# Standards-based Security for Energy Utilities

White Paper

## Introduction

There are a multitude of factors increasing the number and severity of cyber threats and vulnerabilities in the energy sector. With the adoption of intelligent distributed technologies that enable remote control and/or monitoring and advanced analytics, more critical data is traversing communication networks necessitating stronger security. In this paper we examine the unique aspects of cybersecurity in energy along with the various applicable industry standards and best practices for reducing risk.

## Major Drivers for Change

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) is focused on control system security issues with the objective of providing information to help in reducing risk. ICS-CERT analyzed a subset of the total number of vulnerabilities reported and determined that the average Common Vulnerability Scoring System (CVSS) score for reported vulnerabilities for the year 2016 was 7.8/10. And 73.8 percent of the vulnerabilities, have CVSS scores of seven and above. A CVSS score of seven or above indicates that these vulnerabilities, if exploited, have the potential to have a high or critical impact. The majority of vulnerabilities tracked by ICS-CERT were most commonly associated with the energy sector. A successful cyberattack in the energy sector could have important consequences or implications, beyond those of just the facility or the organization, due to the critical nature of their services to other organizations that rely on energy to function. One of the illustrious cases in 2016 was that attackers successfully blacked out a portion of Kiev, the capital city of Ukraine, using malware capable of deleting data and causing physical damage to industrial control systems. The energy industry is expected to continue to be a high priority target for threat actors, particularly given its importance to national and economic security. However, by acknowledging the threats, performing a comprehensive and recurring risk assessment, and implementing a mitigation strategy, organizations can be in position to prevent cyberattacks.

There are several factors which could cause an increase in threats and vulnerability trends in the energy sector. Until recently, utilities have primarily relied on serial comunications or a dedicated and isolated control and automation network. With the evolution in device technologies and support for more advanced data processing mechanisms deployed at field and central locations, more data needs to be transferred from the field to a central location in near real-time. Earlier communication technology needed to evolve to provide greater bandwidth. Convergence of operational technology (OT) and information technology (IT) infrastructure has enabled bidirectional flow of information and more advanced data analysis, interconnecting more devices and systems than ever before.

Secure connectivity enables both energy providers and consumers alike to reap the benefits of an increasingly connected world. It is critical that security be standards-based so that vendors and asset owners/operators can identify security vulnerabilities and develop effective mitigation strategies in a timely manner. Standards-based security solutions help ensure interoperability and availability of affordable and secure solutions in a rapidly evolving environment. It is achieved by combining robust digital certificate-based authentication with strong encryption at the network level to conceal device and other sensitive information as well as implementing application layer security to ensure authentication, authorization and accounting on any operations. There are several industry standard initiatives, of which NERC CIP, IEEE1686 and IEC 62351 are the most advanced and should be considered by utilities in developing overall cybersecurity policies and practices.

## Overview of Energy-Focused Cybersecurity Standards

### IEEE1686 and C37.240

**Intelligent Electronic Devices (IED) Cybersecurity Capabilities**
This standard describes IED cybersecurity capabilities. It also defines functions and features that must be provided in substation IEDs to accommodate critical infrastructure protection programs. It addresses security in terms of access, operation, configuration, firmware revision, and data retrieval from IEDs. Security functionality with respect to confidentiality of the transmission of data is not part of this standard. The system aspects are addressed by the IEEE C37.240.

### IEC 62351

**Power Systems Management and Associated Information Exchange – Data and Communication Security**
A goal of IEC 62351 is the assurance of end-to-end security, which can be achieved on different OSI levels. The standard comprises multiple parts to cover the security of data in motion as well as at rest. The standard also provides general guidelines for designing power systems with security in mind. Portions of IEC 62351 covers different scenarios and applies directly to substation automation deploying IEC 61850 and IEC 60870-x protocols as well as to adjacent communication protocols supporting energy automation, like ICCP (TASE.2) used for inter-control center communication.

### NERC CIP

NERC CIP standard is one of the mandatory standards issued by NERC in order to protect critical infrastructures and is used to secure bulk electric systems. NERC CIP provides a suite of standards that ensures the overall security of computing systems that directly manage the power grids and all supported subsystems or resources.

