POLICY UPDATE

The Federal Energy Regulatory Commission's (FERC) proposal for the NERC CIP standards

The FERC has issued a Notice of Proposed Rule-making (NOPR) to the North American Electric Reliability Corporation (NERC) to develop new regulations for the Critical Infrastructure Protection (CIP) standards that may affect most power utilities in North America and beyond.

SIEMENS

Introduction

The incidence of advanced, successful cyber attacks on critical infrastructure organizations in the United States has led regulatory authorities to explore issuing new security-related mandates on the electric power industry.

The Federal Energy Regulatory Commission (FERC) has issued a Notice of Proposed Rulemaking (NOPR) that may affect most power utilities in North America and beyond.

Utilities, which will be impacted by these developments, should consider acquainting themselves with the proposed cybersecurity requirements and plan ahead to prepare their internal processes and security infrastructures to meet any new compliance requirements in time.

FERC's mandate is to oversee the "reliable, safe, secure, and economically efficient energy for consumers at reasonable cost," thus its role is to respond to cyberattacks, which ultimately threaten reliability, safety, security, efficiency, and cost. A NOPR is the U.S. federal government's process for announcing and explaining an executive branch or independent agency's plan for addressing a challenge or accomplishing a goal through the rule-making process.

In a 20 January 2022 NOPR, FERC asked the North American Electric Reliability Corporation (NERC) to develop new or revised regulations under the latter's Critical Infrastructure Protection (CIP) program to mandate the protection of "trusted networks" within electric power substations.

Specifically, FERC directed NERC to "develop and submit ... new or modified Reliability Standards that require Internal Network Security Monitoring (INSM) within a trusted Critical Infrastructure Protection networked environment for high and medium impact Bulk Electric Cyber Systems."

It appears that FERC's proposal was partially motivated by a relatively new and potentially damaging style of cyberattack. This novel type of cyberattack appears to have bypassed current utility cyber defense practices by posing as authorized staff or vendors and acquired access to the trusted networks within substations. As FERC articulated the issue in its NOPR: "Under existing CIP reliability standards, network security monitoring is focused on defending the electronic security perimeter of networks. FERC is seeking to address concerns that the existing standards do not address potential vulnerabilities of the internal network to cyber threats... INSM addresses situations where vendors or individuals with authorized access that are considered trustworthy might still introduce a cybersecurity risk."

> Under existing CIP reliability standards, network security monitoring is focused on defending the electronic security perimeter of networks. FERC is seeking to address concerns that the existing standards do not address potential vulnerabilities of the internal network to cyber threats... INSM addresses situations where vendors or individuals with authorized access that are considered trustworthy might still introduce a cybersecurity risk.

Potential impacts of FERC's NOPR

We expect FERC's directive to NERC to produce proposed changes to NERC CIP mandates that will affect regulated utilities and force currently unregulated utilities under the CIP regulatory umbrella. Utilities in countries that voluntarily adhere to the United States' NERC CIP Reliability Standards are expected to subsequently adopt new best practices for cybersecurity.

