



SOC as a Service – Cyber Secure Substations

November 2022

Confidential © Siemens 2022

Siemens.com

SIEMENS

Market for SOC as a Service

- SOC market is fragmented with several security vendors, services vendors, and telecom providers competing for larger market share.
- SOC service models include:
 - In-house
 - Hybrid
 - Fully outsourced
- Trends market research report predicts that the Security Operations Centre market revenue is estimated to be:
 - \$31,796.9 million in 2019
 - Expected to reach \$61,199.7 million by 2025,
 - Growing at a CAGR of 11.5% during the forecast period 2019–2025.

Critical Infrastructure Defense Center

SOC as a Service

Siemens Introduces

The Siemens Critical Infrastructure Defense Center (CIDC)

- SOC is a dedicated monitoring and protection platform
- For critical infrastructure services industry and large manufacturing



SOC is the first and only dedicated Operational Technology (OT) Security Operations Center (SOC) in NA



SOC services are one of our core specialty offerings provided by **Siemens Critical Infrastructure Defense Center (CIDC)** under our **Security Operations** portfolio of Cybersecurity services

Critical Infrastructure Defense Center

SOC as a Service

SOC as a Service Models

- **Enterprise SOC:** is a dedicated monitoring and protection platform within the CIDC
- **Cloud SOC:** Hosted in the cloud this model is intended to interface with the client's on-premise SOC
- **Out-Sourced SOC:** Siemens will provide Out-sourced SOC Services for Clients who want to focus on core business activities

Siemens will support Client's cybersecurity requirements through dedicated SOC as a Service focused on Operational Technology challenges.



Siemens Critical Infrastructure Defense Center portfolio of Cybersecurity SOC as a Service:

- *Incident Response Planning*
- *Forensics and Malware Analysis*
- *Vulnerability Assessments Scans*
- *Incident and Breach Response Service*
- *Threat intelligence and analyst*
- *Penetration Testing and Red Team Services*

Why SOC as a Service for Cybersecurity?

Cyber attacks are shifting from IT services to **OT services** and **critical infrastructure**.

For example: Recent attacks on Electric Utilities and Oil/Gas Pipelines in order to negatively impact the safety and economic wellbeing of the society.

Motivation include



Gartner predicts "The impact of these attacks will result in fatal casualties and cost over \$50 billion by 2023."

1. The Siemens Critical Infrastructure Defense Center (CIDC) -, offers a **cyber-resilient, matured, Cybersecurity program and approach**. Siemens has more than a decade experience of competence and solutions developed internally to identify, protect, detect, respond and recover from cyber threats.





***SOC – Cybersecurity
Services***

Siemens Capability

Our Portfolio of Services

Our portfolio of services delivered through our consulting, professional, managed, and research security services support the day in the life of security professionals



SOC as a Service

We provide a range of services across these portfolios including but not limited to

Forensics and Breach Investigations



Threat Hunting



Vulnerability Management



Penetration Testing



Red/Blue Team Exercises



and much more!



SOC as a Service

Horizontal Cybersecurity Services



Cybersecurity Services

Our holistic cybersecurity approach helps mastering the challenges of an increasingly digitalized world.



Cybersecurity for Industry

Protected in every aspect: Cybersecurity as an essential component of Digital Enterprise.



Cybersecurity for smart buildings

Protect what you value - with our holistic approach and leading technology expertise.



Grid Security

You shouldn't trust just anyone! Full protection 24/7 – thanks to interoperable products that meet strict cybersecurity requirements.



Cybersecurity for rail and road

As experts in digitalization and pioneers in cybersecurity, we are dedicated towards making mobility more secure for everyone.



Cybersecurity at Healthineers

Protecting healthcare institutions against cyberthreats

1

Cybersecurity Assessment

Our advisory services provided by our team of experts across Canada, US, and Europe include a variety of cybersecurity assessments to help organizations understand their cybersecurity programs relative to baselines and different frameworks

