

Nokia Mission-critical Communications Networks Solution for Power Utilities

Attaining NERC CIP reliability standards compliance

Application note

The Nokia logo is displayed in blue, consisting of the word "NOKIA" in a stylized, sans-serif font. The logo is positioned in the lower right quadrant of the page. A large, solid blue diagonal bar runs from the top left corner towards the bottom right, partially obscuring the lower left portion of the page.

NOKIA

Abstract

Electricity is the bedrock of modern societies and economies. A secure electric grid is crucial for ensuring the reliable delivery of electricity for daily use by commercial and residential users. As a result, power utilities worldwide consider grid security a top priority. In particular, power utilities in North America have long been required to comply with the Critical Infrastructure Protection (CIP) standards specified by the North American Electric Reliability Corporation (NERC).

This application note summarizes the NERC CIP Reliability Standards and explains how the Nokia Mission-critical Communications Networks Solution for Power Utilities can help you protect your grid and comply with the NERC CIP requirements.

Contents

Abstract	2
Introduction	4
Summary of CIP version 5 standards	5
Nokia mission-critical communications networks solution	6
Attaining CIP compliance with the nokia solution	7
Conclusion	10
Abbreviations	11

Introduction

Highly secure communications are crucial for maintaining daily operations in mission-critical networks, particularly those that support public infrastructure such as electric power grids. The reliable and secure delivery of electricity to commercial and residential users is an essential part of the foundation for modern societies.

In November 2013, the Federal Energy Regulatory Commission (FERC), the independent government agency that regulates the interstate transmission of electricity in the US, approved Version 5 of the NERC CIP Reliability Standards for Bulk Electric Systems (BESs) in North America.

Version 5 of the standards significantly expands on the requirements defined in the CIP Version 3 standards.¹ It includes new cyber security specifications and extends the scope of the systems that the CIP standards protect.

Compliance with the NERC CIP standards is critical for mitigating cybersecurity risks to BESs. This application note details how the Nokia Mission-critical Communications Networks Solution for Power Utilities can play a seminal role in helping electric grid operators comply with the mandatory NERC CIP requirements.

¹ Version 4 will not be implemented because Version 5 provides more comprehensive improvements to the standards. FERC approved NERC's proposal to bypass implementation of Version 4 and allow utilities to transition directly from Version 3 to Version 5..

Summary of CIP Version 5 standards

In 2008, FERC approved eight reliability standards that NERC developed to protect BESs, considered as mission-critical infrastructure, from cyberattacks. These standards formed the first version of the CIP Reliability Standards. Since then, NERC has expanded the set to 13 standards.² In addition, FERC has published implementation guidance and practice guides to help utilities attain compliance.

This application note focuses on the mandatory NERC CIP standards that are subject to enforcement. A synopsis of each standard follows. The latest version of the standards can be downloaded from the links in the [NERC CIP one-stop shop spreadsheet](#).

CIP-002-5.1a: Cyber Security – BES Cyber System Categorization

Purpose: To identify and categorize all BES Cyber Systems³ and their associated assets for the application of cybersecurity requirements according to the adverse impact (high, medium or low) that loss, compromise or misuse of those BES Cyber Systems could have on the reliable operation of the BES. The associated assets can include control centers, transmission stations and substations, generation resources, system restoration facilities and special protection systems.

CIP-003-8: Cyber Security – Security Management Controls

Purpose: To specify consistent and sustainable security management controls that establish responsibility and accountability to protect BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

CIP-004-6: Cyber Security – Personnel and Training

Purpose: To minimize the risk against compromise that could lead to misoperation or instability in the BES from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training and security awareness in support of protecting these systems.

CIP-005-7: Cyber Security – Electronic Security Perimeter(s)

Purpose: To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter (ESP) in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

CIP-006-6: Cyber Security – Physical Security of BES cyber systems

Purpose: To manage physical access to BES Cyber Systems by specifying a physical security plan in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

CIP-007-6: Cyber Security – System Security Management

Purpose: To manage system security by specifying select technical, operational and procedural requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

² The latest NERC CIP standards comprise a set of documents ranging from CIP-002 to CIP-014.

³ This is a new term introduced in CIP Version 5 and referring to cyber assets subject to CIP protection. For definitions of terms used in CIP Version 5, see [CIP V5 Definitions](#).

CIP-008-6: Cyber Security – Incident Reporting and Response Planning

Purpose: To mitigate the risk to the reliable operation of the BES as the result of a cyber security incident by specifying incident response requirements.