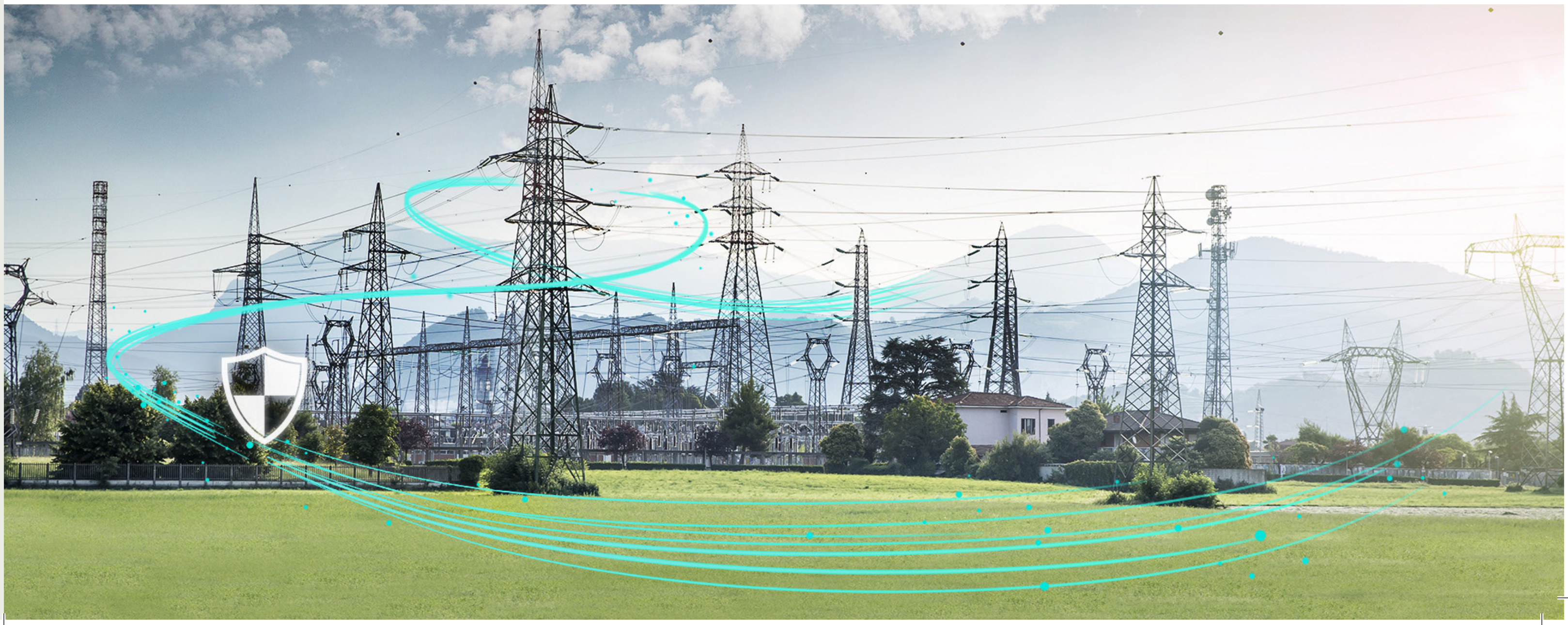
According to FERC, incorporating INSM requirements into the CIP Reliability Standards to modify existing requirements for perimeter-based network protection would help utilities maintain visibility over communications in their internal trusted networks. The language of FERC's NOPR appears to address errors with unintended consequences by authorized staff and vendors, in addition to guarding against malicious attacks.

From a purely technical standpoint, new INSM requirements can support utility efforts to swiftly detect an attacker's intrusion into a trusted network. This will provide enough time to identify, locate, and isolate the malware before it can compromise the internal network operations and impact the Bulk Electric System (BES). Adopting INSM for your OT network can detect vulnerability in your network. And by isolating a cyberattack, an INSM can also speed up system recovery.

The NOPR process

In response to an FERC NOPR, NERC typically forms a subcommittee that evaluates and articulates potential changes to CIP requirements and produces proposed language for FERC's approval. Historically, this process has taken from months to years to finalize. As a result, the timeframe from NOPR issuance to approved regulatory changes to compliance deadlines can be unpredictable.

Utilities that seize the opportunity to anticipate regulatory changes and develop a response strategy will be well-positioned to achieve compliance and, most importantly, enhanced cybersecurity. Moreover, for utilities outside North America not subject to NERC CIP that model their cybersecurity approach on its requirements, a similar opportunity exists to improve cybersecurity practices.



Expected NERC CIP changes and impacts

The specific cyberattack that likely prompted FERC's NOPR penetrated an IT vendor's trusted internal network by posing as the actions of an authorized party. The IT vendor then delivered a periodic, scheduled software update to thousands of its clients, which included government agencies as well as private sector businesses. However, this software update contained surveillance software that embedded itself within the trusted networks of the IT vendor's clients. Thus, the initial attack falls within the scope of supply chain risk management, addressed by CIP-013. So, NERC might review CIP-013 for new or revised requirements to prevent a similar attack in the future.

Perhaps of greater concern to power utilities in particular is that FERC is also asking NERC to address how the initial attack affected end users of software updates from the original, compromised vendor. In that case, NERC will likely address new or revised requirements for networks at the edge, such as the entry point to the trusted Local Area Networks (LAN) within a power substation. For example, suppose there's a protection relay or Human-Machine Interface (HMI) in the substation. A malevolent cyber intrusion could compromise the entire substation without involving the control center and triggering the latter's perimeter-style defenses.

Who needs to act

Currently, if a utility's power grid network is interconnected with the transmission system in the U.S. – which includes several utilities based in Canada and Mexico – and a failed asset can impact the Bulk Electric System within 15 minutes, it falls under NERC CIP rules. NERC CIP further classifies utilities by whether they can have a high or medium impact on the nation's grid. Medium-impact utilities with External Routable Connections (ERC) are typically the intended focus of NERC CIP requirements. But those requirements also apply to medium-impact utilities with no ERC and utilities with low-impact substations. (See NERC's definitions and rules regarding ERC.)

The most probable outcome of FERC's NOPR is that, even though a utility currently doesn't fall under the rules for high- or medium-impact utilities with ERC, new NERC CIP requirements may be expanded to include most utilities' Operational Technology (OT) networks.