>	NIST CSF	Assessment and review of cybersecurity program and existing controls using the NIST Cybersecurity Framework
>	NIST SP800-53	Assessment and review of Enterprise/IT cybersecurity program and existing controls using the NIST Special Publications 800-53
>	NIST SP 800-82	Assessment and review of OT network and existing controls using the NIST Special Publications 800-82 for Industrial Control Systems
>	ISA/IEC 62443	Assessment and review of cybersecurity management system (CSMS) against the ISA/IEC 62443 cybersecurity standards
>	C2M2	Assessing the maturity of an organization's cybersecurity program using the cybersecurity capability maturity model from the United States Department of Energy (DoE)
>	AESCSF	Assessment and review of cybersecurity program and existing controls using the Australia Energy Sector Cybersecurity Framework
>	ISO/IEC	Assessment and implementation of an Information Security Management Systems (ISMS) based on ISO/IEC 27001

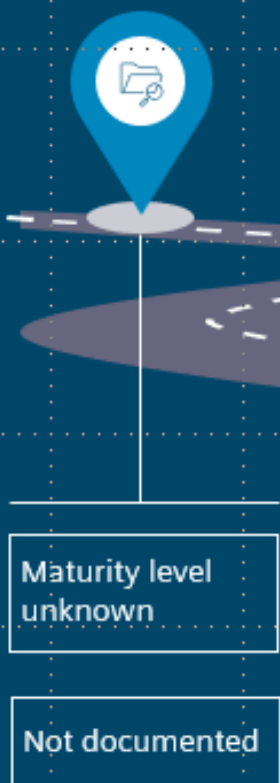
Our Services

We provide a wide range of cybersecurity services delivered through our Consulting Services, Professional Services, and Managed Security Services. Our services include the following:

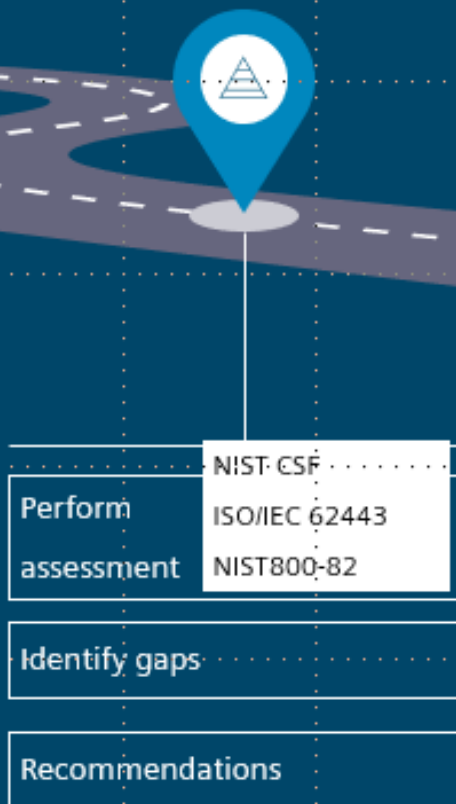
Cyber Assessment Library

Cybersecurity Program Development Approach

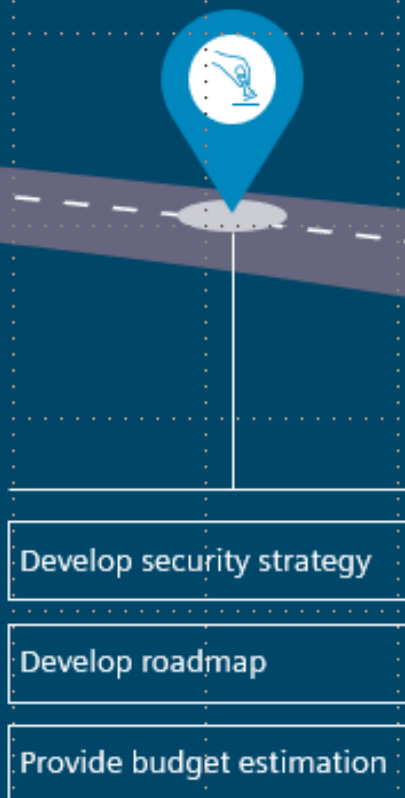
Current State



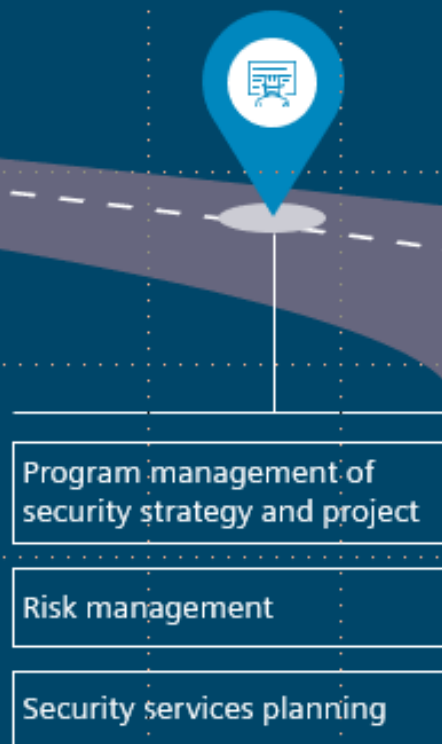
Determine Security Posture/Maturity Level



