Authors

David McMullan is the subject matter expert in technical resources for the Colorado region of Xcel Energy. Jeff Reams is responsible for supervising the maintenance of two Ovation systems in Grant County PUD's two hydro powerhouses on the Columbia River. Jaime Foose is the manager of the Security Solutions group at Emerson Process Management Power & Water Solutions.

Security in Real Life: Two Case Studies

BY DAVID MCMULLAN, XCEL ENERGY, JEFF REAMS, GRANT COUNTY PUBLIC UTILITIES DISTRICT, AND JAIME FOOSE, EMERSON PROCESS MANAGEMENT

The following describes two cases of "security in real life." The first is the security approach deployed at the Xcel Energy Pawnee plant, which was not subject to compliance regulations but was interested in developing a strong security posture using industry best practices. The second case is the approach deployed at Grant County PUD's Wanapum and Priest Rapids sites, which was geared towards achieving both a strong security posture and meeting NERC Critical Infrastructure Protection (CIP) version 3 compliance regulations to ensure WECC audit readiness for March 2014. This article describes the different security controls and technologies deployed at each plant and offers recommendations on how to achieve a strong security posture while also becoming compliance ready. Also, the authors explain how each site has implemented security technologies and lessons learned in support of a multi-vendor, plant-wide approach.

The industrial control system industry faces many challenges when it comes to cyber security and regulatory compliance. Diverse equipment, an aging workforce and antiquated security practices all come together in a perfect storm leaving critical systems vulnerable to cyber-attack. Some plants enact security controls as a best practice to protect their cyber assets, while other plants enact security controls solely to meet compliance obligations.

This article examines the challenges of compliance and security, demonstrating how two companies approached regulatory compliance and security best practices to protect their systems against threats and cyber attack.

SECURITY AND COMPLIANCE AT XCEL'S PAWNEE STATION

Xcel Energy's Pawnee Station, a 540-megawatt plant, was recently upgraded to the latest control system technology available from Emerson – Ovation 3.5.0 and Ovation Security Center (OSC) 3.0 with intrusion detection. The Pawnee station does not have compliance obligations under NERC CIP version 3. However, as a large power plant, maintaining a system with a strong security posture was very important to the organization. A team was formed to develop and implement a world-class security program.

Three drivers formed the basis of the security program at Xcel Pawnee.

1. Protect the plant, employees and local residents from any danger that could emerge from an unsecure facility.
2. Reduce or eliminate the risk of
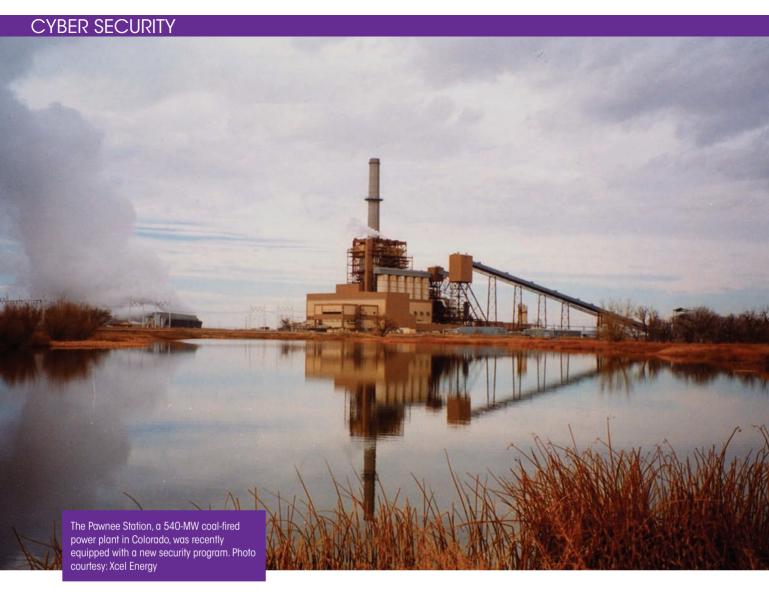
Technologies, Processes and Procedures | 1

Technologies
- Ovation Security Center
  - Antivirus
  - Patch Management
  - Whitelisting
  - SIEM & IDS
  - No external connection
- User Accounts
  - Shared by role
- Back to back firewalls
- Monthly backups
- Trusted USB drives

Processes & Procedures
- Physical security controls
- Identified interconnection rules and rules for control system connections
- Documentation requirements
- Training
- Evergreen program every 3 years

The Pawnee Station revised its processes and procedures to meet or exceed industry standard protocols for security and upgraded its technologies to support its required processes.

The Pawnee Station, a 540-MW coal-fired power plant in Colorado, was recently equipped with a new security program. Photo courtesy: Xcel Energy

attacks by outside hackers.

