Landis+Gyr

NERC CIP COMPLIANCE IN ELECTRICAL SUBSTATIONS

AN EXECUTIVE VIEW ON HOW TO FULFILL THE CYBERSECURITY REGULATIONS THROUGH A NETWORK INTRUSION DETECTION SYSTEM

I. INTRODUCTION: THE ELECTRIC GRID IS A MATTER OF NATIONAL SECURITY

In September 2023, the GridWise Alliance and The National Electrical Manufacturers Association, two groups of electricity industry stakeholders, met with Congressional staff and representatives from the Department of Energy and other government organizations. The 300-strong conference, held in the Rayburn Office Building at the US Capitol in Washington, D.C., aimed to bring political awareness to grid modernization requirements. Naturally, cyber security of the critical infrastructure was at the heart of many discussions.

The importance of energy grid security was reinforced by the Grid Innovation Caucus co-chairs, U.S. Representatives Robert Lata (Republican, Ohio) and Marilyn Strickland (Democrat, Washington). In her opening remarks, Strickland urged all stakeholders that ”having a modernized grid is a public safety issue. Having a modernized grid is a national security issue.“

The need to see and act on US electricity distribution as a matter of national security requires the coordination of many stakeholders. As Latta made clear ”we have to make sure we’re getting it right, not only on the legislative side, but also on the regulatory side.“

The North American Electric Reliability Corporation (NERC) is tasked with creating and enforcing the right reliability standards for Bulk Electric Systems (BES). NERC regularly updates its Critical Infrastructure Protection (CIP) standards, which primarily focus on management processes rather than offering specific technical guidance. This lack of guidance can become overwhelming for those responsible for implementation at utilities, especially when facing the prevailing OT security skills gap and an overwhelming number of technological options. Given that compliance with legally-binding CIP standards is a top priority and necessity for energy companies, the solutions should be simple and manageable to fulfill the minimum requirements.

In this ebook, we will discuss the vital role that network intrusion detection systems (NIDS) play in enhancing NERC CIP compliance within electrical substations. We also showcase the advantages and functionalities by which the Rhebo NIDS from Landis+Gyr enables an efficient defense-in-depth cybersecurity strategy in OT networks.

CONTENT LIST

II. WHY THE NERC CIP STANDARDS ARE IMPORTANT

NERC CIP standards are a set of regulations designed to protect the reliability and security of the electric transmission and distribution systems.

The CIP standards require energy utilities to establish and maintain stringent security measures to safeguard their critical infrastructure assets, including electrical substations and distribution networks. Compliance is not only essential for ensuring the resilience of the North American electrical grid. It is also a regulatory necessity required by law. Non-compliance can be penalized by the respective authorities.

The majority of the CIP standards apply specifically to the cybersecurity aspects of the grid. Only CIP-006 and CIP-014 address the physical security of critical infrastructure. Together, the 13 CIP standards create a baseline set of cyber security standards. Each part represents a piece of the cyber security puzzle. Thus, the requirements mirror the five main foundations of building a strong (cyber) security posture that ensures the availability of the critical assets (Figure 1):

1. General **management guidelines and processes** that anchor cyber security as a relevant activity throughout the company.
2. Measures to prevent **cyber security** breaches at the network perimeter.
3. Measures to **detect cyber threats** and cyber security breaches within the network and systems.
4. Measures to **mitigate** cyber security incidents.
5. Measures to ensure **physical security** of substations and control centers.

RELEVANT ACRONYMS
BES The Bulk Electric System
CIP Critical Infrastructure Protection
NIDS Network Intrusion Detection System
Syslog System Logging Protocol

Figure 1 *The NERC CIP standards mirror the different layers of a comprehensive security architecture*

III. WHAT IS A NIDS?

A OT Network Intrusion Detection System (NIDS) is a critical component of any comprehensive cybersecurity strategy within an electrical substation. The NIDS sits within the network (Figure 2) rather than just at the perimeter (though sensors can be integrated there as well).

A NIDS passively and continuously monitors all OT network traffic for signs of unauthorized access, suspicious behavior, and cyber threats that have breached the perimeter or originate from within the company. Contrary to typical firewalls, the NIDS does not rely on defined signatures of known attack patterns. Instead it compares all communication to a baseline that defines the expected and legitimate communication behavior of the OT components. Any deviation from this baseline is considered a change or anomaly that can negatively affect substation operation. This can be security-relevant incidents like scans, changes in communication patterns and new connections, as well as existing vulnerabilities and technical error states.

In that sense, a NIDS acts as a vigilant sentinel, continually analyzing network traffic to detect and report anomalies or patterns indicative of cyber attacks, human error, device or system failure.

To prevent unwanted disruption of the sensitive industrial processes of the BES, the anomaly detection does not actively block any detected activities. Instead, it sends real-time alerts to the security team which include all information to make informed decisions on further actions.

