cause physical damage, so an enterprise system would be beneficial in a critical response scenario. Process integrity, platform integrity, and endpoint security would minimize risk of a cyber intrusion. Should an adversary get in, it would be unlikely that he could disrupt the critical processes protected by application and memory controls.

---

Figure 8, Distributed Control System
Use Case #4 – Gas Pipeline Management Systems

The Gas Pipeline Management System (EMS) topology typical provided by vendors such as Siemens, ABB, etc., operate on multiple platforms. AIX, Windows, Solaris, and even Linux are operationally deployed today. The pipeline management system is the central brain for critical flow calculations that balance demand and flow. The software has many individual and dependent processes on a single platform and would represent a very high-value target should an adversary compromise it. It is reliant on a high level of connected resources and information. The system is located in what is generally known as a “Primary Control Center”. A secondary “Backup Control Center” is also required should the primary be disrupted and is unable to fulfill its operational function. It is vital that not only both systems be identical, but has the same operational integrity should a transition occur. Herein lies a critical contribution for the McAfee® Solidifier solution.

*As a central integrity host, McAfee® can accomplish full configuration and operational process integrity that would enable a confident and instant transition from a primary to backup operational mode. As well, the distributed integrity controls would offer the ability to provide parity between the process relationships that were established with the primary location and remote stations, while being transferred instantaneously over to the backup location. Critical back centers such as these operate in tandem with their master centers. As the primary is dealing with the issues at hand that cause the instantiation of the backup center, personnel can rely on the integrity of the remote stations that are protected within their network. In the case below, the Regional Control Center (RCC) would also be a part of this overall integrity-based community.

![Figure 9, Typical Energy System EMS Topology](image-url)
Summary and Conclusion

The current approach to mitigating vulnerability within critical infrastructure is highly leveraged by policy and procedures, and an assumption that employees will always act diligently according to such paperwork. As important as policy is in providing a critical foundation for a site’s security posture, they remain bounded by the simple fact that the paperwork is becoming so complicated it is only surpassed by a daunting rule set resident in many our current firewall configurations. Current defensive postures that only rely on general IT computer networks (firewalls), information flow (secure tunnels), and platforms (anti-virus) are roadblocks to the ICS world. Coupled with complex passwords, and any flavor of active directory or LDAP server configuration there remains many active attack vectors designed to breach any of the aforementioned electronic barriers. Assume that your environments will not maintain confidentiality, nor are always available. In any case, ultimately the integrity of your system becomes the highest priority from the ICS perspective. From operational integrity to storage and recovery, ICS environments rely heavily on the information within their scope in order to enable a wide range of control algorithms. A bad sensor can be trouble-shot, communications channels may be monitored and diagnosed, but what’s actually going on onboard the ICS computing platform remains a mystery to the operator, and even some of the most skilled IT professionals. PNNL’s assessment of the overall capability and features of the Solidification™ process (including Application Control and Change Control) provides very high assurances (in many cases absolute assurance), that the software executives, configurations, processing environments, and external data communications endpoints possess the highest level of platform protection available for ICS environments today. Many challenges related to technical security requirements, ranging from best practice to regulatory, can be mitigate with a diligent application of this technology. Fully enabled enterprise solutions will continue to offer much better wider-area situational awareness and control, and these will provide a very important capability to ensure the integrity of the hundreds of devices and platforms that formulate very complicated and diverse ICS environments being used in critical infrastructure.

It is rare to find implementations of application and memory level security protection within an asset owners ICS environment. While this approach will be deployed in greater numbers in the near future, it is important to understand where it may provide the best mitigation approach relevant to current industry security guidance and requirements. Utilizing a comprehensive solution such as McAfee Application Control, McAfee Change Control, McAfee Integrity Control, and an overarching ePO solution, coupled with the Solidification™ process, the asset owner is able to secure disparate applications and endpoints that are defined within their system profiles, at an acceptable and affordable risk portfolio.
About the Authors

**Philip A Craig Jr**

Mr. Craig has many technical and leadership accomplishments throughout his 28 years of engineering and management experience in the fields of cyber security, supervisory control and data acquisition (SCADA) technologies, computing and communications infrastructure, Internet technologies, assembly and inspection automated controls, material handling control systems, and many additional automated process control solutions.