These standards are mapped into four quadrants based on the levels of detail by which each addresses the security requirement and solution:

- **Details for Operation**: Organizational and procedural means applicable for all or selected actors.
- **Devices and Equipment**: Directly influences component and/or system functionality and needs to be considered during product design and/or development. It addresses technology to be used to integrate a security measure.
- **Design Details**: Describes the implementation of security in enough detail to achieve interoperability between different vendors' products for standards on a technical level and/or procedure to be followed for standards addressing organizational means.
- **Completeness**: Addresses not only one specific security measure but addresses the complete security framework, including technical and organizational.

Mapping security standards per the above classification provides scope on the level of detail each standard address on an abstract level. Moreover, it also addresses the relevance of the standards for organizations (utilities /operators) as well as products and services (manufacturer or service providers).

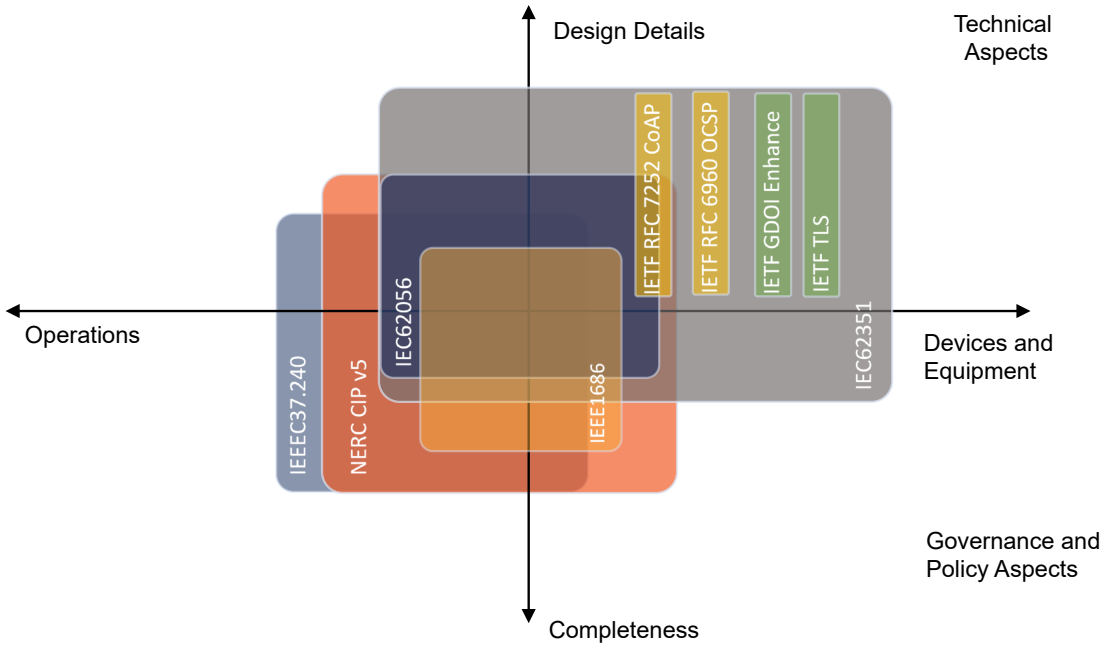



Diagram recreated and modified from source: CEN-CENELEC-ETSI Smart Grid Coordination Group Report

*Figure 1: Quadrant Mapping of Standards*

## Cybersecurity Best Practices

Best practices for cybersecurity should include both technological as well as operational controls of the system. Technological control includes strategies adopted for cybersecurity protection, detection of vulnerabilities and response to incidents. Operational aspects include polices, procedure and guidelines defined by the utilities and industries to effectively manage attacks. Utilities must continuously monitor and adapt these practices as attackers continue to evolve and find new ways to access critical systems.

Below is the mapping between technological controls with the various security standards defined for utilities.

