Protecting Critical Infrastructure and Cyber Assets in Power Generation and Distribution

Embracing standards helps prevent costly fines and improves operational efficiency

Bradford Hegrat, CISSP, Principal Security Consultant
Clark Case, Logix Software Product Manager, Rockwell Automation

With access to power – namely electricity – considered as one of the basic requirements for modern society, it's hard to believe that there once was a time when access to electricity was a luxury reserved only for the wealthy.

Access to consistent, reliable power is so important that the U.S. Government has made it a priority to assure that it's protected from physical and cyber threats – natural or intentional. Regulations put in place by the Federal Energy Regulatory Commission (FERC) are quickly moving toward final adoption, and they have far-reaching implications for companies involved in power generation and distribution. Staying ahead of these regulations can prevent costly fines, but the silver lining is that preparing for them can help identify ways to improve operational efficiency. Rockwell Automation takes a blended approach to helping companies embrace and comply with these new standards through a combination of advanced control and information systems, and industry experience and consultation.

FERC, NERC and Emerging CIP Standards

The Federal Energy Regulatory Commission (FERC) regulates the interstate transmission of electricity, natural gas, and oil. One of those regulatory responsibilities is to ensure the reliability of high-voltage interstate transmission systems. Formed in 1968, the North American Electric Reliability Corporation (NERC) is a voluntary consortium of power companies that takes the reliability standards set by FERC and helps companies execute plans to ensure the reliability and availability at a regional level. FERC sets reliability standards for all types of energy while NERC helps member electric companies translate how those standards apply to them.

While power companies have had safeguards to protect physical and human assets in place for some time, the emergence of new technologies that allow for long-distance control and information sharing within the power infrastructure has created the possibility of threats coming from the Internet rather than the physical world.

In order to continue its mission, NERC developed a set of enforceable reliability standards that must be followed by companies responsible for the reliability and availability of the Bulk Electric System (BES) in North America. The standards specifically pertaining to the identification and protection of Cyber Critical Assets are known as the NERC Critical Infrastructure Protection (CIP) standards, more commonly referred to as NERC CIP standards.

Cyber Critical Assets are the devices used to support the day-to-day operation of Critical Assets and the distribution of electricity to the BES. A Critical Asset is one which is necessary to maintain the reliability of the BES, such as a generating unit with blackstart capacity (i.e. a unit that does not require a secondary power source for initial startup purposes). Guidelines for identifying Cyber Critical Assets are contained in the NERC CIP standard CIP-002-1. A broad majority of companies do not recognize that they own or operate Critical Assets, at least when it comes to complying with the NERC CIP standards. When NERC completed its 2009 self-certification compliance survey for CIP-002-1, it found that less than one-third of generation owners and operators had identified at least one Critical Asset within their facilities.

The primary reason for the low number of Cyber Critical Assets identified by generation owners is the ambiguous language used in NERC-CIP-002-1. This is currently under review and revision by NERC and FERC.

Investments to meet NERC CIP standards could significantly increase operating budgets which in turn will drive costs and power prices upward. This is a real concern for generation owners as their market evolves toward a “Smart Grid” requiring them to be the “low cost” power provider. However, sanctions for noncompliance to the NERC CIP standards are also significant, with fines reaching up to $1 million per day. Finding a clear path amidst the confusion is critical for generation owners. The end result will reach beyond simply checking off another box in a long regulatory checklist. Reaching an appropriate balance of the investment needed to be competitive while simultaneously complying with NERC CIP is essential and will dramatically influence the growth or loss of the generation owner’s customer base.

A brief overview of NERC CIP

There are key resources, which can be publicly or privately controlled, that are essential to the minimal operations of the economy and government. These are collectively known as the Critical Infrastructure. The power generation and distribution system makes up an important part of the Critical Infrastructure. In order to protect this portion of the Critical Infrastructure, NERC developed the NERC CIP standards. The primary objective of the NERC CIP standards is to help assess the reliability of each facet within the power infrastructure, evaluate power companies’ preparedness in the face of an attack or unplanned interruption of operations, and to continue education and awareness for employees of these companies. As defined by NERC, Critical Infrastructure Protection covers “the assets, systems and networks, whether physical or virtual, considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof.”