Phil possesses significant experience in the development of complex system and policy solutions in a variety of critical infrastructures including the nuclear power, electric power. He is engaged in both strategic and tactical cyber security defensive solutions for the wide range of critical infrastructure. From the events of 911 he has participated in the physical and cyber security codification efforts for the Nuclear Regulatory Commission (NRC) Offices of New Reactor Research (NRR) and Nuclear Security and Incident Response (NSIR). A significant contribution to the Nuclear Industry resulted in the final presentation of the NRC Title 10 Code of Federal Regulations, Part 73.54 Protection of Digital Computer and Communications Systems and Networks. Falling under the Part 73 Physical Protection of Plants and Materials, the cyber security mission is to protect U.S. Nuclear Power Plants and Facilities from cyber attacks that challenge safety, security, and emergency preparedness.

Mr. Craig’s role as a PNNL Project Manager for DOE-OE related programs, such as the National SCADA Test Bed (NSTB) program, allows him to provide strategic leadership and technical direction relevant to address important cyber security issues in our Nation’s critical infrastructure. Mr. Craig provides response and analytic support for control system related cyber security incidents through his membership with the Nuclear Sector Coordinating Council (NSCC), US-CERT and ICS-CERTs, the FBI InfraGuard program, and the Homeland Security Information Network (HSIN).

**Thomas P McKenna Jr**

Mr. McKenna currently serves as a manager in the Computational Sciences & Mathematics Division at the Pacific Northwest National Laboratory. He is responsible for business development and technical project management related to high performance computing, green technologies, and cyber security for the Smart Grid.

Tom has over 24 years of experience in defining, building, and marketing world-class computing solutions to commercial and government marketplaces, working primarily on high performance computing, carbon capture, network communications, object oriented software, embedded systems, and intellectual property protection at the executive and program management levels.

On the entrepreneurial side, Tom co-founded and served as CEO at InterGroup Technologies. This company produced and sold three complimentary object oriented development tools. This software was licensed by over 30 OEM customers including IBM, Sybase, Symantec, Cognos, Progress Software, Cambridge Technology Partners, Wall Data, and many others spanning a variety of vertical markets.

Tom currently has one issued patent for object-oriented software (6,915,528), and has other patents pending. Tom has received awards such as “Product of the Year” with InterGroup, and was part of a team that won a “Technological Emmy Award” while at Digeo. Tom holds a B.S. in Computer Science from Seattle Pacific University, an executive MBA from the University of Washington, and is a certified Project Management Professional (PMP).
About the Pacific Northwest National Laboratory

The Pacific Northwest National Laboratory (PNNL) operates in x locations and is managed by the Battelle Memorial Institutes for the U.S. Department of Energy. Real-Time research in operational centers, precision information environments and deep knowledge analytics, high performance Supercomputing, and highly innovative research enable a portfolio at PNNL that is highly recognized Research and Development resource. Supporting an annual average of $53M is cyber security research, the subject matter experts at PNNL have capabilities from energy, nuclear, defense, and other sector engagements.

The PNNL Energy Information Operations Center (EIOC) enables researchers to fully immerse themselves and our industry partners in real-time operational testing and analysis of frontier innovations of energy related capabilities to create resilient and secure results.

Precision information environments provide a clear and concise use of very large and dynamic data sets to provide analysts the data necessary to describe highly accurate and repeatable results using highly enabled analytic tools and techniques developed by our scientists at PNNL. These skills coupled with the ability to leverage advanced high-performance computing clusters challenge our scientists to continually provide new computational capacity and capability. PNNL’s science is highly innovative.

New paradigms that employ ideas such as “borrowing natures code”, illustrate that we are in touch with our world around us allowing noted discoveries and technological adaptations to our ever-evolving digital surroundings.
Tables
Table 1, NIST IR 7628 – High-Level Smart Grid Security Requirements ................................................. 24
Table 2 – Guidance and Requirements Matrix ......................................................................................... 39
Table 3, McAfee® - NERC Feature Mapping ..................................................................................... 41
Table 4, McAfee® - NIST IR 7628 Feature Mapping ........................................................................ 44
Table 5 - GridEx Scenario Attack Evolution Matrix .............................................................................. 52