CIP-009-6: Cyber Security – Recovery Plans for BES Cyber Systems

Purpose: To recover reliability functions performed by BES Cyber Systems by specifying recovery plan requirements in support of the continued stability, operability and reliability of the BES.

CIP-010-4: Cyber Security – Configuration Change Management and Vulnerability Assessments

Purpose: To prevent and detect unauthorized changes to BES Cyber Systems by specifying configuration change management and vulnerability assessment requirements in support of protecting BES Cyber Systems from compromise that could lead to misoperation or instability in the BES.

CIP-011-2: Cyber Security – Information Protection

Purpose: To prevent unauthorized access to BES Cyber System Information by specifying information protection requirements in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES.

CIP-012-1: Cyber Security – Communications between Control Centers

Purpose: To protect the confidentiality and integrity of real-time assessment and real-time monitoring data transmitted between control centers.

CIP-013-2: Cyber Security – Supply Chain Risk Management

Purpose: To mitigate cyber security risks to the reliable operation of the BES by implementing security controls for supply chain risk management of BES Cyber Systems.

CIP-014-3: Cyber Security – Physical Security

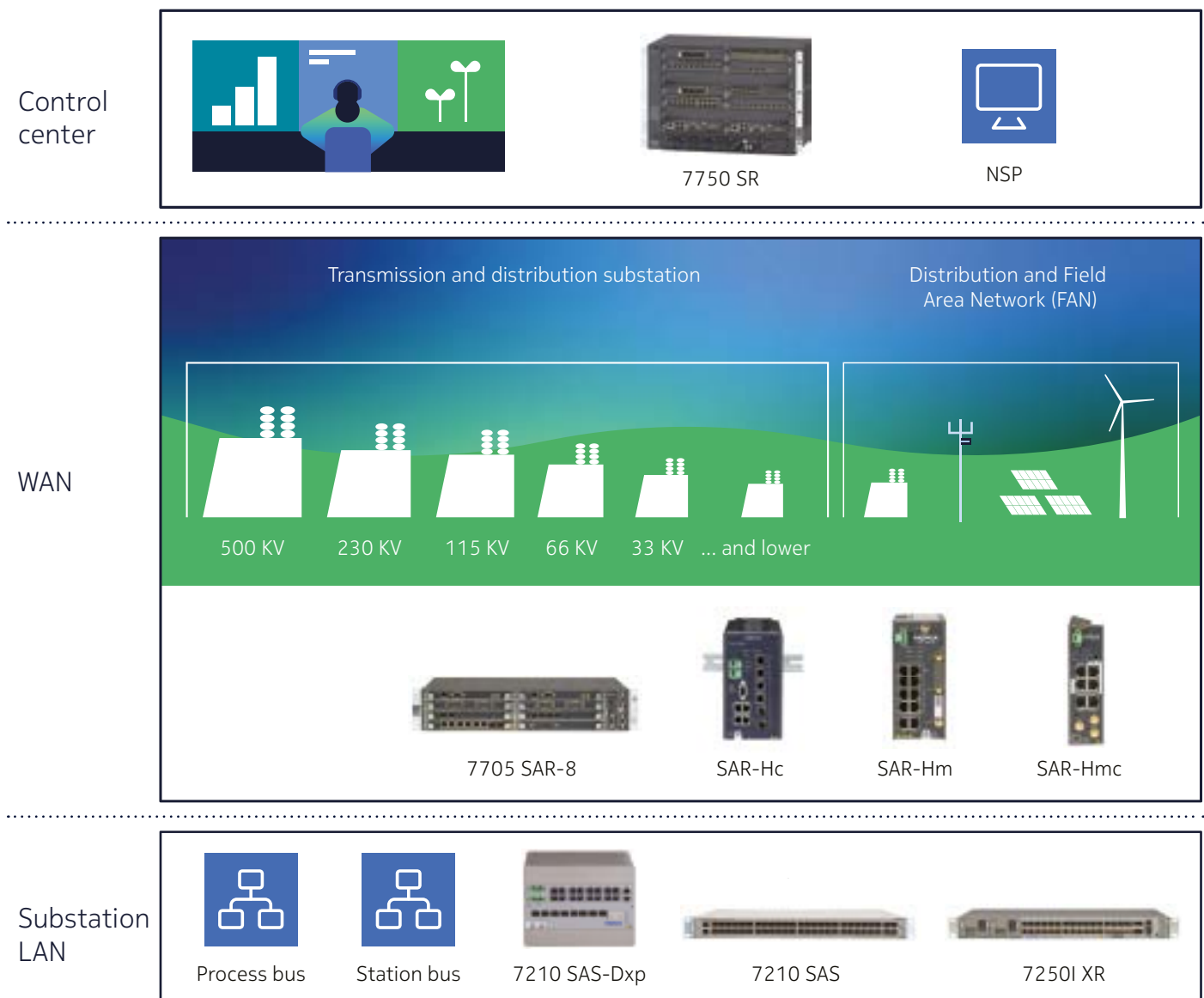
Purpose: To identify and protect transmission stations and transmission substations, and their associated primary control centers, that if rendered inoperable or damaged as a result of a physical attack, could result in instability, uncontrolled separation or cascading within an interconnection.