Develop Security Program



Implement Security Program



Desired state

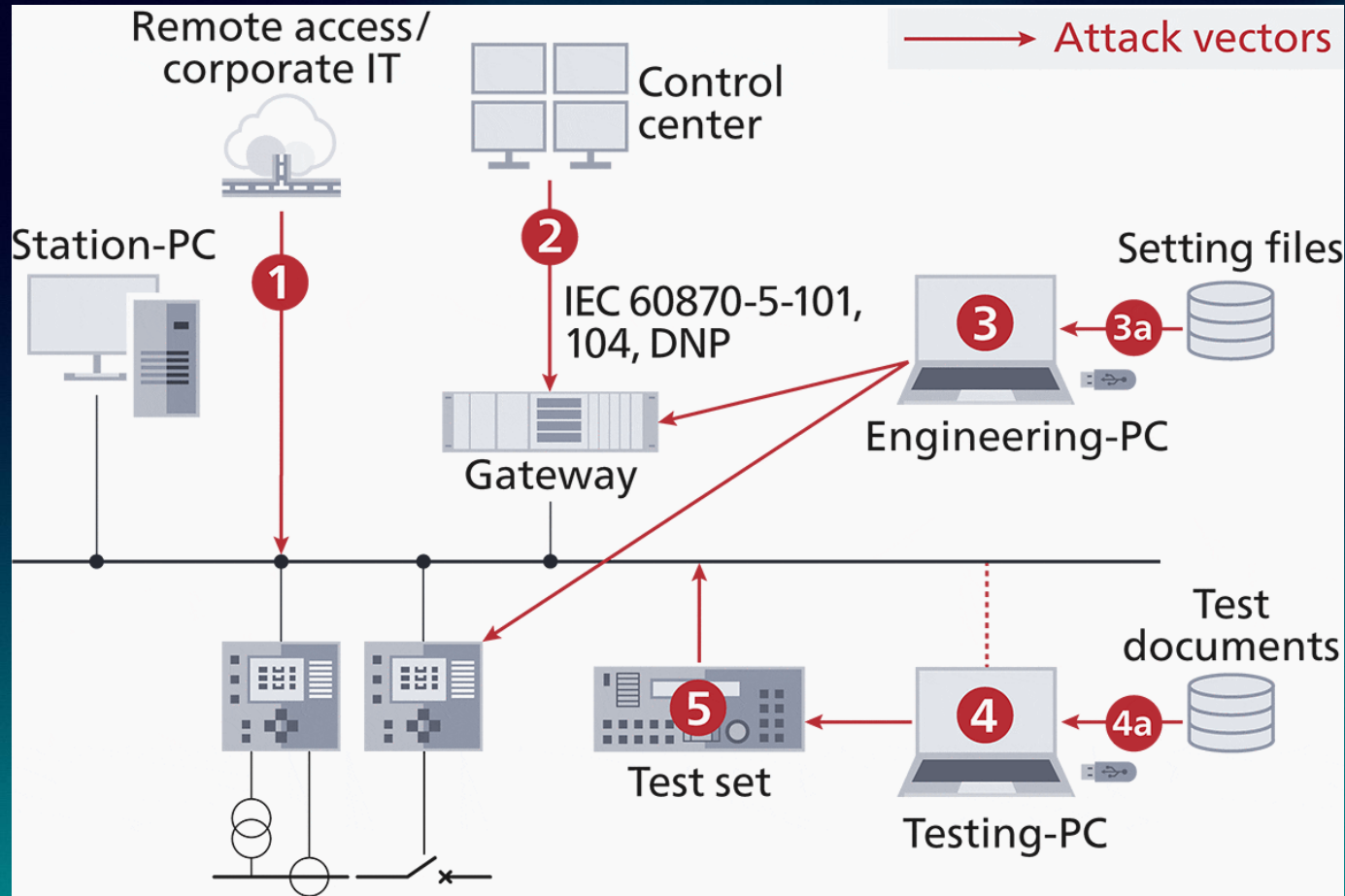




Cyber Secure Substations

SIEMENS

SOC as a Service – Cyber Secure Substations



1. The most frequent attack vector used is the connection from corporate IT
2. An attacker could also enter through the control center connection
3. Another entry point is through engineering PCs connected to substation equipment or the network – 3a Setting Files
4. Laptops used for testing the IEC 61850 system are often directly connected to the station bus which is also a potential way to infect IEDs - 4a Test Documents
5. This leaves the testing device itself as a potential attack vector