Figures
Figure 1, Conceptual Reference Diagram for Smart Grid Information Networks ................................. 18
Figure 2, Power System Layers ............................................................................................................ 28
Figure 3, Example SCADA Architecture ............................................................................................ 29
Figure 4 - Example SCADA Architecture - SECURED ........................................................................ 45
Figure 5 - 2011 GridEx Move/Event Timeline .................................................................................. 48
Figure 6, Local Industrial Control System .......................................................................................... 54
Figure 7, NERC Electronic Security Perimeter .................................................................................... 55
Figure 8, Distributed Control System .................................................................................................. 56
Figure 9, Typical Energy System EMS Topology ............................................................................... 57
Figure 10, Schematic of a Typical Control Center .............................................................................. 64
Figure 11, Schematic of Most Likely Implementation of the Security Options .................................. 65
Figure 12, Schematic of Primary and Secondary Fluid Loops .............................................................. 69
Appendix-A

Examples of Power Grid ICS Protocol and Device Vulnerabilities

ICCP and PLC Vulnerabilities

The efficient management of much of our country’s critical utility infrastructure depends on near real-time monitoring and control. For the Electric Power market, the complementary infrastructure that provides that monitoring and control is typically called SCADA (Supervisory Control And Data Acquisition). SCADA encompasses the network and distributed systems that enable the communications and processing of data from numerous remote control points.

What has made these SCADA systems, and the underlying infrastructure they support, more vulnerable in recent years is their increased connectivity to the rest of the world. For example, as electricity is moved from one provider to another provider’s domain, each with its own SCADA system, there is a need to share information about the current and planned loads. In addition to the basic operational need, there is the requirement that scheduling and loading information be shared equitably to multiple parties for energy trading applications. There is similarly a need to provide this and other information to intra-corporate enterprise servers for different administrative back-office, customer-service, and engineering functions. Those systems, in turn, are exposed to the Internet. Through this connectivity, a malicious insider or outside hacker could potentially misuse or undermine the SCADA controls.

The Inter-Control Center Communications Protocol (ICCP)

ICCP is an application layer protocol specifically tailored to the needs of electric utilities for exchange of data between control centers or other utility entities over Wide Area Networks (WANs). The entities can be utility control centers, utility and non-utility generators, power pools, regional control centers, regional transmission offices, and independent system operators.

The data exchange information typically consists of real-time and historical power system monitoring and control data including measured values, scheduling data, energy accounting data, and operator messages.

Most of security threats are introduced when ICCP is deployed over public networks. There is a certain level of specificity of SCADA-related applications and protocols, such as requirement for “always on” business continuity and real-time communications, as well as specific versions of OSs and applications, that cannot be patched while servers are operating. The potential impact of untested information security products may be a disruption of operations introduced directly by security products, or due to delays in real-time communications.
A server in a utility control center typically communicates with 10 or more entities (as many as 30 entities) on dedicated frame relays or leased T1 connections using ICCP (Inter-Control Center Communication Protocol). Seldom do the ICCP servers communicate with each other over the public wide area networks (the Internet). The size of entities that exchange data using ICCP vary from a small municipal utility with a limited resources and staffing to large public utilities with adequate resources and staffing. Large utilities may have adequate physical security in place to control access to the control center, while the small entities may not.

For details on ICCP refer the IEC 60870-6 IEC Standards referenced below:

- IEC 60870-6-1: Application context and standards organization
- IEC 60870-6-2: Use of basic standards (OSI layers 1-4)
- IEC 60870-6-503: TASE.2 Services and protocol
- IEC 60870-6-505: TASE.2 User’s Guide
- IEC 60870-6-702: TASE.2 Application profile
- IEC 60870-6-802: TASE.2 Object models

**Access Control**

Access control is fundamentally the responsibility of the ICCP server, which means that the server has to validate all incoming requests for data from ICCP clients before serving them the requested data. For access control ICCP uses address of the remote node. The address can be used on either OSI or TCP/IP transports. OSI has a defined security methodology specified in the OSI layer standards. However, TCP/IP Rev 4 does not have this structure imbedded in the transport stack. For OSI the TASE.2 recommends using the OSI security services and for TCP/IP, Transport Layer Security from the IETF is recommended.

**Data Confidentiality**

ICCP does not specify or support authentication of legitimate users; therefore, cannot discriminate between real and wrongful use. In other words, there is no protection against unauthorized disclosure of data or information. However, it does use ANS 1 encoding.

**Data Integrity**

ICCP protocol does not provide any additional data integrity other than what is provided by TCP. However, most utilities have already had to implement market systems with digital certificates such as OASIS and other Market Systems interfaces.