> *An innovator in OT security solutions for the electrical distribution sector since 2015, Landis+Gyr company Rhebo offers a dedicated NIDS for digitized industrial environments.*

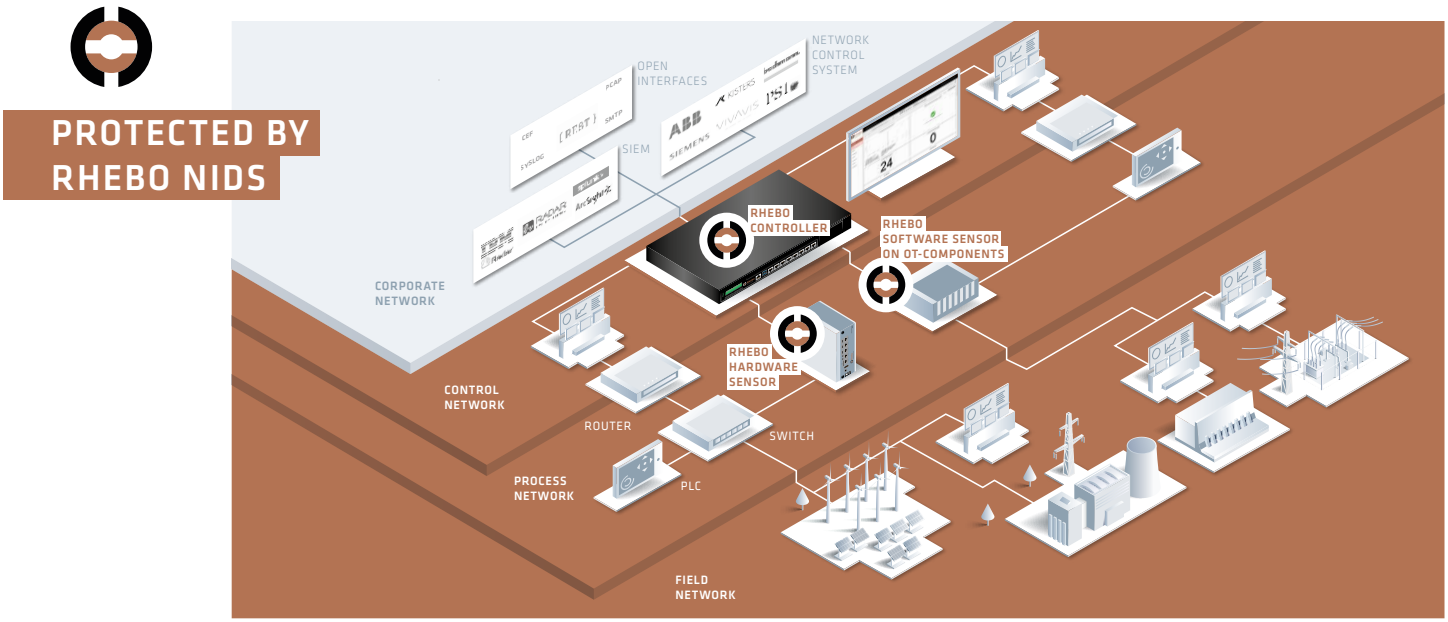


Figure 2 *The NIDS sensors mirror the OT network traffic via switch ports or network taps and send the data to the controller where the anomaly detection analyzes the entire traffic in real-time. Integration in automation platforms and SIEM systems is possible.*

IV. HOW NIDS BENEFITS NERC CIP COMPLIANCE

As Figure 3 showcases, the Rhebo NIDS from Landis+Gyr is a multi-use tool that fundamentally helps in the different phases of system hardening and increasing the cyber security posture. By this it enables energy utilities to become and stay compliant with the different levels of NERC CIP requirements.

OT VISIBILITY

By monitoring the network traffic the NIDS identifies all BES cyber systems. This allows companies to define the security perimeter and conduct an efficient, comprehensive risk analysis & vulnerability assessment.

CONTINUOUS MONITORING

The NIDS operates 24/7, ensuring continuous monitoring of network traffic. This aspect aligns with NERC CIP requirements, which emphasize the need for continuous monitoring and incident response capability.

THREAT DETECTION

The NIDS detects and informs operators of potential threats and vulnerabilities in real-time, including unauthorized access, malware, and other malicious activities that may compromise the reliability of the BES. This is amplified by integrating the OT NIDS alerts with a Security Event & Information Management (SIEM) system.

INCIDENT RESPONSE

The NIDS provides a valuable resource for incident response. When a security incident occurs, the NIDS can help security teams quickly identify the source, location, scope, and nature of the attack, allowing for rapid containment and mitigation of the threat.

ASSET PROTECTION

By detecting and responding to threats promptly, the NIDS helps to protect critical assets within electrical substations, thereby reducing the risk of damage to physical infrastructure and ensuring the availability and reliability of the electrical grid.

COMPLIANCE MONITORING AND INCIDENT REPORTING

The NIDS also aids in compliance monitoring by keeping records of anomalous network activities, which can be crucial for audits and reporting in accordance with NERC CIP requirements.