Notice of Proposed Rule Making Asset Impacts

Expected NERC CIP Location Impacts

- The most probable outcome of FERC's NOPR is that new NERC CIP requirements may be expanded to include most utilities' Operational Technology (OT) networks
 - NERC CIP further classifies utilities by whether they can have a high or medium impact on the nation's grid
 - Potential requirements may apply to medium-impact utilities with no ERC and utilities with low-impact substations
 - Expected proposed changes to NERC CIP mandates will affect regulated utilities and force currently unregulated utilities under the CIP regulatory umbrella





Secure Access Management Solution

SOC as a Service – Intrusion Detection Systems

IDS



Non-intrusive, anomaly-based signature-less Intrusion Detection System software for mission-critical operational networks, operating on RUGGEDCOM hardware, provides early warning notification and alerting on vulnerabilities and sophisticated cyber threats that may be undetectable by conventional IT security tools



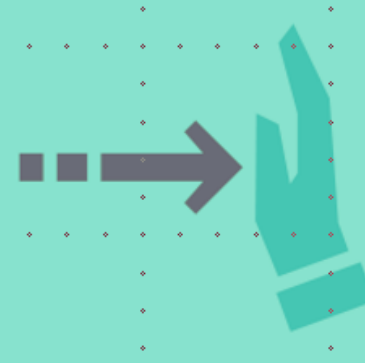
DPI



Deep Packet Inspection (DPI) on the RUGGEDCOM RX1500 with the APE1808 examines data packets utilizing a non-intrusive methodology for mission-critical networks. DPI helps to secure the communication to control centers and IT networks



IPS



An Intrusion Prevention System (IPS) is a capability available on the RUGGEDCOM hardware if equipped with a NGFW solution. IPS is located between the WAN and the LAN to deny the traffic that represents known threat based on a security profile



NGFW



RUGGEDCOM switching and routing platform with leading Next-Generation Firewall functionality on a single integrated appliance provides for additional integrated DPI/IPS functionalities, as well as security when connecting non-critical IT networks to critical deterministic operational networks.