**Availability**

The ICCP protocol does not guarantee availability of the system, if part or the entire system is compromised. However, when a client/server makes a query request the client/server expects a normal or exception response within a finite time (usually few seconds). If it does not receive a
response, the client/server is expected to process a timeout condition for the query (for example, resend the query or resend the query to a redundant server at the same control center). In addition, ICCP provides the ability to assign a priority level to each request depending on the nature of the request. Typically, controls and time critical request are assigned high priority and schedules, critical text are assigned normal priority, while the non-time critical requests are assigned low priority. In general, critical request result in short packets (less than 100 bytes). Currently, none of the major implementers of ICCP support assigning priority to requests; therefore, all messages are sent with the same priority.

Typical Control Center Configuration

A typical control center configuration is shown in Figure-6. Most control centers typically have three majors operational areas: 1) the main SCADA network and associated data acquisition servers used to monitor and control the various generation, transmission and distribution assets, 2) the ICCP communication network, and program development system. The SCADA network is generally behind a firewall and protected, while the ICCP network and program development system are not behind the firewall and generally not protected. Although the SCADA networks are generally behind firewalls, servers within the SCADA network may have FTP and HTTP services that are open.
Likely Implementation

Figure-7 shows where security improvements can be made in the typical ICCP Control Center Network. The use of gateway security technology, as represented by the network firewalls, is the first major difference. Placing a firewall between control centers allows only authorized protocols to flow freely between entities. The gateway device can also prevent known viruses and worms from infiltrating the network. The second major improvement is the use of host-based security products such as intrusion detection system (IDS), firewalls, and virus protection. The host-based utilities provide an extra layer for the defense in depth architecture and protect the communication servers from local threats.

![Diagram of ICCP Control Center Network](image)

**Figure 11, Schematic of Most Likely Implementation of the Security Options**

Potential ICCP Vulnerabilities

When discussing vulnerabilities it is important to keep the following in mind:

- ICCP traffic is encoded using ASN.1
- Most traffic sniffers do not support decoding ASN.1 traffic
- Traffic between two ICCP communication servers is usually occurs over dedicated lines (T1 or frame relay) limiting exposure
- ICCP does support remote control capabilities, but this is rarely, if ever, implemented
- ICCP uses MMS, ISO 9506, functions to implement data exchange and controls.
• MMS uses ASN.1 encoding to parse messages at the service element level of the OSI stack.

With these in mind, the following vulnerabilities exist:

• Denial of Service
• Disgruntled Employees (client / gateway / ids)
• Virus / worms (client / gateway)
• Packet sniffing at ISP / carrier (gateway p2p vpn, tls)
• Modifying packets
• Unauthorized access to control center network (local or remote)

Denial of Service Attack

ICCP servers and clients are constantly requesting and exchanging information, and without access to the requested information the power grid may not work reliably or may be rendered useless. Gateway security devices are not typically used between communication servers allowing all types of traffic to flow between entities. The denial of service can occur several different ways.

1. By sending repeated request for information from the ICCP server an intruder can lock up the server for legitimate users and operations. Implementations have not used QOS thus no priority has been implemented. Although repeated requests for setting up a dataset could have an adverse effect on other users. ICCP is not a poll/response protocol a dataset transfer must be validated before a transfer can occur.
2. ICCP communication parameters can be inadvertently configured to flood the control center with information. For example, requesting that all parameters be updated at a very high frequency (for example, every second).
3. A device in a control center could be generating large volumes of traffic due to failing hardware, malicious activity (probes/scans), or non-ICCP protocols.

Disgruntled Employees

The insider threat is of concern for all entities. It is common for many organizations to spend all of their cyber-security efforts on protecting the perimeter without adequate attention spent on attacks from within.

Infection of ICCP Server with a Virus

If the ICCP server or other devices are not protected with anti-virus software, they can potential be infected. The infection can be benign, create unnecessary network traffic by sending mass emails, or a Trojan that monitors the activity of the server and potentially e-mails critical information to another host.
ISP

Even though dedicated lines are used for communication between ICCP entities, the end-points and the carrier are possible points of capturing and/or modifying traffic.

Modify ICCP Packet Contents

Most data exchanged between ICCP entities is un-encrypted, but encoded; therefore, the data packets can be read and modified or fictitious traffic injected by proper decoding.

Unauthorized access to data or ICCP server

If the password to access the ICCP server is cracked, an intruder can take control of ICCP server and potential delete system files or even control and modify the bi-lateral table. This can be accomplished either locally through poor physical security controls or remotely.

