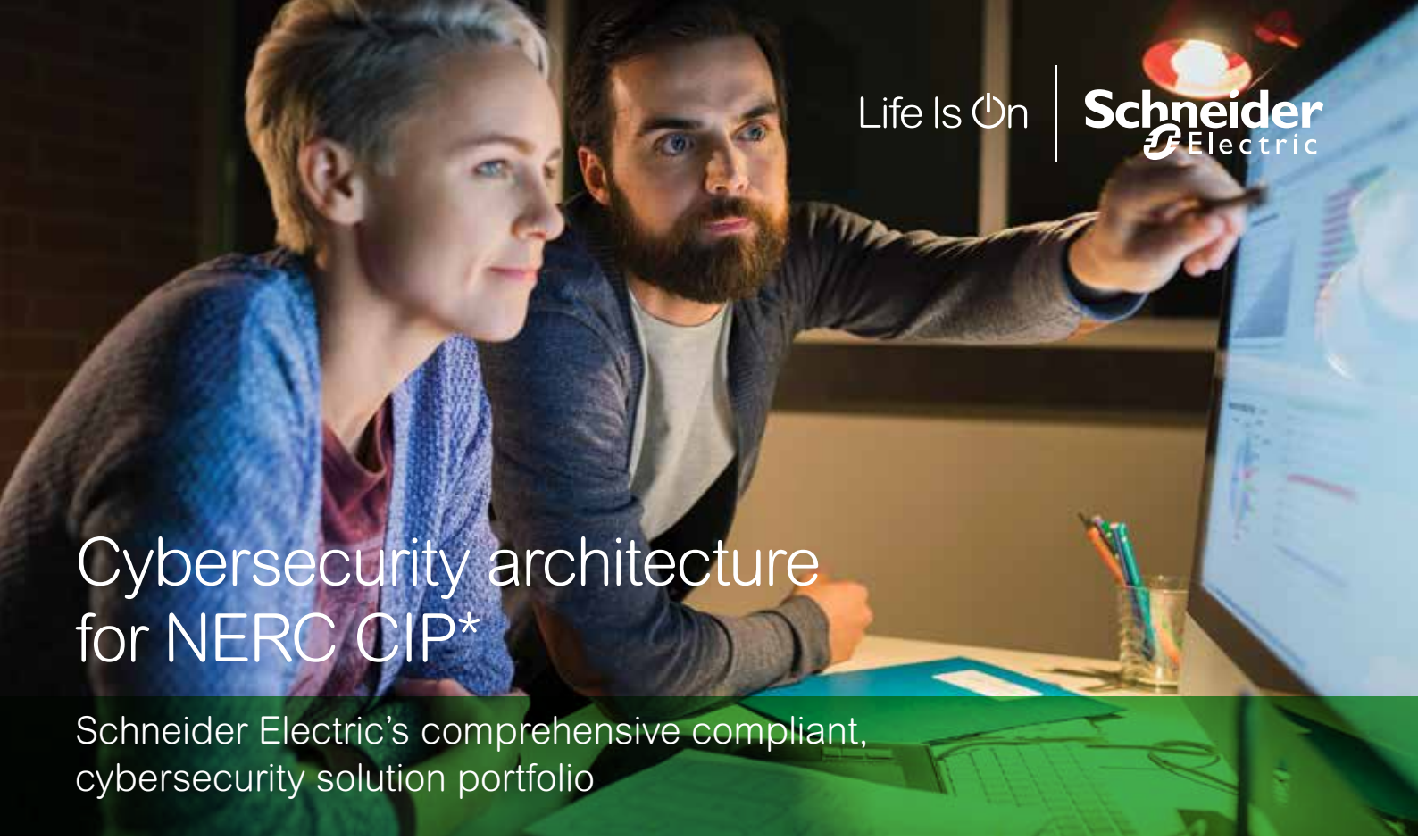


Life Is On | Schneider Electric

Cybersecurity architecture for NERC CIP*

Schneider Electric's comprehensive compliant, cybersecurity solution portfolio

Product at a glance

The power generation industry must become compliant with NERC CIP regulations; otherwise it risks significant fines and penalties. The Schneider Electric cybersecurity team helps you become compliant and meet your deadlines through staff augmentation and a comprehensive portfolio of cybersecurity services.

Our cybersecurity portfolio solution is unique in its platform-independent lifecycle methodology, which integrates seamlessly between manufacturing operations and corporate IT networks.

NERC CIP basics

Compliance with NERC CIP cybersecurity standards requires identifying critical assets, performing detailed assessments, outlining remediation steps, and maintaining the network for the lifecycle of the system. All of these tasks put a burden on resources that are already thinly distributed.