The NERC regulations boil down to eight standards. At Rockwell Automation, we've found greater simplicity and speed in the compliance process by dividing these eight standards into three groups.

Plan to protect your Cyber Critical Assets.
CIP-003-1, -007-1, -008-1, and -009-1 all offer guidance on how to secure individual assets within a system. These standards include requirements for identifying the owners of cyber critical assets and for documenting exceptions to those cyber critical assets. They also have requirements for applying standards that protect the information associated with those assets and similarly include an annual evaluation of managing these security controls. Maintaining these security standards is also defined within this set of four standards, as are guidelines for reporting and responding to a system threat and recovery recommendations in the event that a company loses access to an asset.

Know what you've got and where it is
With CIP-002-1 and -005-1, the most important step companies can take is to understand what Critical Assets exist within a system, and what cyber critical assets are essential to the operation of those Critical Assets. Examples can include systems and facilities at master and remote sites that provide monitoring and control, real-time power system modeling, and real-time inter-utility data exchange. With those assets identified, companies must then ensure and document that every cyber critical asset resides within an electronic security perimeter. This perimeter needs to include electronically monitored access control, as well as an annual review of the perimeter's cyber vulnerability.

Tend to the physical security of your assets.
While many already have addressed physical security, CIP-004-1 and -006-1 standards direct companies how to create and maintain a physical security plan that complements the cyber security measures already in place, with requirements for documenting physical access controls. Additionally, these standards address the need to ensure that companies have proper screening processes in place for hiring personnel, and that all employees are aware of the security measures used and are trained on how to use them.

Implications of NERC CIP noncompliance

In an industry that's already regulated, the introduction of new standards always prompts a review of how these standards will affect or change current operating systems. From an operations standpoint, these standards mean more systems testing and more paperwork — unwelcome news to companies operating with margins that are already stretched thin. In addition, the standards also will have an impact on how control systems are put together to ensure compliance is maintained during system upgrades or expansions.

Yet, the imperative for understanding how compliance applies, and documenting how systems are in compliance, is clear in how violations are reported and sanctions are meted. Once an incident of noncompliance is confirmed by NERC, it is posted to a public forum where it is widely accessible. Companies found in noncompliance are required to submit a mitigation plan detailing how it will be brought back into full compliance. Fines are then assessed to the company based on calculations involving the timeframe of the violation; whether repetitive violations were recorded; any failure to comply with compliance directives; if the violation was intentional or if company representatives attempted to conceal the violation; how cooperative the company was during the investigation; any self-disclosure or voluntary corrective actions undertaken by the company; and other extenuating circumstances. Fines start at $1000 per day, and can go up to $1,000,000 per day for the most blatant and egregious violations.

As is the case with many regulatory standards, compliance can be both a burden and a boon. Generally speaking, it's sound business sense to regularly evaluate your systems, identify potential weaknesses within those systems, and take steps to strengthen those areas. While avoiding fines may motivate some, there are other business benefits to consider. For example, while power companies design their systems to optimize efficiencies and maintain continuous operations, these standards reinforce a sound practice of regularly reviewing critical systems for any potential vulnerabilities and addressing them before they create an interruption of service or are used as an inroad for some malicious act. This encourages operations directors to reduce the number of unknowns that can compromise the stability of a power control system. Avoiding system downtime means avoiding the costs associated with bringing the system back up and compensating for the interruption of service.

Rockwell Automation Can Help

Having taken that critical first step in defining your cyber critical assets, finding the most efficient way to achieve and document your company's compliance and avoid NERC sanctions is the next. At Rockwell Automation, we already offer the solutions and services that help you fulfill the NERC requirements.