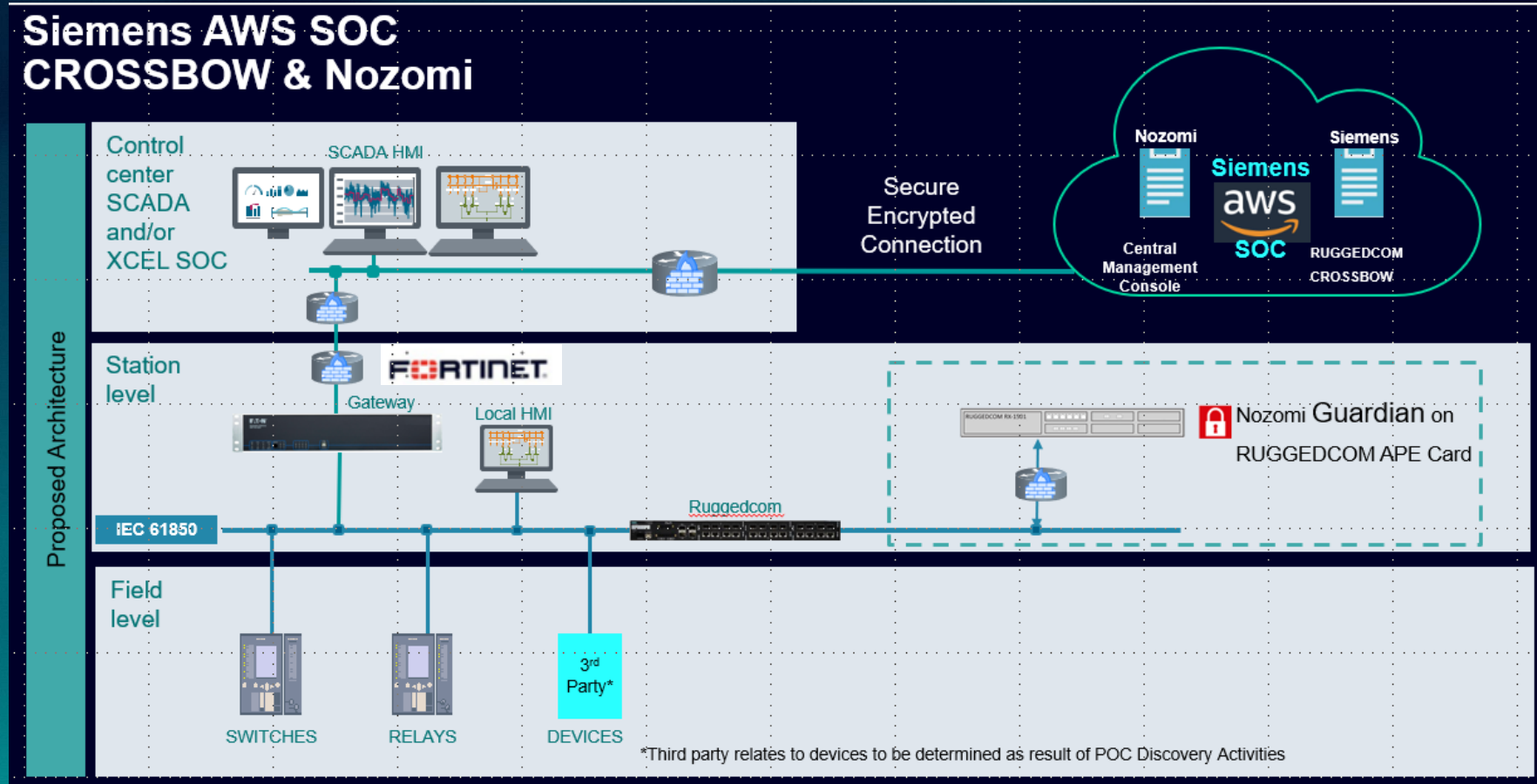
High-Level Substation Architecture

The cybersecurity sensors can communicate with local or central management consoles through a dedicated management LAN, completely separated from the production environment.

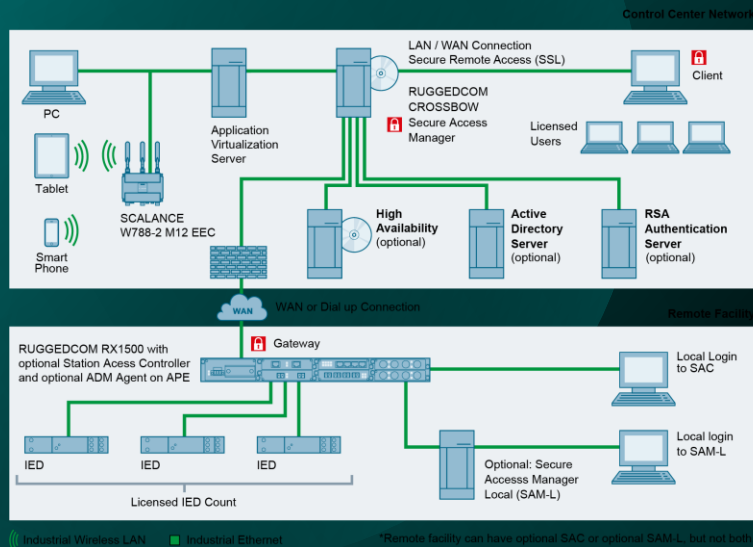
This ensures that the transmission of IEC 61850 communications is not disturbed in any way.

Sample Deployment Architecture

Example substation and SOC architecture showing the deployment of an OT and IoT threat detection and monitoring solution.



Secure Remote Device Access and Management



Addresses NERC CIP requirements for remote IED access, activity logging and data privacy

- Provides **abstraction of device level passwords** from individual users

Securely connect users to substation IEDs and communications infrastructure without going to the field

- **Automate repetitive tasks** including device password changes, firmware and configuration management

Strong user authentication through RSA SecurID, Active Directory & RADIUS

- **Extract fault and event files** from relays automatically without the need for additional substation hardware

Visualization Layer

“If our organization could swiftly identify unintentional and accidental cyber incidents, we could reduce operational risks and prioritize our cybersecurity staff’s time and resources.”