IMPROVEMENT OF THE SECURITY SYSTEM

As the second line of defense, the NIDS indirectly watches the watchmen. Any reported anomaly can be an indicator that the first line of defense (i.e. firewalls, authentication procedures etc.) has a blind spot or is itself compromised (see chapter VII). By this reporting, the NIDS helps to identify security gaps and new threats to trigger the review and improvement of the existing security system.

V. HOW THE RHEBO NIDS FROM LANDIS+GYR ALIGNS WITH NERC CIP REQUIREMENTS

As part of defense-in-depth security architecture, an OT NIDS aligns with the NERC CIP requirements in three ways:

1. The NIDS directly implements and supports key infrastructure security with the ability to detect any malicious activity (CIP-007) within the OT network, as well as provide comprehensive knowledge on the OT network, structure, assets, and risks.
2. The NIDS functions as a breach detection system that identifies attacks which may have compromised or blindsided the first line of defense, i.e. firewalls, port restrictions, and authentication procedures defined in security plans (CIP-007, CIP-008).
3. The NIDS delivers crucial intelligence for the risk assessment, network asset management, and security plan review as well as event correlation in a SIEM system (CIP-002, CIP-009, CIP-010).

This is summarized in the following matrix (Figure 3) and mapped to the respective CIP standards in Table 1.

To fulfill the isolation requirements many electrical substations must adhere to, it is important that the NIDS can be deployed without an external connection. The NIDS Rhebo Industrial Protector supports both deployment strategies. It can be operated without external connection where the anomaly detection is run, and visualized on a local machine and Rhebo controller. It can also be operated with an external connection to a central controller in the control center or Security Operations Center (SOC) to analyze the OT network traffic of several locations.

Additionally, anomaly notifications can be sent as pre-qualified events to a Security Information & Event Management (SIEM) system using the standard Syslog protocol.

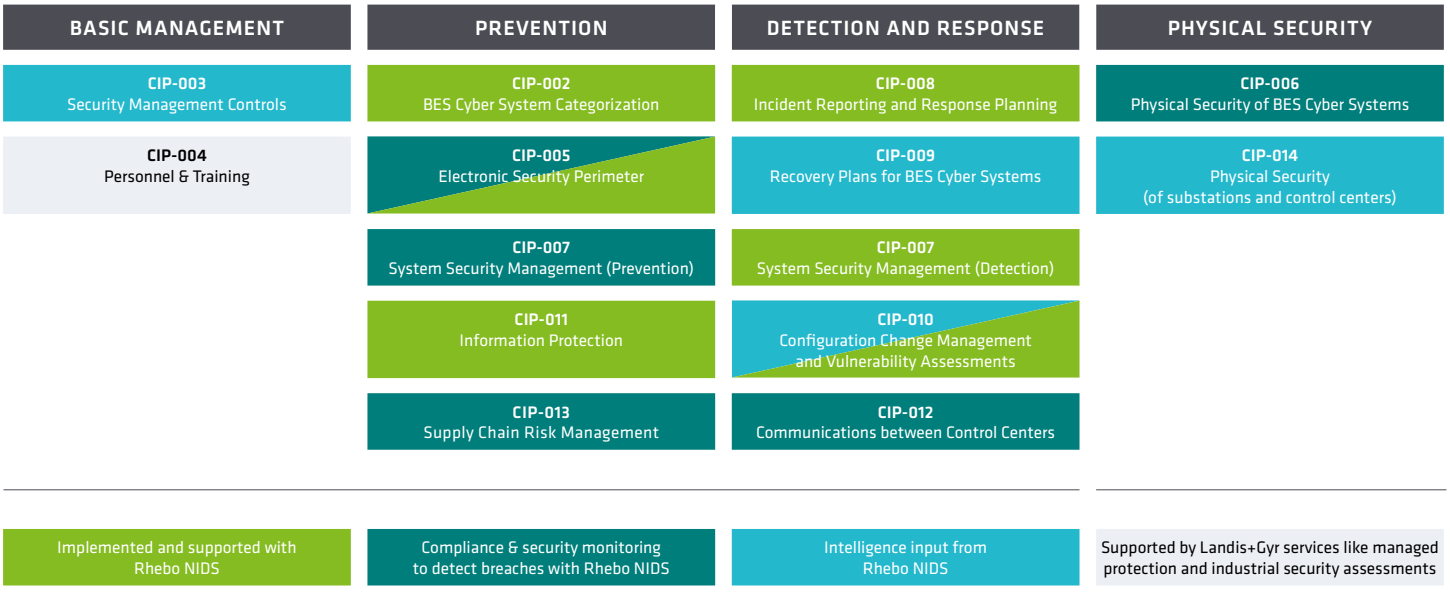


Figure 3 *The Rhebo NIDS from Landis+Gyr enhances cyber security on different levels enabling system operators to cover NERC CIP compliance on more than one requirement.*

Table 1 *Detailed description of how the Rhebo NIDS advances the compliance with the NERC CIPs (as of January 2024)*