How Intrusion Detection Systems (IDS) address the challenge

Protecting trusted OT networks to ensure business continuity requires a non-intrusive, cost-effective solution with a minimal footprint. FERC's NOPR essentially signals that if a utility's assets include a substation classified as having a high or medium impact with ERC, management will need to review the need for an Intrusion Detection System (IDS). There's a possibility that power utilities currently not facing NERC CIP mandates will also need to deploy an IDS in their network. IDSs have been on the market for years, and their effectiveness continues to evolve to address evolving threats. A properly designed and implemented IDS can monitor trusted networks at the edge and respond to intrusions in timeframes that pass muster with pending regulatory revisions.

Power utilities should consider implementing an IDS that can deliver several vital results and functionalities, including:

- Achieving compliance with NERC CIP requirements and security standards, such as IEC 61850-3, IEEE 1613
- Providing comprehensive asset inventories and an ability to prioritize the protection of vulnerable assets
- Real-time visibility to detect anomalies in the network and reduced time for troubleshooting
- Minimizing impacts without compromising network efficiency
- Automation with context-based alerts if human intervention is needed

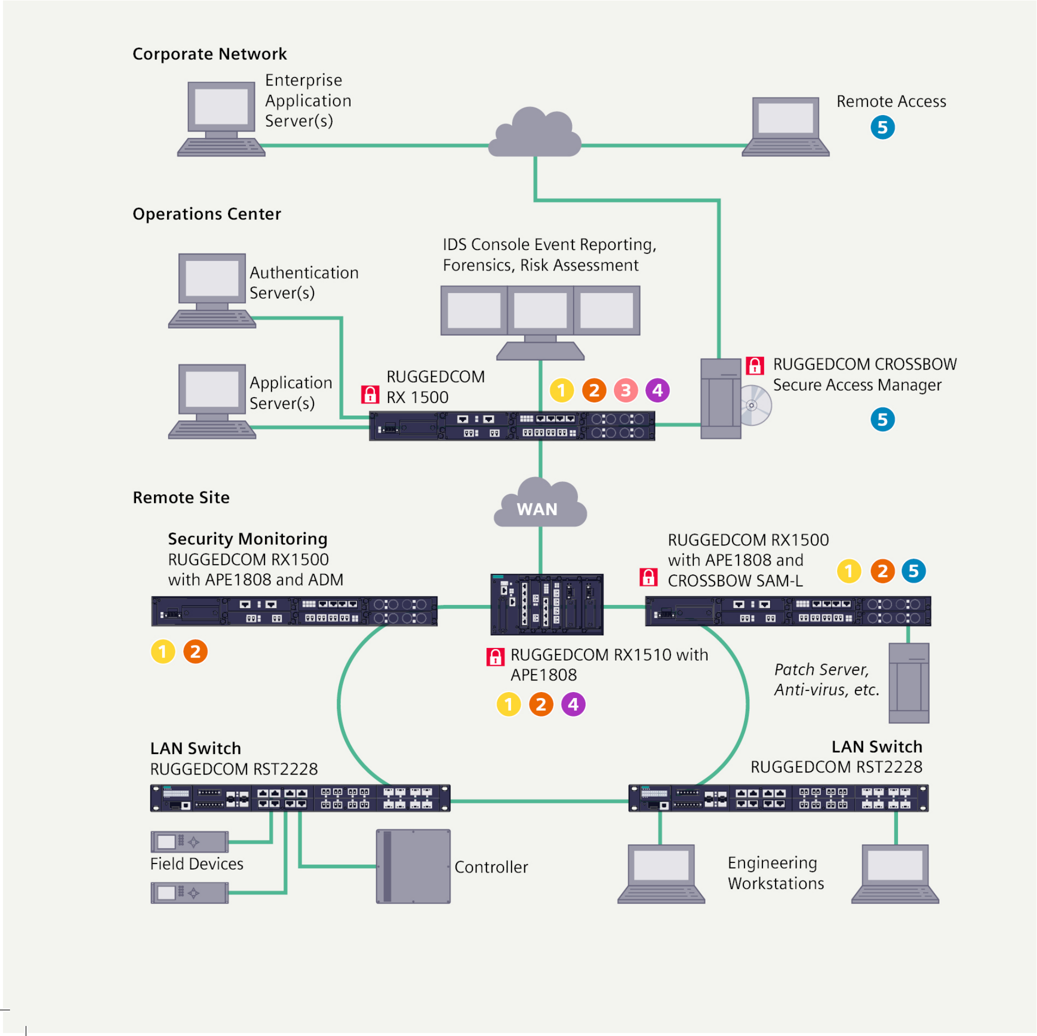
How we can help

As a globally trusted expert in designing, building, and protecting industrial networks, Siemens works with certified cybersecurity partners to test different IDS solutions to meet diverse client challenges. Siemens' unique contribution is its deep experience in designing and implementing software and hardware purpose-built for harsh industrial environments at the network's edge, such as electric power substations.