“Creating and maintaining an accurate, detailed, and up-to-date inventory of OT/IoT network assets in large scale deployments has proven to be costly, time-consuming, technically daunting, and outside my organization’s resources and expertise.”



***Regulatory
Compliance***

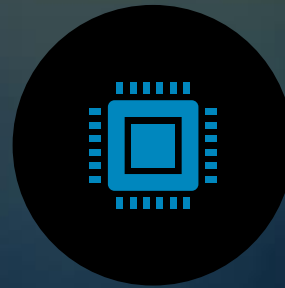
CYBERSECURITY COMPLIANCE MATRIX

NERC CIP			IEC 62443			
TOPIC	STANDARD(S)		TOPIC	REQUIREMENT		
CRITICAL CYBER ASSETS	CIP-002.5-1a	Y	Risk identification, classification and assessment	62443-2-1	4.2.3	Y
SECURITY MANAGEMENT CONTROLS	CIP-003-8	Y	Access control: Account administration	62443-2-1	4.3.3.5	Y
PERSONNEL AND TRAINING	CIP-004-6	Y	Staff training and security awareness	62443-2-1	4.3.2.4	Y
			Detailed of the remote access applications	62443-2-4	SP.07.02	Y
ELECTRONIC SECURITY	CIP-005-6	Y	Access control: Authentication	62443-2-1	4.3.3.6. 4.3.3.7	Y
			Profiles	62443-2-4	4.1.4	Y
			Access Control/Multifactor Authentication	62443-2-4	SP.03.07	Y
			Remote Access Applications	62443-2-4	SP.07.01	Y
PYHSICAL SECURITY	CIP-006-6		Physical and environmental security	62443-2-1	4.3.3.3	
SYSTEMS SECURITY MANAGEMENT	CIP-007-6	Y	Verify that all control actions and data flows	62443-2-4	SP.03.09	Y
INCIDENT REPORTING AND RESPONSE MANAGEMENT	CIP-008-6		Incident planning and response	62443-2-1	4.3.3.5	
RECOVERY PLANS	CIP-009-6		Backup procedures and Recovery	62443-2-4	SP.12.01	
CONFIGURATION CHANGE MANAGEMENT	CIP-010-3	Y	CHANGE MANAGEMENT	62443-2-4	SP.06.02	Y
INFORMATION PROTECTION	CIP-011-1		Information and document management	62443-2-1	4.3.4.4	
Supply Chain Risk Management	CIP-013-1		Requirements for IACS solution suppliers	62443-2-4	SP-11	

NERC CIP Compliance



External Cybersecurity professionals reduce risk of achieving NERC CIP Compliance



Formal assessment and certification of controls based primarily on the NIST Cybersecurity Framework



External assessment can help organizations identify their control gaps and develop a roadmap to remediate those gap



Establish repeatable best practices approach for NERC CIP Compliance

SOC as a Service Benefits

Helps meet NERC CIP Cybersecurity Standards

- **Detect intrusions in near real time.**
- **Identify maintenance anomalies** (such as wrong firmware or configuration files) before personnel leave site.
- **Manage password changes remotely and automatically.**
- **Remove authorization privileges automatically** via Active Directory connection to HR system.

O&M Savings

- **Automated reporting** saves time and money.
- **Remote password resets** eliminates site visits.
- **Secure Remote Access** eliminates cost of site visits to retrieve fault records and reduces time when diagnosing failures.
- **Centralized server design** reduces O&M costs as compared to decentralized designs.



SOC as a Service Partners

Siemens SOC – Value Added Partners



OT and IoT device discovery, network visualization, vulnerability assessment, risk monitoring and cyber threat detection – all in a single platform.



Agentless cloud security and compliance for AWS, Azure, Google Cloud, and Kubernetes - in a fraction of the time and operational costs of other solutions



Optimize Return on Cyber Investment with Cyber Risk Quantification & Management Solutions.



A holistic view of cyber risk throughout the entire IT and OT ecosystem of critical infrastructure and its extended supply chain.

| Thank you

Siemens Power Technologies International
Executive Business Development, Siemens Smart Infrastructure

Gerry Vurciaga

Siemens PTI

Mobile: +1 720-628-3918

E-mail: Gerry.vurciaga@siemens.com