POWER
BUSINESS AND TECHNOLOGY FOR THE GLOBAL GENERATION INDUSTRY
ELECTRONICALLY REPRINTED FROM OCTOBER 2017

Tackling NERC CIP and Cybersecurity at America's Largest Gas-fired Cogeneration Plant

The Midland Cogeneration Venture (MCV) in Midland, Michigan, is the largest natural gas-fired combined electrical energy and steam energy generating plant in the U.S. It is capable of continuously producing 1,633 MW of electrical power, and in parallel producing process steam at a rate of 1.5 million pounds per hour.

The MCV (Figure 1) is a major supplier of electricity to customers in Michigan and the midcontinent, and supplies bulk process steam energy to nearby chemical production companies. The plant's first priority is to ensure safe and reliable plant operation. As cyber threats continue to intensify and become more sophisticated, protecting the plant from vulnerabilities has become increasingly burdensome.

MCV always has taken cybersecurity measures seriously, even in the absence of formal regulatory obligations. When MCV was officially classified as a medium-impact bulk generating asset under the North American Electric Reliability Corp. (NERC) Critical Infrastructure Protection (CIP) Standards Version 6, effective July 1, 2016, plant operators knew there was a need to re-examine the facility's cybersecurity.

The plant would need to comply with NERC CIP Standards 2 through 11, after having no prior NERC CIP obligations. This meant the facility needed a formal, documented process for patch management, configuration management, security event monitoring, and more. Only two people out of a staff of 120 are responsible for the control systems at the 12-plus-unit facility, and they took on the task.

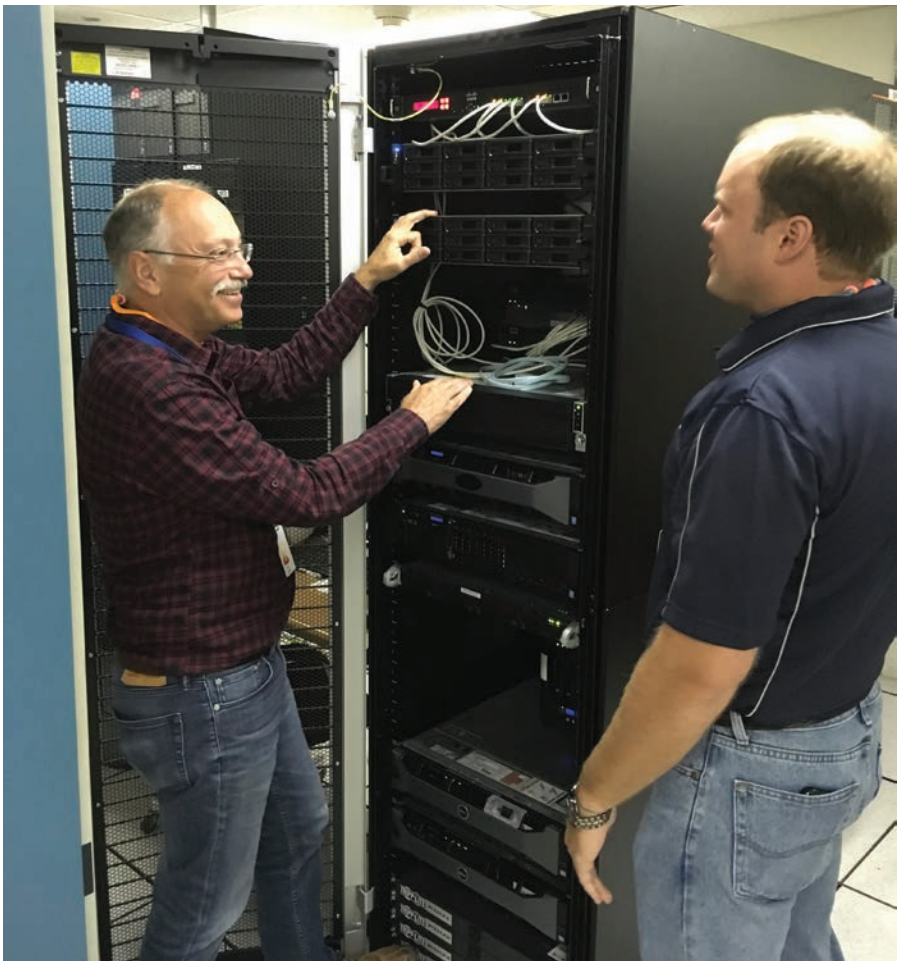
1. Serving Michigan and the Midwest. The Midland Cogeneration Venture (MCV) in Midland, Michigan, produces power and steam, supplying electricity to Michigan and other areas of the Midwest. The plant was originally designed to produce nuclear power before that project was abandoned in the mid 1980s.The facility was converted to its current use soon after, and began producing electricity in 1991. *Courtesy: MCV*

Manpower Limitations

Previously, following industry best practices, the control system operators loaded critical control system and operating system patches, which were received from plant vendors on a regular basis. However, due to manpower limitations and a desire to ensure no process interruptions, patches for third-party, less-critical software such as Adobe Reader were installed on more of an as-needed or as-time-permitted basis—anywhere from two to four times per year.