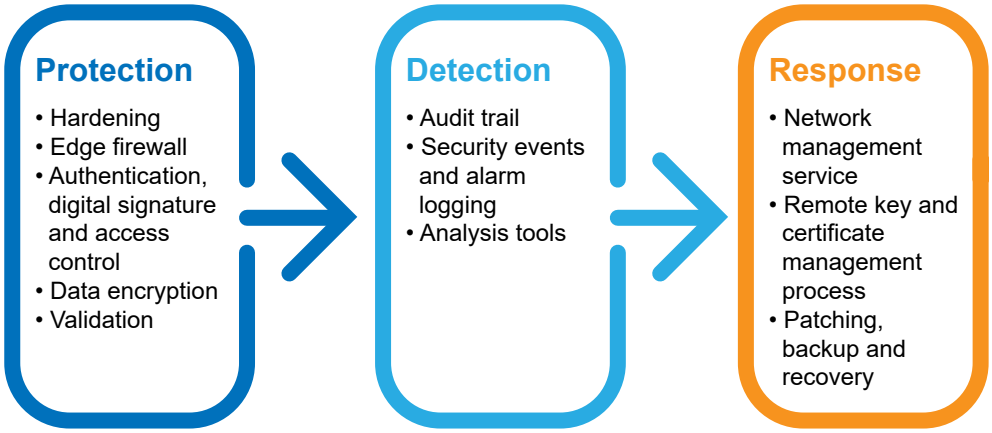



*Figure 2: Mapping of Technological Controls*

WHITE PAPER

## Protection

**Hardening** of the devices is the first step which needs to be part of protection. Any devices or equipment deployed on a physically secured system should have restricted access for management and operation of the device. Any super user or root access to the devices should be provisioned only for local access. For remote access by system or security administrator should always require two-factor authentication to ensure that attackers cannot get into the system or devices even if one of the authentication mechanisms is compromised. All passwords should be enforced as per password policy outlined in CIP-007-5 R5 (5.5) and it should be rotated at a minimum, every 15 months CIP-007-5 R5 (5.6).

CIP-007-6 R5.7 also mandates that if any user has failed to login to the device after a defined maximum number of retry attempts, their account should be locked out for a specified period as defined by the asset owners.

All perimeter equipment must have a built-in firewall as per NERC CIP 005. It should be possible for users to control the physical port as well as the logical port of the devices. It is an important defense tool which protects network assets from external attacks. Firewalls should be flexible enough to be configured for inbound and outbound traffic policies on each interface and local ports.

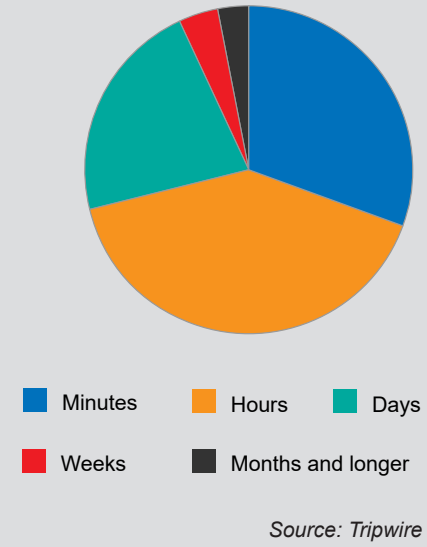
After physical protection the next priority is for security of data in motion, at rest and in use. Confidentiality and integrity of the data is ensured by encrypting the data in all the states mentioned above. Algorithms and protocols used for data encryption should be per the standard to have a truly vendor independent system. IEC62351-3 substandard defines the standard mechanism on implementing TLS-based security for all TCP-based communication used in utility networks. This is a generic standard which can be applied across all utility protocols including DNP3.0, IEC 60870-5-104, Modbus, IEC 61850, etc.

**230,000** new malware samples are produced every day — and this is predicted to only keep growing.

*Source: Panda Security*

By 2020 there will be roughly **200 billion** connected devices

How long would it take to detect configuration changes to endpoint devices in organization's network?




*Source: Tripwire*

Associated services including network management, time synchronization, file transfer terminal access used in the utility network, should mandate the use of only the secure version of the protocols. Network management should be enabled only if the devices have Simple Network Management Protocol version 3 (SNMPv3) or IETF RFC 7252 CoAP; similarly, only Network Time Protocol version 4 (NTPv4) should be used. File transfer from devices and system if used should mandate only Secure File Transfer mechanism (SFTP/SCP). Online and offline device access should be over a secure link. If any offline configuration tool connects with a device, it should be compliant with IETF TLS 1.2 tunnel. Web access for configuration or monitoring should be over Hyper Text Transfer Protocol Secure (HTTPS) or using a secure proxy channel connected on a TLS1.2 tunnel.