Nokia Mission-Critical Communications Networks Solution

The Nokia Mission-critical Communications Networks Solution is designed to meet the networking needs of power utilities worldwide. It consists of the following IP/MPLS products, as shown in Figure 1:

- [Nokia 7750 Service Router \(SR\)](#)
- [Nokia 7705 Service Aggregation Router \(SAR\)](#)
- [Nokia 7210 Service Access Switch \(SAS\)](#)
- [Nokia Network Services Platform \(NSP\)](#)

Figure 1: Nokia Mission-Critical Communications Networks Solution for Power Utilities





The solution provides four key characteristics to enable the resilient communications that mission-critical networks need to help utilities accomplish their tasks reliably:

1. Support for legacy and next-generation IEC 61850 applications with full scalability and flexibility for future evolution.
2. Streamlined network management, operations, administration and maintenance (OAM) across the grid communication infrastructure.
3. A single and consistent end-to-end network management solution and network operating system with a common operations paradigm and Command Line Interface (CLI).
4. Comprehensive installation options, including:
 - Standard rack and cabinet-based installations
 - Versatile DIN rail, wall, panel and stand mounting options
 - High- and low-voltage support in small enclosures for outdoor deployments

Attaining CIP compliance with the Nokia solution

Table 1 describes how the Nokia Mission-critical Communications Networks Solution can play an integral role in helping utilities achieve NERC CIP compliance.

Visit the [NERC CIP compliance guidance web page](#) to learn more.

Table 1. How the Nokia IP/MPLS solution helps utilities comply with NERC CIP requirements

Standard	Security requirement summary	How Nokia IP/MPLS solution help
CIP-002-5.1a	Classify BES assets as high, medium or low impact to effectively prioritize their security efforts. Implement appropriate measures to safeguard these assets from cyber threats and enhance the overall resilience of the BES.	Nokia Network Services Platform (NSP) allows operators to classify the assets connected to the Nokia communications equipment into different asset types. As asset classification information is reviewed and updated (every 15 calendar months or less), operators can update the classification on NSP accordingly.
CIP-003-8	Establish requirements for developing, implementing and maintaining a documented security management program to identify and mitigate risks to the BES. Documenting the implementation of security controls, policies, processes and procedures is important for streamlining security across the assets of the BES.	NSP allows operators to centralize network security control and security policies for access management according to defined processes and procedures across all BES locations. As policies, processes and procedures are reviewed and changed, operators can update the NSP configuration accordingly.
CIP-004-6	Develop the capabilities and readiness of personnel through security training and awareness programs. The scope includes proper implementation of cybersecurity policies, handling of sensitive BES information and security risk management.	The Nokia solution offers highly customizable security policies, including user access levels, role-based access control (RBAC), span of control and scope of commands with a detailed activities log for auditing purposes.
CIP-005-7	Develop and implement cyber security controls for ESPs that protect BES-connected networks through routable protocols. Define, document and manage security perimeters and implement measures such as access controls, monitoring and incident response.	The Nokia solution includes an Electronic Access Point (EAP) that offers rich network security capabilities, including encryption, firewall, access control list (ACL) and extensive nodal security management features for a fortified ESP to protect the BES. EAP configurations can be tailored to meet unique ESP requirements. As security measures are updated, configurations can be updated accordingly.
CIP-006-6	Develop and implement physical security controls and procedures to protect BES. Develop, document and manage physical perimeters and security measures.	The Nokia solution offers secure and reliable communications to support physical security systems such as CCTV with video analytics capabilities, badge access and physical intrusion detection. Its scalable and high-performance IP multicast solution is well-suited to backhaul a large number of CCTV feeds to data center for real time- and post-processing video processing.
CIP-007-7	Manage system security by specifying technical, operational and procedural requirements. Key measures include disabling or “closing” unnecessary or unused physical or logical output interfaces.	The Nokia solution offers broad but granular control of network configurations. Only necessary interfaces and ports are “open.” Use of IP/MPLS VPN with strict data flow segregation and filtering and MPLS label-switched paths ensure that only legitimate communications are allowed. Also, role-based user privileges are tailored according to operational needs to minimize security exposure.