In early 2015, as the plant looked to establish a formal security program, operators initially thought it would be possible to manage compliance using some homegrown tools and tracking sheets to document the program and overall progress. There also was a brief consideration to do patch management manually. With 70 control system-related workstations, and only two people available to identify and deploy the relevant patches for each machine, logging-on, loading, and rebooting each station before moving onto the next proved unmanageable. Deploying

2. A two-man team. Scott Woodby (left) and Brandon Frost (right) are the two engineers responsible for implementing the security program at Midland Cogeneration. They worked with Emerson for months on a comprehensive cybersecurity assessment of the plant. *Courtesy: MCV*



the monthly patches in this fashion took about 45 days—so literally, there were not enough days in the month to get the work done before having to start the next month's patches. This effort did not include patching workstations on the other plant networks that were under the care of other departments. In addition to patch management duties, the two operators were also tasked with managing malware protection, annual vulnerability assessments, and configuration management—all in addition to regular distributed control system (DCS) responsibilities.

It quickly became evident there was a need to look outside for additional resources or tools to help the plant meet NERC CIP obligations. Discussions were held with several independent security consultants as well as information technology (IT)-focused businesses, each of which could offer a piece of the overall solution—one for malware protection, for example, another for backup and restore functions, yet another for Security Information and Event Management (SIEM), and so on.

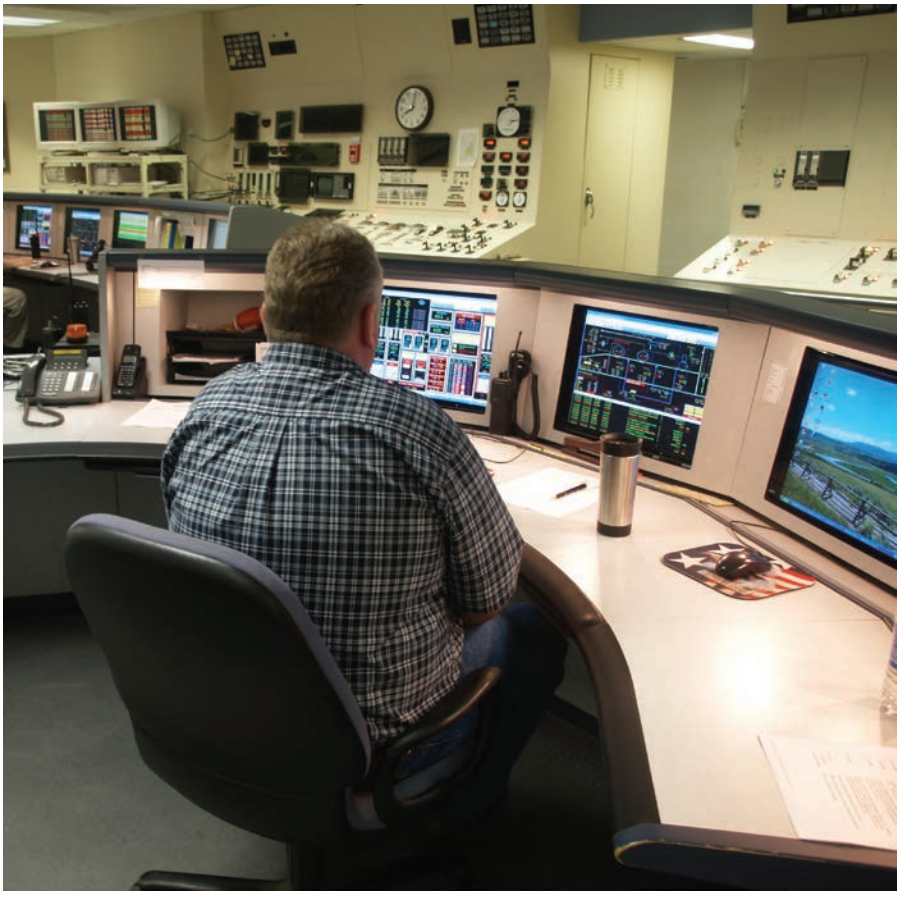
The most comprehensive solution would require working with four different companies to install four different systems that would each address a specific aspect of the plant's security program. Not only was this going to be costly, but also the burden on MCV's limited resources would still be significant. The two operators (Figure 2) would have to make sure the systems worked together, develop deployment processes and procedures, collect and sort through the various types of patches to determine which were appropriate for which systems, and test them before releasing them for install. Add to that concerns that in this burgeoning and competitive market, many of the smaller companies might not survive to support the plant over the long term, and it became clear that this was not the ideal path forward.

Customizable Cybersecurity Suite

In search of a more appropriate solution, MCV turned to the plant's DCS supplier to see what help it might be able to provide. Unlike the other suppliers, Emerson not only knew the operators, the plant, and its system, but also had for years been developing and deploying a full-featured cybersecurity suite that had many of the elements plant operators had been evaluating from other vendors. Emerson's customizable cybersecurity suite integrates hardware and virtualized software modules to provide a variety of security management functions not only for its own Ovation control system network, but also for control systems supplied by other vendors.