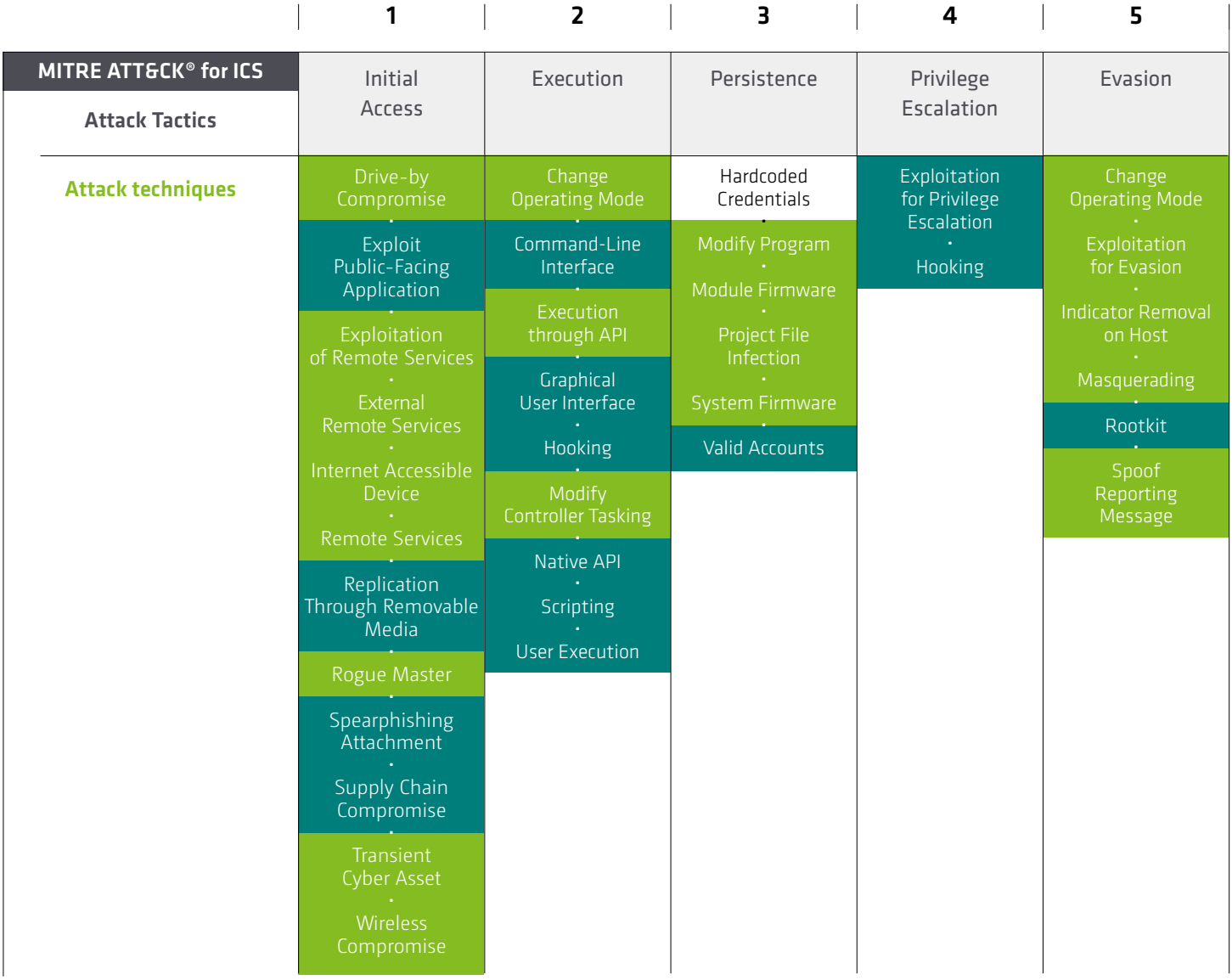
CATEGORY	CIP	TASK	HOW THE RHEBO NIDS FROM LANDIS+GYR ENABLES COMPLIANCE
BASIC MANAGEMENT	**CIP-003** Security Management Controls	Specify consistent and sustainable security management controls incl. security plan(s) and responsible roles.	**Provides valuable input** • on the perimeter, assets and vulnerabilities within the OT network, • for the definition of measures for the security plan.
	CIP-004 Personnel & Training	Select the right personnel and ensure that all personnel has a clear understanding of cyber risks, a strong cyber awareness and that they »live« cyber security.	**Implements requirement** • to provide trustworthy and experienced staff via Landis+Gyr managed services. **Provides valuable input** • for training plans by providing information on existing OT vulnerabilities, risks and interdependencies.
PREVENTION	**CIP-002** BES Cyber System Categorization	Identify and categorize BES Cyber Systems and their associated BES Cyber Assets.	**Implements requirement** • to identify BES Cyber Systems by visualizing the OT network. **Provides valuable input** • to categorize BES Cyber Systems by providing detailed asset information.
	CIP-005 Electronic Security Perimeter	Manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter.	**Implements requirement** • to detect malicious code, active vendor remote access sessions and unauthorized vendor-initiated remote connections. **Implements compliance monitoring** • to detect security policy breaches like unauthorized access, incorrect routing and direct external access to BES Cyber Systems.
	CIP-011 Information Protection	Specify information protection requirements.	**Implements requirement** • to protect BES Cyber Security Information (BCSI) from unauthorized access. **Provides valuable input** • to identify suspicious behavior of assets that host BCSI.
	CIP-013 Supply Chain Risk Management	Implementing security controls for supply chain risk management of BES Cyber Systems.	**Implements compliance monitoring** • of some supply chain cyber security risk management plan(s) through detection of e.g. publicized vulnerabilities, and vendor access by revoked hosts. **Provides valuable input** • to determine the vulnerability of vendor systems in the OT network by comparing assets' properties with CVE data base.
DETECTION AND RESPONSE	**CIP-007** System Security Management	Specify select technical, operational, and procedural requirements.	**Implements requirement** • to deploy method to detect malicious activities, • to log unsuccessful log-in attempts, detected malicious code, and to retain these logs, • to send alerts for these incidents, • to identify outdated firmware and known vulnerabilities of BES Cyber System assets. **Implements compliance monitoring** • to detect illegimate port use, • to detect inefficiencies of signature-based detection methods, • to detect unauthorized access via a new host. **Provides valuable input** • to determine vulnerability or redundancy of available ports, • to update signature-based detection methods, • to define mitigation measures using recordings of malicious activities, • to review logged events, • to identify shared accounts.