There are numerous diverse IDS solutions on the market. However, these solutions need to be deployed on reliable hardware platforms that can withstand harsh environments in order to perform to their fullest potential for mission-critical applications.

Siemens' utility-grade, IEC 61850-3 compliant RUGGEDCOM Multi-Service Platforms deliver reliability in environments with high resistance to Electro-Magnetic Interference (EMI) at operating temperatures between –40 °F and +185 °F (–40 °C to +85 °C). Our partners' IDS software is deployed on our industrial application processing engine (RUGGEDCOM APE1808), a line module of the RUGGEDCOM layer 2 and layer 3 Multi-Service Platforms – siemens.com/rx1500

Installation and operation of Siemens' integrated hardware and IDS software solutions are non-intrusive with zero disruption to ongoing operations. The hardware is built as a software-agnostic modular platform, offering the flexibility of easily upgrading to the latest software without changing the hardware. This reduces Capex investment and training expenses and further reduces the total cost of ownership of the integrated solution.


Corporate Network
Enterprise Application Server(s)
Remote Access
5
Operations Center
IDS Console Event Reporting, Forensics, Risk Assessment
Authentication Server(s)
Application Server(s)
RUGGEDCOM RX 1500
1 2 3 4
RUGGEDCOM CROSSBOW Secure Access Manager
5
Remote Site
WAN
Security Monitoring
RUGGEDCOM RX1500 with APE1808 and ADM
1 2
RUGGEDCOM RX1500 with APE1808 and CROSSBOW SAM-L
1 2 5
RUGGEDCOM RX1510 with APE1808
1 2 4
Patch Server, Anti-virus, etc.
LAN Switch
RUGGEDCOM RST2228
LAN Switch
RUGGEDCOM RST2228
Field Devices
Controller
Engineering Workstations

🟩 Industrial Ethernet

1 Anomaly-based Intrusion Detection System (IDS)

2 Deep Packet Inspection (DPI)

3 Intrusion Prevention System (IPS)

4 Next Generation Firewall (NGFW)

5 RUGGEDCOM CROSSBOW – Secure Access Control

This generic industrial control system diagram illustrates the role and placement of Siemens' RUGGEDCOM integrated IDS solutions, which operate on RX1500 platforms designed for harsh industrial environments. The RX1500 platforms host a compact application processing engine (APE1808) that drives our partners' IDS applications.

Let’s talk!

Siemens’ globally experienced Professional Services staff can support and guide your assessment of how NERC CIP requirements may change, how that impacts your organization, and ensure that your trusted networks are effectively protected and compliant with regulatory mandates. The answer to the myriad challenges your utility faces is to engage with a trusted advisor and single-source solution provider with a legacy of designing, building, and protecting OT networks.

Every power utility has a unique topology and individual cybersecurity needs. Siemens provides deep expertise and global experience in meeting regulatory mandates through the comprehensive protection of your power networks for business continuity. Give us a call today to explore how we can support your ongoing efforts to comply with federal regulatory requirements and enjoy operational reliability and cybersecurity.

To learn more about how you can position your organization to stay ahead of FERC’s proposed rule for utilities, please give me a call.

Jeff Foley
Chief Technology Evangelist for Cybersecurity
Siemens Digital Industries
Mobile: +1 (954) 296 5648
Email: jeff.foley@siemens.com

About Siemens Digital Industries
Siemens Digital Industries (DI) is an innovation leader in automation and digitalization. Closely collaborating with partners and customers, DI drives the digital transformation in the process and discrete industries. With its Digital Enterprise portfolio, DI provides companies of all sizes with an end-to-end set of products, solutions and services to integrate and digitalize the entire value chain. Optimized for the specific needs of each industry, DI’s unique portfolio supports customers to achieve greater productivity and flexibility. DI is constantly adding innovations to its portfolio to integrate cutting-edge future technologies. RUGGEDCOM hardware and software products are part of the Siemens Digital Industries portfolio. They provide a level of robustness and reliability that have set the standard for communications networks deployed in harsh environments. Siemens Digital Industries has its global headquarters in Nuremberg, Germany, and has around 76,000 employees internationally.
To learn more, visit www.siemens.com

For more information, please visit:
siemens.com/ruggedcom

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Germany

Siemens Canada Limited
300 Applewood Crescent
Concord, Ontario, L4K 5C7
Canada

Subject to change without prior notice
Article No. 6ZB5531-0BE02-0BA0
Dispo 26000
BR 0722 0 PoD 8 En
Printed in Germany

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit: **siemens.com/industrialsecurity**

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends to apply product updates as soon as available and to always use the latest product versions. Use of product versions that are no longer supported, and failure to apply latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under: **siemens.com/industrialsecurity**

The information provided in this brochure contains descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice. All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.