The challenge for any operator is to develop a cybersecurity program that aligns with the NERC CIP standards. The eleven major NERC CIP standards can be organized into three primary work groups:

- Electronic security (CIP-002, CIP-003, CIP-005, CIP-007, CIP-008, CIP-009, CIP-010, CIP-011)
- Physical security (CIP-006, CIP-014)
- Personnel & training (CIP-004)

*North American Electric Reliability Corporation, Critical Infrastructure Protection

Cybersecurity architecture for NERC CIP

Schneider Electric's comprehensive, compliant cybersecurity solution portfolio

Four tenets of compliance

The Schneider Electric cybersecurity team has developed a comprehensive cybersecurity-compliant portfolio of solutions that takes a holistic approach to cybersecurity based on the four tenets of critical infrastructure compliance:

1. Information security
2. Physical security
3. Plant safety
4. Business continuity

Power generation plants must become compliant or face stiff fines and penalties that can reach up to $1 million per day.

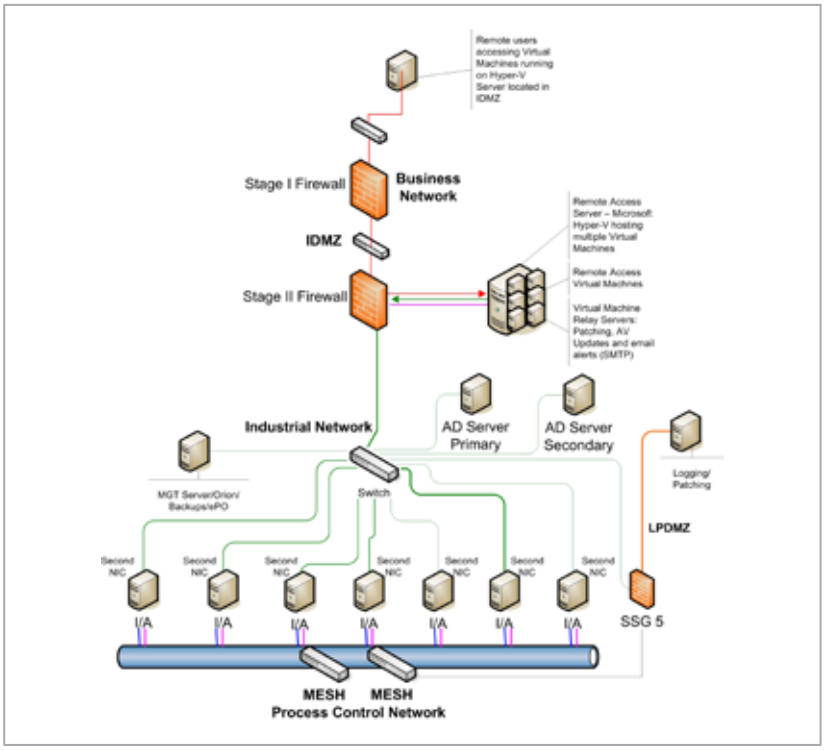
Architecture

Initially, you must look at the current first-generation network deployments. These control networks are typically layered between the IT corporate network and control networks, resulting in an ad hoc control network.

Our cybersecurity team addresses the control network that lies between business systems and the process systems. This defines the second-generation networks. We work with operators to properly assess their first-generation networks — to identify gaps in compliance and provide a remediation plan. Afterwards, a network solution is deployed that addresses the operators' unique system requirements, but meets the goals of NERC CIP compliance.

These second-generation networks will provide the operator with more traffic and security controls, including:

- Access controls — multiple secure zones
  - Centralized management
  - Backups
  - Antivirus management
  - Patch management
  - Event management
- Network performance monitoring and historical data and reporting
- Active directory access controls
- Secure remote access relay server



Cybersecurity architecture for NERC CIP

Schneider Electric's comprehensive, compliant cybersecurity solution portfolio

Cybersecurity methodology

Schneider Electric's solution is based on a lifecycle management methodology. This methodology can be applied to any system, regardless of the existing lifecycle of the network.

In addition, our security solution is completely network-agnostic, working with any process control safety system in the field. Our security lifecycle methodology is based on four independent service elements. Each service element complements and builds on the other.

Cybersecurity solutions portfolio

Schneider Electric defines the lifecycle of any networked system as four distinct stages, each of which has a separate solution for each technology area. These solutions are the roadmap to your plant's efficiency.

Security assessment —
We assess your current network, identify problems or issues, and suggest areas that require improvement.

Security architecture and policy development —
Utilizing an assessment plan as guidance, we identify what elements need to be implemented and develop a detailed design.

Security modernization and implementation —
At this stage, we transform the network design into reality, from procurement to staging and commissioning.

Security management and optimization —
We get involved in the management of the network and provide a mechanism to improve and optimize the network as it continuously evolves with usage.

The Schneider Electric cybersecurity solution portfolio will help achieve regulatory compliance.

Schneider Electric

70 Mechanic Street
Foxborough, MA 02035 USA
+1 877 342 5173

schneider-electric.com/processautomation

Life Is On Schneider Electric