3. Stay out of the media.

The main challenge with developing a security program was limited funding. Because there were many other high-priority projects underway at the Pawnee station, capital dollars were hard to justify. They needed to develop the best security program at the lowest cost possible.

SECURITY PROGRAM STRATEGY AT PAWNEE STATION

The security program strategy at the Pawnee Station combines trusted technologies with specific processes and procedures.

Program Documentation

The Pawnee Station security team began by documenting the program and policies. Because Pawnee was not required to be CIP-compliant, the team avoided CIP-specific language in their documentation. Their worry was that if they used the same language as CIP, auditors would use that as justification to require the plant to become CIP compliant. They used a practical, manageable approach that avoided unnecessary wording. Program documentation is housed in a secure location and a training program has been developed for all employees who are involved in the process.

Separation of IT and OT

As they worked through the process, the team determined that there needed to be a separation between the IT department, which controlled corporate security, and the OT department, which controlled the security of the DCS network. The IT department originally wanted to control the security of the DCS. The OT group, however, was opposed to this. The resolution they agreed upon is described as "mutual distrust." They installed back-to-back firewalls using the mutual-distrust model. The IT firewall is managed and maintained by the IT group while the DCS firewall is managed and maintained by the plant operations staff, ensuring that traffic between the two networks is tightly controlled.

Tighter Control of the DCS Network

The Pawnee station maintains tight

control of the DCS. Very few people have access, and any changes must go through a specific request process.

For plant operations, Xcel prefers to setup individual user accounts although this is not always possible. Because of this, a few generic operator accounts exist. This occasionally causes issues, when different people want different configurations yet share an account.

The plant has physical security controls that prevent unauthorized access to the facility, as well as additional security that limits access to the rooms where the engineering and network equipment is stored. The Pawnee Station even regulates the use of USB drives. No outside USB drives are permitted to be used in the plant. The company provides new, approved USB drives when visitors are on site and need to transfer data. Once completed, the USB drives are destroyed. Xcel's USB program for employees deploys USB drives from Kanguru that have onboard antivirus, encryption and other features that help ensure USB sticks remain clean and are not a threat to the system.

In order to keep the control system current with the latest technology and security features, Xcel's lifecycle care program includes a system Evergreen every three years. The Evergreen program is designed to upgrade critical equipment to keep the DCS network current as technologies advance.

CHALLENGES & LESSONS LEARNED AT PAWNEE

The biggest challenge in implementing the security program at the Pawnee Station has been cultural. There was a general feeling that because the plant was not required to be CIP-compliant, implementing security protocols was unnecessary.

The team created an internal campaign to educate employees about the importance of security, even when it is not required by law. The team found that once people became more knowledgeable about the goals of the security program, they recognized its importance and became supporters.

Another challenge the team faced was related to manpower. There were not enough knowledgeable people available to do what was required to keep systems secure and updated with the latest content. There was a learning curve associated with updating the OSC which is used to implement many of the security functions identified as part of Xcel's security program. However, the team found that once they better understood how to use the OSC for tasks such as antivirus definition updates, patch management and logging, the entire process was easier and saved them significant manhours of effort. For example, the Pawnee Station has 32 workstations. Applying monthly security patches and antivirus updates to these workstations could take up to five days when done manually. Using the OSC, Xcel is able to complete this same task in only four hours.

NERC CIP regulations continue to change. Version 5 has been ratified and plants must be auditably compliant by April 1, 2016 for medium and high impact sites and by April 1, 2017 for low impact sites. Under CIP version 5 the Pawnee Station will be classified as a low impact site. The team has hired contractors to evaluate the effectiveness of the current program and compare it to what they will be required to do in the future to become compliant. Each year, the team reviews the security policy and procedures to ensure best practices continue to be followed.

SECURITY AND COMPLIANCE AT GRANT COUNTY PUD

Grant County Public Utility District owns and operates two hydroelectric powerhouses on the Columbia River in the state of Washington. In 2008, both powerhouses were listed as CIP critical assets. Grant County PUD was motivated by several factors when it came to their security and compliance program. First was their corporate philosophy to keep their plants, their employees, and local residents safe. Secondly, they had compliance obligations and wanted to eliminate any need to self-report non-compliance. Finally, they wanted to secure their Ovation system from any external threats.

In the 1990s, the two hydroelectric powerhouses were each controlled by their own Westinghouse WDPF system. When they were upgraded to Emerson's Ovation DCS in 2000 the two systems were configured such that one Ovation system controls both powerhouses. Combined, they have a generating capacity of more than 2000 megawatts.