continue on next page

CATEGORY	CIP	TASK	HOW THE RHEBO NIDS FROM LANDIS+GYR ENABLES COMPLIANCE
DETECTION AND RESPONSE	**CIP-008** Incident Reporting and Response Planning	Specify incident response requirements.	**Implements requirement** • to identify, categorize and be able to respond to security incidents. • to retain records related to reportable security incidents via packet captures (pcap). **Supports** • the definition of roles and responsibilities for CSIRTs via Landis+Gyr managed services. **Provides valuable input** • to evaluate and correlate security incidents by rating the severity of a detected anomaly as well as enabling the integration of anomaly alerts into SIEM systems. • to review and update security policies, • to report security incidents to the authorities.
	CIP-009 Recovery Plans for BES Cyber Systems	Specify recovery plan requirements in support of the continued stability, operability, and reliability of the BES.	**Implements requirement** • to preserve data to determine cause of security incident via event logging and pcaps. **Provides valuable input** • to document lessons learned and update recovery plans using recorded traffic events and pcaps.
	CIP-010 Configuration Change Management and Vulnerability Assessments	Specify configuration change management and vulnerability assessment requirements.	**Implements requirement** • to monitor for configuration changes by detecting changed communication behavior, • to detect and document changes to baseline configurations that affect communication patterns, • to update the NIDS baseline to authorized configuration changes, • to detect transient media, • to regularly conduct and document vulnerability assessments via the Rhebo Industrial Security Assessment services. **Provides valuable input** • to define the baseline via full OT network visualization (Rhebo NIDS) and analysis (Rhebo Industrial Security Assessment), • to determine if configuration changes affected CIP-005 and CIP-007 measures, • to determine software identity and integrity.
	CIP-012 Communications between Control Centers	Protect the confidentiality and integrity of real-time assessment and monitoring data transmitted between control centers.	**Implements compliance monitoring** • to detect threats to confidentiality and integrity of real-time monitoring data, e.g. through man-in-the-middle attacks or unauthorized diversion of data to external servers (data extraction).
PHYSICAL SECURITY	**CIP-006** Physical Security of BES Cyber Systems	Manage physical access to Bulk Electric System (BES) Cyber Systems by specifying a physical security plan.	**Provides valuable input** • to identify all BES Cyber Systems within the critical infrastructure. • to detect physical breaches of BES Cyber Systems by detecting changes in the system's communication behavior triggered by manipulation or damage of BES Cyber Systems through the adversary.
	CIP-014 Physical Security (of substations and control centers)	Identify and protect transmission stations and substations, and their associated primary control centers (incl. 3rd party-operated facilities).	**Provides valuable input** • to identify associated control centers. • to detect a physical breach if it affects the device or network behavior, e.g. due to manipulation or damage to the infrastructure.

VI. THE CASE FOR A NIDS FOR STRENGTHENING OT CYBER SECURITY

Obviously, there is more to an NIDS than to ensure compliance with NERC CIP requirements. The cyber threat landscape has become ever more complex and sophisticated over the last years. The most comprehensive public library of attack techniques and practices on Operational Technology, MITRE ATT&CK for ICS[1], lists 110 different techniques for the 12 different attack phases (Figure 4). Of these, 12 techniques alone are reserved for initial entry.