Rockwell Automation Network & Security Services can help companies at any point in their progress toward NERC CIP compliance. Our converged team made up of manufacturing engineers and IT professionals collaborate with you to help manage the differences between manufacturing and IT enterprises and their associated risks. This can be done not only through technology, but also through policies, procedures and behavior — allowing you to achieve your production and business goals. Our consultants consider where you are in your control system or security lifecycle, and develop a plan to help improve system reliability and increase overall equipment effectiveness.

From a product perspective, two system-oriented offerings in particular can help you meet NERC CIP requirements – Rockwell Automation FactoryTalk® Security and FactoryTalk AssetCentre.

The FactoryTalk Services Platform is embedded in all control and information products from Rockwell Automation including RSLogix, PlantPAx™, FactoryTalk View, FactoryTalk Historian, FactoryTalk Asset Centre. The FactoryTalk Services platform provides a centralized role based access control system through a software service called FactoryTalk Security. The FactoryTalk Security architecture is similar to that of Microsoft Windows and provides many of the same capabilities, plus additional features customized specifically for the needs of automation systems. FactoryTalk Security controls user access to applications and devices and provides user authentication and authorization. Using FactoryTalk Security can help you address several of the NERC CIP requirements. For example:

- CIP-004-1 R4.2 calls for revoking access to Cyber Critical Assets within 24 hours for personnel that have been terminated. With FactoryTalk Security, an administrator can revoke access to software products and devices immediately.
- CIP-007-1 R5 contains several requirements in the area of Account Management. With FactoryTalk Security, you can meet all of these requirements.

FactoryTalk AssetCentre provides you with a set of asset-centric focused tools to securely and centrally manage your factory and process automation production environments by tracking users' actions, managing asset configuration files, and providing backup and recovery of operating asset configurations. With these capabilities, compliance with many CIP requirements is much easier. For example:

- CIP-003-1 R6 requires a comprehensive change control and configuration management process. FactoryTalk AssetCentre can be a key technical part of such a process. FactoryTalk AssetCentre has add-ons which support Calibration Management and Process Device Configuration. The Calibration Management capability allows for a paperless calibration solution: managing calibration requirements, specifications, schedules, calibration results and reporting. Process Device Configuration allows you to access instrument parameters, aids in configuration and commissioning process devices and helps with diagnostics. Acting as a host system, or frame application, it gives you the ability to work with multiple vendors' instruments in one common platform.
- CIP-009-1 R4 calls for a recovery plan to restore Cyber Critical Assets to operation. Configuration backup and recovery is a core feature of FactoryTalk AssetCentre, and can help make this plan much easier to execute. FactoryTalk AssetCentre provides control system backup that is integrated with source control to provide reliable and easy access to the latest control system configuration file. Both Rockwell Automation and third-party assets are supported.

Rockwell Automation provides information and solutions that help you meet other requirements as well.

- A list of TCP and UDP ports used by Rockwell Automation products is maintained on our Knowledgebase, helping you meet CIP-007-1 R2, "Ports and Services".
- All TechConnect℠ subscribers can access results of the Rockwell Automation Patch Qualification process, in which Microsoft operating system patches are tested for compatibility with Rockwell Automation software products. Using this service can help you meet CIP-007-1, "Security Patch Management".

Make the most of compliance measures

The companies who move the fastest to meet compliance will not only avoid sanctions and fines, but also offer customers the added assurance that comes with regular security reviews. They can help ensure the reliability and availability of the power needed to serve homes and businesses throughout the country. Partnering with Rockwell Automation can help you protect your ability to generate and distribute the valuable energy resource. Additionally, Rockwell Automation can simultaneously help you comply with key government standards and regulations designed specifically to protect critical assets on which the United States critical infrastructure relies.

To learn more about Rockwell Automation's capabilities to address your compliance needs, visit http://www.rockwellautomation.com/security. Here you will find information regarding our security products and services, including a link to our Network & Security Services consultancy.

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication ENET-WP020A-EN-P – July 2010