Grant County PUD has two major control systems that need to be CIP compliant – an Alstom EMS and Emerson's Ovation for the GMS. These systems have been audited by WECC with a spot audit in 2009, a full combination 693/706 audit in 2011, and a selective 693/706 audit again in 2014.

SECURITY PROGRAM STRATEGY AT GRANT COUNTY PUD

In 2007, Grant County PUD hired a consultant to provide a basic assessment and asset inventory and to generate procedures to make them compliant for the 2009 spot audit.

A team of Process Owners was

assigned by senior management and assigned to each of the CIP standards. Those responsible for CIP-005, CIP-007, CIP-008, and CIP-009 met every Monday afternoon to work on the procedures. By the 2011 audit, many of the procedures in the original program were identified as "overkill," and were streamlined to match actual practices and still remain compliant.

The security program strategy at Grant County PUD involved a combination of technologies and processes.

TECHNOLOGY REVIEW

To help maintain compliance with the Ovation system, the Ovation Security Center (OSC) as deployed offered antivirus protection, patch management, malware white listing, and logging (SIEM). To aid product updates, the plant maintains a tightly controlled connection for downloading security content to the OSC.

User account controls are an important part of any system. Shared accounts require justification to comply with the requirements. They continue to use shared operator accounts to eliminate the need to login/logout at operation shift changes. Because the operator workstations in each control room use operator shared accounts they are able to ensure continuity of screen information and control during shift changes. The senior operator is in charge of the control room, so they always know only authorized personnel are on those workstations. They use the plant operations log to demonstrate the operator of record and to document changes in personnel. The engineers responsible for programming and maintenance use individual login IDs.

Technologies
- Ovation Security Center
  - Antivirus
  - Patch Management
  - Whitelisting
  - SIEM & IDS
  - External connection for downloading content
- User Accounts
  - Shared for operators
  - Unique accounts for engineers
- Daily backups via IT

Processes & Procedures
- Comprehensive processes and procedures
- Physical security controls
- Protected information Practices
- Document Management System
- Evergreen program every 5 years

Technologies deployed and processes implemented at Grant County Public Utility District.

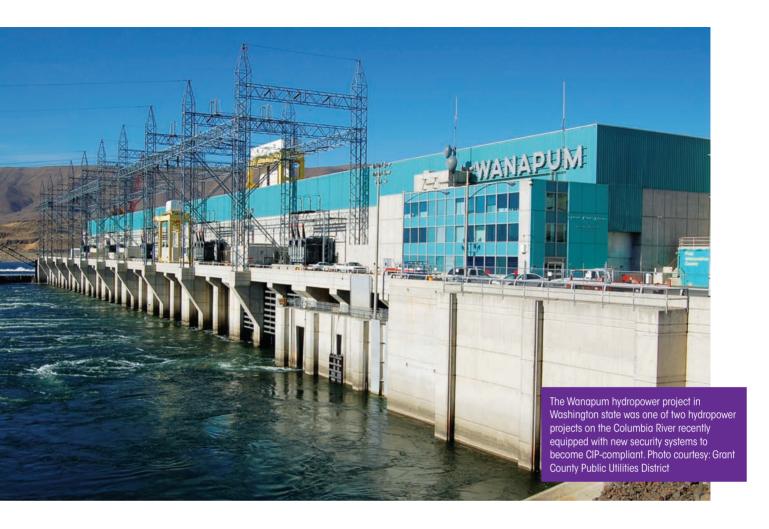## COMPREHENSIVE PROCESSES AND PROCEDURES

The procedures provided by the contractor early in the CIP effort were quite restrictive to guarantee the system was compliant. When reviewing the number of peripheral devices on the GMS network an effort was made to limit the number of cyber assets that needed to actually reside on the control network. Non-essential cyber assets, such as printers, were eliminated or moved to a DMZ area. Now printing is done to devices on the corporate network via strict firewall policies, thus reducing the number of Technical Feasibility Exceptions (TFEs) that the team had to take for the GMS. Only the Ovation controllers and workstations are listed as cyber assets in their inventory, along with very few peripherals, namely the switches. Their non-critical PLC systems and other data sources are routed through the firewall. As for the Ovation Security Center, the only component that is considered to be a cyber asset is the Security Incident and Event Management (SIEM) component.

Physical Access Controls

Grant County PUD already had physical access controls installed for all employees and contractors to enter the plant. Additional access controls were implemented to restrict entry to the controls room to meet CIP-006. There are several Physical Security Perimeters that are managed for the Ovation system. The cabinets for the controllers are secured with padlocks with unique keys that must be checked out and logged by the senior operator. The procedure requires each employee needing access to have a legitimate reason before being issued the key.