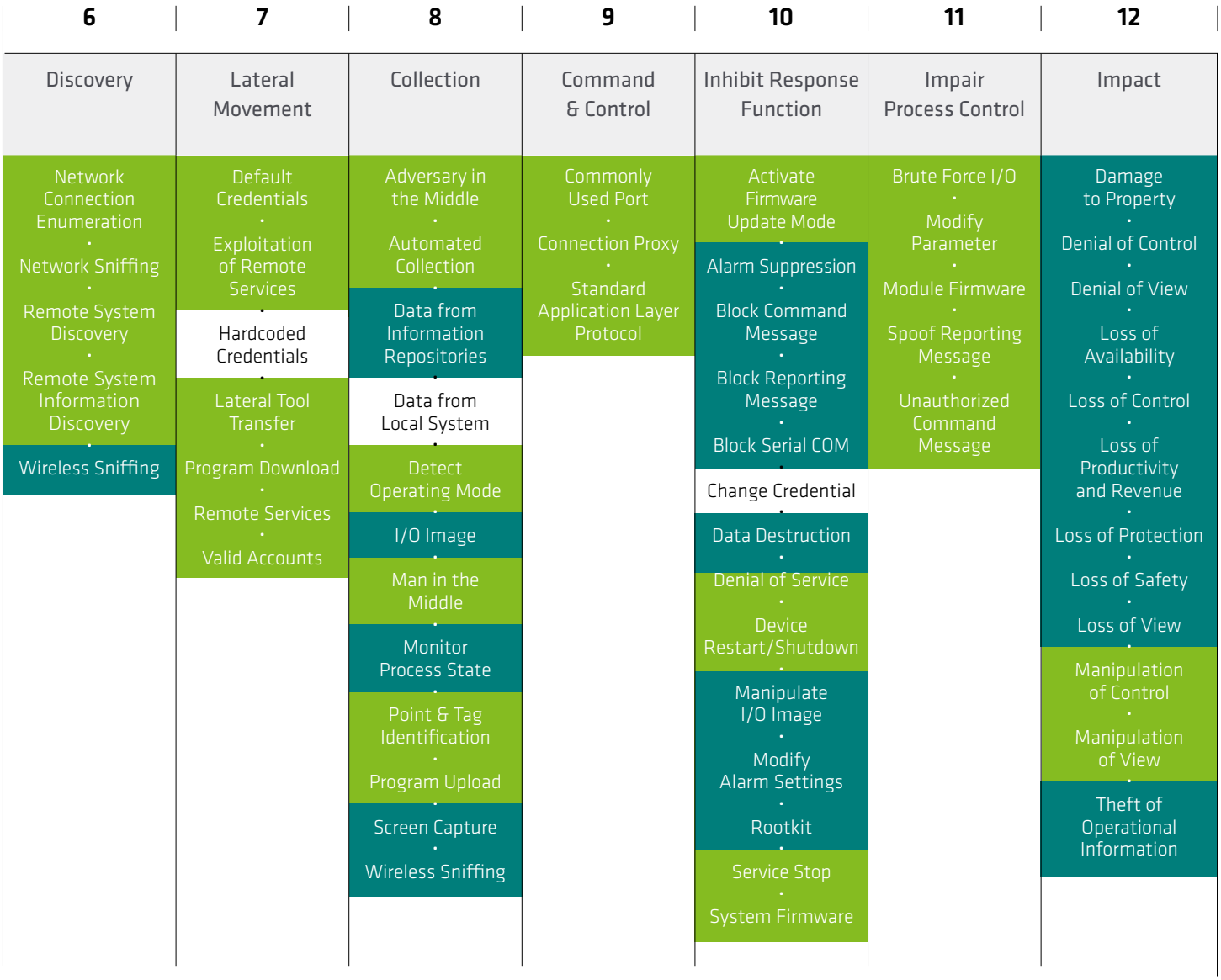


continue on next page

Techniques that can be detected on inception in real-time with industrial NIDS Rhebo Industrial Protector.
Techniques where Rhebo Industrial Protector supports detection when combined with indicators obtained from other security controls.

Figure 4 *Adversaries have a large variety of tools at their hands. This matrix also shows which activities can be detected by the Rhebo NIDS from Landis+Gyr.*

1 *https://attack.mitre.org/matrices/ics (last accessed, Jan 10, 2024)*



Today, it is commonly accepted that no system can be guaranteed to be impenetrable. There are four key reasons why this is true of OT systems:

1. In industrial environments, availability – typically 24/7/365 – takes precedence over information security.
2. Digital industrial components usually lack both default cyber security functions and the capacity for additional security functions. They also lack transparency regarding vulnerabilities and security gaps. In short, they are often ”insecure by design“ as the nearly daily ICS advisories by the CISA show. During 2023, CISA published 415 industrial control systems advisories.
3. Companies have only limited influence on
   a. the cybersecurity of a vendor.
   b. the cybersecurity and cyber awareness of service companies (e.g., maintenance companies that work on the industrial control system)
   c. the product development in OT component vendors.
4. Classic IT security tools are often inadequate for OT environments. They are also blind against zero-day vulnerabilities, which – due to their ”insecure by design“ characteristics – are expected to be widespread in OT components.

There is no reason to trust perimeter security and the components’ design (alone). And why should one? Nation states don’t rely solely on border security, either. They also depend on institutions which detect any perimeter security breach and in-house threats within their borders.