Gateway Security

Gateway Security has traditionally been thought of as a firewall that is used to protect a network from the Internet or to separate the corporate network from the control center network. However, new technologies are being built into gateway security devices that allow for greater control and capabilities. Examples include virtual private networks (VPN) concentrators for point-to-point and client access, virus scanning software, and protocol anomaly analysis.

Client Security

Client or host-based security is far more than anti-virus software. Advances in technology again improve how the client can protect itself against attack. Besides the ability to protect against Internet threats such as spyware and adware, client-based firewalls can be configured in a granular fashion similar to gateway security devices.

Enterprise Security Management

Enterprise Security Management (ESM) products are used to enforce security policy at the client desktop. Examples of enforceable policies include checking for weak passwords, ensuring folder or share permissions are stringent, and ensuring service packs are up to date.

Programmable Logic Controllers (PLC) Vulnerabilities

Industrial digital automation networks can be categorized according to the following bus classes, depending on the capabilities they offer (in increasing order of complexity):

- At the lowest level are the sensor networks, which were originally designed primarily for digital (on/off) interface. These are fast and effective but have only limited applications beyond relatively simple machine control.
At the next level are the device buses, which provide analog and digital support for more complex instruments and products.

Next are fieldbus networks designed for deterministic communication between computers and programmable logic controllers. Fieldbus networks constitute one of the most widely accepted international networking standards.

At the highest level are the control networks that provide the ability to communicate with each device with 100% determinism while achieving faster response than traditional master/slave poll/strobe networks.

Many PLC protocols are simple and open; and therefore a message can be easily intercepted before it gets to its destination. In addition, many PLC protocols lack password authentication to access memory addresses. A few potential vulnerabilities are described in this section. Many potential attacks are of “man-in-the-middle” type of attacks.

### Overriding Output Coils

In many process control applications output coils (or registers) are activated or deactivated based on the process condition(s). For example, a pump may be controlled by a temperature sensor as shown in Figure-8. If the process fluid temperature exceeds a certain predefined set point, the programmable logic controllers (PLC) will activate the pump and circulate the secondary fluid through the heat exchanger to the cool the primary process fluid as shown in the figure below.
In the scenario shown in Figure-8, there are a minimum the following possible attack scenarios.

- An intruder can override the output coil that activates the pump and compromise the process operation and safety. This scenario requires that the intruder knows the actual output coil address that activates the pump on the secondary loop.
- If the intruder doesn’t know the exact address of the output coil that controls the pump, he/she can blindly deactivate/activate all output coils. However, if a significant number of outputs coils are compromised, it is likely that alarms may be set off.
- Another scenario is for the intruder to monitor all inputs, outputs, and temporary registers and over time correlate inputs and outputs and find the right address to compromise. For example, the intruder can over time note that when a particular input reaches a certain value a particular output is being activated.
- Another possible scenario is to download the control logic and reverse engineer the control.
Denial of Service Attack

PLC devices are constantly scanning or polling sensors, actuators and other devices that are connected to them. Without access to these devices the PLC device may be rendered useless.

*The possible attack scenario is by sending repeated queries to the PLC devices an intruder can lock up the device for legitimate users and operations.

Modify/Erasing Control Logic

Many PLCs provide hardware locks to prevent accidental overriding of the control logic. If the locks are not set or if the PLC doesn't support hardware locks, it is possible to modify or erase the control logic by use of third-party software applications that are commercially available.

*An attacker may override the control logic using a third-part software application.

Overriding Temporary Registers

Many PLCs use temporary registers to store values that are derived or calculated from other primary sensor measurement. These stored values are sometimes used in the control logic to dictate the control path.

*The attacker may override the value stored in the temporary storage register. Or, it is possible that the scan rate of the PLC is much faster than the frequency of the attacker’s override (limited by how fast the PLC can answer a query). If the scan rate is faster than the query update, the overrides using queries could be useless. If the control logic can be downloaded, then the logic can be modified to look at a temporary register that is not being updated by the PLC, but is being controlled by the attacker then the security of the operation can be compromised.

Buffer Overflows

Because PLC protocols are simple, buffer overflows generally are harmless. According to the standard, a PLC packet that doesn't conform to the standard is ignored. If the PLC protocol is not correctly implemented there is the possibility that buffer overflows lead to some unforeseen cause.

*An attacker can execute a buffer over situation by creating an overflow address field (1 byte), function code field (1 byte), in data field (252 bytes), or message field (256 bytes).
PNNL Technology Assessment for McAfee®, Inc.