Standard	Security requirement summary	How Nokia IP/MPLS solution help
CIP-008-6	Develop and implement a security incident response plan and establish procedures for incident reporting. Consolidate and correlate events and alerts to identify and respond to incidents in a timely way.	NSP centrally consolidates and correlates network alarms and alerts to isolate the root cause. In addition, it also monitors events and incidents in the network and reports them to support remedial actions.
CIP-009-6	Develop and implement procedures for restoring, testing and validating the functionality of the BCS. Develop recovery capabilities that will minimize BCS downtime.	The Nokia solution is fully redundant to minimize network downtime. All network configurations are securely backed up to support restoration if needed.
CIP-010-4	Improve the ability to prevent unauthorized configuration changes, detect vulnerabilities and maintain a secure and reliable BES.	The Nokia solution plays an integral role of protecting BES from illegitimate access to make unauthorized changes. The Nokia NSP Work Flow Manager enables utilities to develop an review-and-approve workflow to ensure changes on network configuration and associated IP filtering policy are authorized before being implemented. All configuration change events are also centrally logged with Syslog. In addition, the Nokia solution offers strong and robust encryption protection to safeguard data in flight. The solution also provides network segmentation with IP/MPLS VPN and firewall.
CIP-011-2	Develop and implement information protection policies and access control to mitigate the risk of data breaches.	The Nokia solution offers strong and robust encryption protection to safeguard data in flight. It also provides network segmentation with IP/MPLS VPN, firewall and ACLs to block unauthorized access.
CIP-012-1	Monitor and secure data transport over the network connections between control centers	The Nokia solution offers strong and robust multilayer (IP/MPLS, Ethernet, optical and microwave) encryption protection to safeguard data in flight. With a symmetric key management architecture, the encryption mechanisms are quantum safe and can withstand the emerging threat posed by the use of quantum computers to break cryptographic algorithms. Additionally, with IP/MPLS pseudowire redundancy capabilities, the solution also provides geo-redundancy protection to enable failover switching without service impacts.
CIP-013-2	Develop processes with suppliers for planning, procurement and assessment of security risks and policy for access to assets by supplier staff.	The Nokia solution is designed to be highly secure. It is Evaluation Assurance Level 3+ (EAL3+) and FIPS-140-2 certified.
CIP-014-3	Conduct risk assessments, develop physical security plans and implement security measures, including access controls, monitoring systems and response procedures.	The Nokia solution offers secure and robust network transport capabilities for physical security systems such as CCTV and physical access system intrusion detection systems that protect the physical perimeter of the BES.

Conclusion

The “electrification of everything” trend has made the reliability of electric service more important than ever. Power utilities in North America are now mandated to dedicate resources for designing and executing actions that will fulfill the requirements and regulations defined in the NERC CIP Version 5 Reliability Standards.

Nokia has real-world expertise in helping power utilities build converged networks that deliver scalable network services, ensure resilient high availability and implement field-proven cybersecurity best practices. Our industry-leading mission-critical communications networks solution meets the reliability, performance and scalability demands of utilities and provides a strong defense against security threats and intrusions.

[Visit the Nokia utility website](#) to learn more about how our utility solutions and expertise can make it easier for you to protect your grid and comply with regulatory requirements.

Abbreviations

ACL	access control list
BES	Bulk Electric System
CCTV	closed-circuit television
CIP	Critical Infrastructure Protection
CLI	command-line interface
DIN	Deutsches Institut für Normung
EAL	Evaluation Assurance Level
EAP	Electronic Access Point
ESP	Electronic Security Perimeter
FERC	Federal Energy Regulatory Commission
FIPS	Federal Information Processing Standards
IP	Internet Protocol
MPLS	Multiprotocol Label Switching
NERC	North American Electric Reliability
NSP	Network Services Platform
OAM	operations, administration and maintenance
RBAC	role-based access control
SAR	Service Aggregation Router
SAS	Service Access Switch
SR	Service Router
VPN	virtual private network

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2023 Nokia

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: August CID181741