In North America, agencies like the FBI or the CSIS form this second line of defense to ensure the inner security of the USA and Canada, respectively. In OT the equivalent is a network intrusion detection system (NIDS).

This concept of multi-level security is called Defense-in-depth which ”involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another.“[2] While firewalls and authentication build the first line of defense, a NIDS forms the second line of defense (Figure 5).

> *In a nutshell, an OT NIDS is the all-seeing eye within an electrical substation and grid detecting any wrongdoing that might threaten the distribution network.*

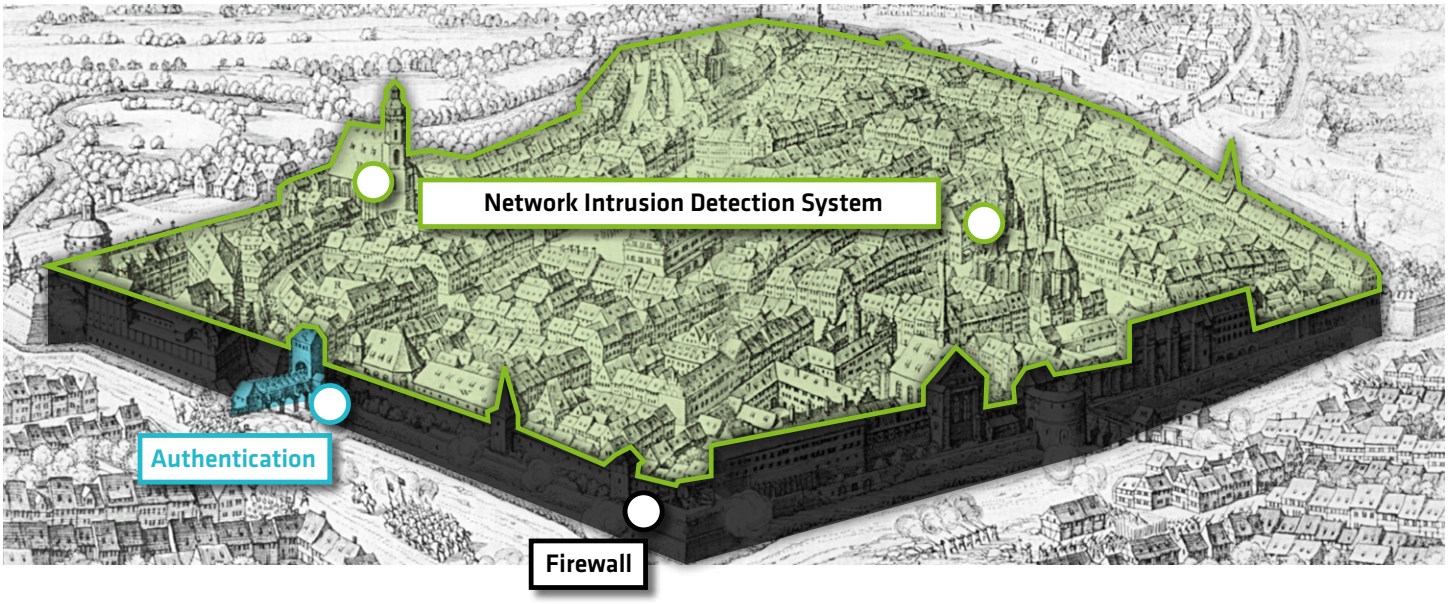


Figure 5 *The Rhebo NIDS from Landis+Gyr forms the inner security layer of an OT network that detects even successful security breaches.*

VII. CASE STUDY: HOW A NIDS HELPED SAVE ONE NATION'S GRID

THE INNER WORKINGS AND BENEFITS OF A NIDS COULD BE OBSERVED IN MAY 2023 WHEN DANISH ENERGY COMPANIES BECAME VICTIMS OF LARGE-SCALE CYBER ATTACKS.

It all started with a new vulnerability on a type of firewall (by Zyxel) commonly used by Danish critical infrastructures. SektorCERT, a non-profit organization, was already on high alert when on May 11, 2023, alarms in their nation-wide NIDS went off. Naturally, the firewalls themselves did not see their own compromise but instead willingly handed over credentials and configuration information to the attackers.

Initially, 11 companies were targeted very specifically by a single adversary. As SektorCERT wrote in their report[3]: *"Our assessment was that it was an attacker who did not want to make too much noise, but wanted to 'fly under the radar'."* Over the following weeks, 11 more companies got compromised.

A few companies went offline to prevent threat propagation. One critical infrastructure lost view of their remote BES and had to fall back to manual operation. Apart from that, the Danish people enjoyed undisturbed electric supply because SektorCERT was able to detect the security breaches early on, even with firewalls disabled due to widespread compromise. And that is thanks to SektorCERT's expertise, commitment and: **a network intrusion detection system.**

SektorCERT runs a huge self-developed network monitoring with anomaly detection operation not unlike the Rhebo NIDS from Landis+Gyr. They continuously monitor the entire communication stream from, to and within their members' networks with an NIDS, and look for anomalous network behavior that does not fit with the expected pattern. In May 2023, this enabled SektorCERT to detect the attacks (some of them 0-day exploits) in their early stages and react quickly for a successful mitigation.