Protected Information

Within each of the four systems and several other key areas there is one person who acts as the authorized approver for anyone who wants access to that system's or area's protected information. Protected information can include structural engineering drawings of the facilities and detailed network cyber security information.

Document Management

Grant County PUD currently uses a program called Doc Minder to issue notifications to the individuals with specific assigned CIP tasks. When particular tasks are completed the individual can make comments and then notify all parties of the task completion. It is anticipated tasks will be moved to Microsoft's SharePoint application in the new future.

CHALLENGES

Manpower is a significant challenge for Grant County PUD. Those responsible for supporting CIP compliance also support the everyday operation of the production systems. On top of these responsibilities other projects would be assigned that would limit the amount of time available to devote to CIP tasks. To ensure CIP compliance one must not consider it a part time position.

Possibly the biggest challenge in meeting compliance is the collection of required evidence, especially for CIP-003 R6 and CIP-007 R. Grant County PUD made use of several freeware products to collect information from the various systems. The ability to use consistent data collection tools between the different systems simplifies the effort of providing evidence documents and reports for an audit.

LESSONS LEARNED

Grant County PUD learned several lessons through this initiative. First, they learned that it was important to have dedicated resources for cyber security. Initially, they did not realize how much time it would take to become CIP-compliant. Even on a small system, it can take a week to apply patches and generate the required evidence documentation.

Grant County also learned that even trivial information can become evidence later. Early on, they began to keep agendas of their weekly group meetings to help them stay organized. This effort ended up helping them during their first audit, as they were able to prove that they were conducting required reviews.

Moving Forward

Grant County PUD is already looking ahead. They are currently working on changes to their program for CIP version 5. Because the configuration allows them to control both plants from two locations, their system has a

medium impact rating under CIP version 5. They have begun to identify other cyber systems that will fall under the low impact rating and will then create procedures to comply with CIP-003 requirements.

They have also assigned Process Owner roles for CIP-010 and CIP-011. Processes and procedures will need to be rewritten or updated to adjust for new standards and tailored to meet new requirements. Grant County PUD hopes to be ready for transition to Version 5 by November 2015.

SUMMARY AND CONCLUSION

This case study compared two organization's approaches to Security and NERC CIP compliance. At the onset of this study we were hoping to identify and learn if securing your systems in the interest of security best practices ended in the same result as an organization securing their systems in the interest of regulatory compliance. Our case study found that while both these approaches employed similar security controls and technologies, the end results were different.

Several key questions we asked ourselves at the start of this study:
1. Does compliance ensure systems are secure?
2. Does a strong security program ensure compliance?
3. Is there a difference between security and compliance?

Understanding both approaches, we determined that compliance does not ensure systems are secured, and a strong security program does not necessarily lead to compliance. There are differences between these programs and approaches. Security-focused programs tend to be more restrictive than compliance-focused programs yet easier to maintain — compliance evidence does not need to be documented, external audits are not required, and the rigor of the program is determined by the organization. Compliance-based programs are more labor intensive due to the requirements for evidence documentation, policy documents, and paperwork. Systems can be left unsecured as long as the organization's security policies align with the regulations and the utility can document that they have been adhering to their established policies and procedures. At times, compliance can become a matter of checking a box on a piece of paper rather than securing the system to ensure it is protected from internal and external threats.

We found that both approaches share similar challenges – mainly manpower and training. As utilities downsize and workers retire, there are fewer and fewer people to manage these systems. The increased work required to secure the system and generate compliance evidence can take a toll on resources. The other key challenge identified was the need for training and expertise. It takes a different skillset to work with many of the newer security controls, software applications and appliances. This equipment, which is typically IT focused, can be a challenge for your typical I&C technician to utilize and maintain. The learning curve associated with security technologies can be steep. In order to successfully maintain the system and keep it secured and updated, training is key.

WHAT YOU CAN DO

Our recommendations for others facing these same challenges include first identifying your compliance obligations. NERC CIP regulations are changing under version 5 and every utility will need to review their systems and classify themselves into the low, medium or high impact category. This is the first and most important part of identifying how you will address security and compliance at your plant.

After you have identified your classification under NERC CIP version 5, it is important to build your program in support of compliance but also keep security best practices in mind. Implementing industry best practices for cyber security combined with a compliance-focused program ensures the security and reliability of our generating facilities and the grid.

Once your program is established, plan to review it annually to ensure it is aligned not only with the regulations, but also with industry advances in security controls, technologies and techniques.

Finally, if you are not sure where to start or where to go from here – call for help, talk to your peers in the industry, attend conferences, workshops, or working groups to get a better understanding of the NERC CIP regulations and how they apply to you, as well as a better understanding of the trends in cyber security and what you can do to ensure your systems are reliable and secure. pe