To address the most-pressing need, in November 2015 MCV installed Emerson's patch management module, which employs an agent-based solution that inventories software, determines patch needs in each workstation and server, and installs the patches. Standard reports document vulnerabilities, patch deployments, patch status, inventory, and trends for each individual device and at aggregated levels. MCV now uses the patch management module to push patches out to Windows-based

3. At the controls. MCV now uses a centralized, automated patch management process that allows its instrumentation and control staff to administer reboots of workstations and servers, and more closely manage the overall patch process. *Courtesy: MCV*



workstations and servers once a month. This centralized deployment allows staff to control the reboots of the workstations and servers, and more closely manage the overall patch process.

Having a centralized, automated patch management process is significantly more manageable, taking roughly one to one and a half weeks to complete—nearly 30 days faster than the previous manual process. In addition to managing the security of the primary DCS system, responsibilities have expanded to include all plant networks and equipment affiliated with plant operations, including turbines, continuous emissions monitoring system, and plant local-area network assets, nearly doubling the scope to 140 workstations and servers.

Once the automated patch process was in place, other cybersecurity modules were deployed, including configuration management, SIEM, backup and restore, and malware prevention.

Vulnerability Assessment

As a medium-impact asset, NERC CIP regulations also required conducting a vulnerability assessment once every 15 months. This entails scanning the entire system, verifying asset inventory, looking for vulnerabilities, and identifying options for mitigating them. Lacking the manpower to handle this internally, MCV again turned to Emerson, which had a dedicated cybersecurity services organization staffed by engineers with a unique combination of skills and experience in both power generation automation and IT.

MCV and Emerson shared similar philosophies about cybersecurity protection. The two agreed that the best protection for the plant required moving beyond a "check the box" mentality that aimed for nothing more than passing a compliance audit. MCV had to commit to developing a security program focused on both compliance and security best practices. This was the best approach for ensuring truly secure systems, keeping the organization compliance-ready, and maintaining production reliability.

Emerson was contracted in early 2016 to conduct a comprehensive cybersecurity assessment. The first step involved an inventory and documentation of all cyber assets (Figure 3). Armed with the facility's preliminary asset list, a team of four engineers spent two weeks physically walking through the plant—even crawling under desks to trace wires—to document the entire system down to the instrument level. As part of this process, they noted the location, asset tag, and how each component was connected to other devices and systems, both internal and external.

After generating detailed and up-to-date network topology drawings, they then used a combination of manual processes and various automated tools, including custom scripts, scanners, system registration utilities, and others, to determine the vulnerability level of each asset, identifying for example open ports and services that the individual equipment vendors didn't specify as required for operation. Using multiple tools—instead of relying on just one approach—not only helped minimize disruption to plant operations, but also made it possible to gather similar data and then compare the results to ensure accuracy.

In addition to identifying discrepancies among the tens of thousands of ports and services, they also ex-

amined the firewall state of workstations, network device firmware and configuration, audit policy and event log settings, system access controls and management of user accounts, and much more.

Final Assessment Report

Four weeks after Emerson's workers left the plant to analyze the data they'd gathered, MCV received a final assessment. The 30-page report contained specific, actionable recommendations about what to do immediately, what to do in the short term, and what to do in the long term to improve the plant's security posture and meet NERC CIP obligations.

The assessment criteria were derived from NERC CIP requirements, Emerson recommended best practices and industry standard benchmarks, organized into nine categories: architecture and topology; asset identification and classification; malware prevention; network device hardening; patch management; ports and services; security and event monitoring; system access controls; and vulnerability assessment. Each finding within those categories was ranked by severity level representing the relative security, compliance, and reliability risks to MCV's systems—low, medium, high, or critical. About 52% of the findings fell into the critical/high-priority categories, and the remaining 48% into the medium- or low-priority categories. Each finding was followed by one or more actionable recommendations as well as a notation on whether an outage would be required to implement them.

Recommendations included removing or rerouting specific external-facing communications, setting up electronic access points, hardening specific network devices, disabling unnecessary services, upgrading GPS firmware, updating asset tag naming conventions, and more. The report also contained a NERC CIP status matrix, enabling MCV to clearly see any compliance gaps and keep track of progress toward meeting them.

Over the past 12 months, MCV has acted to mitigate all the initial, high-priority findings while proactively budgeting for and scheduling implementation of some of the remaining, lower-priority findings. Its team is now preparing for a second cybersecurity assessment, which is expected to document a much-improved security posture over the earlier baseline. Because cybersecurity threats are always evolving and plant systems rarely remain static, MCV engineers expect there will be some new findings as well. No plant will ever be 100% secure, but the group is confident that the facility is making good progress and will continue to use the assessments as a roadmap for year-over-year improvement.

This approach is just one for tackling NERC CIP requirements and overcoming the challenges of having to secure a large system with very limited resources. Help from the control system vendor, along with cooperation from MCV's internal team, enabled development of a solid cybersecurity program that not only enables the plant to meet compliance obligations but also focuses on best practices to ensure reliable plant operation, all without the need for additional staff. ■

*—**Scott Woodby** is manager of engineering at MCV and **Brandon Frost** is instrumentation and control engineer for MCV.*