2 *e. g. NIST SP 800-171, NIST SP 800-172, NISTIR 8183*

3 *For the full timeline of how the attacks and incident response unfolded, read the SektorCERT report: https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf*

VIII. CONCLUSION

Network intrusion detection systems are a vital component in enhancing NERC CIP compliance for electrical substations. These systems not only help in the early detection and mitigation of cyber threats but also aid in maintaining records for compliance reporting.

The Rhebo NIDS from Landis+Gyr enables cybersecurity teams to establish OT visibility and early detection of security incidents. The simple deployment and clean dashboard do not require complex configuration processes and allow security officers to easily integrate the OT monitoring into their daily work routine.

Implementing NIDS is a proactive measure that not only safeguards the distribution grid operations but also ensures the security and reliability of critical infrastructure in accordance with NERC CIP standards. Power utilities must recognize the critical importance of NIDS in achieving and maintaining NERC CIP compliance, and invest in these systems to bolster the security of their electrical substations.

IX. OT SECURITY IN 3 STEPS WITH LANDIS+GYR

1

OT RISK ANALYSIS AND VULNERABILITY ASSESSMENT

The first easy step to OT security:
Rhebo Industrial Security Assessment

Cybersecurity starts with visibility.

The Rhebo Industrial Security Assessment is an OT cyberrisk and vulnerabillity analysis that provides a deep understanding of your ICS / OT assets, risk exposure as well as recommendations for effective measures for hardening the systems.

You profit from

- the identification of all devices and systems within the OT including their properties, firmware versions, protocols, connections and communication behavior (Asset Discovery & Inventory);
- an in-depth analysis of existing CVE-documented vulnerabilities;
- the identification of risk exposure, security gaps and technical error states;
- a detailed audit report and workshop with actionable recommendations.

2

OT NETWORK INTRUSION DETECTION SYSTEM (NIDS)

The seamless transition to comprehensive OT security:
Rhebo Industrial Protector

Cybersecurity does not end at the network perimeters.

The NIDS Rhebo Industrial Protector combines OT monitoring with next generation OT threat and intrusion detection to detect anomalous communication within OT networks. It advances the existing perimeter firewall security by integrating OT-dedicated, network-based anomaly detection that reports security incidents in real-time while not interfering with the critical industrial processes.

You profit from

- real-time visibility of communication behavior of all OT and ICS assets (protocols, connections, frequencies);
- real-time reporting and localization of events (anomalies) that indicate cyberattacks, manipulation or technical error states;
- early identification of attacks via backdoors, previously unknown vulnerabilities and internal adversaries that firewalls fail to detect (defense-in-depth).

3

MANAGED DETECTION AND RESPONSE

The recipe to peace of mind.
We monitor so you don't have to:
Rhebo Managed Protection

Cybersecurity needs resources and know-how.

With Rhebo Managed Protection, we support you in operating the OT NIDS Rhebo Industrial Protector, in particular in evaluating and responding to incidents, as well as continuously reviewing and improving mitigation mechanisms.

You profit from

- expert support for running the OT NIDS;
- fast forensic analyses and assessment of OT security incidents;
- fast actionability in case of incidents;
- regular OT cyber risk analyses and vulnerability assessments for continuous improvement.

EXPLORE LANDIS+GYR AND ITS RHEBO SECURITY PORTFOLIO FOR ELECTRICAL UTILITIES

Landis+Gyr's OT Security
Security for electrical substations, grids and utilities.

Rhebo Industrial Security Assessment
OT risk analysis and vulnerability assessment

Rhebo Industrial Protector
The network intrusion detection system (NIDS) for OT security

DOWNLOAD AT WWW.LANDISGYR.COM/SOLUTION/CYBERSECURITY

ENSURE NERC CIP COMPLIANCE AND SECURE YOUR DISTRIBUTION SUBSTATION OPERATIONS

CONTACT US

WWW.LANDISGYR.COM/CONTACT | +1 855 3455 454

ABOUT LANDIS+GYR

Landis+Gyr is the leading global provider of integrated energy management solutions for the utility sector. Offering one of the broadest portfolios, we deliver innovative and flexible solutions to help utilities solve their complex challenges in smart metering, grid edge intelligence and smart infrastructure. With sales of USD 1.8 billion, Landis+Gyr employs approximately 5,600 people in over 30 countries across five continents, with the sole mission of helping the world manage energy better.

www.landisgyr.com

ABOUT RHEBO

Rhebo provides simple and effective cybersecurity solutions for Operational Technology and distributed industrial assets for the energy sector, critical infrastructure and manufacturing. The German company supports customers with OT security from the initial risk analysis to managed OT monitoring with intrusion & anomaly detection. Since 2021, Rhebo is part of the Landis+Gyr AG.

www.rhebo.com

Landis+Gyr & Rhebo 30000 Mill Creek Avenue, Suite 100 | Alpharetta, GA 30022 | USA