As more and more devices and software system are connected and exchange information, there is a strong need for device identification and access control, specifically, each device and users should be required to present authentication credentials and be verified by an authority to establish the trust before allowing connectivity to the system. Centrally deployed Identity and Access Management (IAM) systems based on Pubic Key Infrastructure (PKI) should act as authority for the authorization of an entity. It ensures that access to a utility system is granted only to authenticated users, groups and software services. PKI cryptographic technique enables entities to securely communicate (encrypt communications using TLS), and reliably verify the identity of an entity via X.509 certificates with digital signatures. Standards for use of certificates within the utility industry includes IEC62351-8 (role-based access control) using attribute certificate or IETF RFC 6960 OCSP.

A digital signature can be used to validate the source and integrity of any information shared between entities. Firmware, configuration file and licenses are examples of the information which needs to be transferred to devices. Information should only be used if the signature appended in it is validated successfully. Security standard IEC 62351-5 defines challenge-response mechanism in telemetry protocols such as DNP3.0 (IEEE1815) and IEC 60870-5 derivatives to verify the control operations in real time. IEC 62056 standard defines authentication and encryption of data used for DLMS-COSEM protocol for meter data exchange.

## Detection

Utilities should invest in threat detection technologies to receive an alert of a potential threat. Monitoring and threat detection tools help to identify and locate intrusions and anomalies in the system. Some of these solutions can also isolate threats early and occlude the attack which could potentially spread to other parts of the system. Detection systems need to identify information about the device type, location, activity, etc. Furthermore, this information must be captured, analyzed, stored, and shared among auditors and security analysts. IEEE1686 and CIP 007 mandates logging this information as syslog for centralized analysis. Syslog can be used to log security incidents generated by system elements as well as user actions in the form of audit trails. User access logs can track operations made to device settings and configuration. It is also mandatory to ensure that all devices have adequate backup for at least 90 days for root cause analysis. IEEE1686 also defines events and alarms which need to be captured by any IEDs such as device reboot, unauthorized access, updates, setting changes, etc.

**81** percent
of data breach victims do not have a system in place to self-detect data breaches.

## Response

A proactive response plan includes policy and operational mechanisms for the management of cybersecurity vulnerabilities reported or detected in all the devices and software, to manage the risks arising thereof. Utilities should ensure that all systems and devices are updated and patched regularly. Vendors should regularly monitor the security vulnerabilities in their products. Whenever a security vulnerability is reported, it should be thoroughly evaluated and analyzed in detail and once confirmed, notify in a public forum to share the information with product users and keep them updated. Alternately or additionally, the reporter may also directly submit the report to ICS CERT, CERT-IN or any other national CERT body designated that handles security vulnerabilities.

If the system has initiated an attack response plan it should document the tools and procedures which help in recovering the system from the attack and analyzing the data to help accelerate system recovery from a similar attack in the future. The response plan should include in-depth analysis of the incident including logs, event and alarm lists which could indicate the path of the attack.

A single data breach will cost the average company **$3.8** million.

And will exceed **$150** million by 2020.

*Source: Juniper Research*

Average number of days to resolve a cyber-attack is **$32** days

*Source: KRYPSYS*

A recovery strategy should also include redundancy and regular data backup to ensure restoration of operations. Response is effective only with strong policies and procedures.

## Conclusion

Cybersecurity solutions for utilities is unique. Systems used in the utility industry often have a life of at least 20 years unlike what is seen in other industries where technology is updated more frequently. Therefore, it is critical to design a security solution which incorporates a strategy to protect legacy and newer devices, protocols and software to meet the requirement of transmission and distribution operators, regulatory bodies along with various new stakeholders including IT and OT technical experts, compliance and analytics team.

## About Kalkitech

Kalkitech helps energy utilities around the globe in enabling and transforming grid communications, improving reliability and energy efficiency. Its solutions enable customers to implement mission-critical applications ranging from advanced metering and distribution automation to wide area monitoring, substation automation and power plant optimization. Kalkitech invests extensively in research and development in areas such as power systems engineering, thermal engineering, control theory and communication and information technology. By building expertise, the company creates robust standards-based communication and optimization solutions and products for modernization of utilities, helping them to harness the power of grid data.

WHITE PAPER

References


https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf

https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/FY2016_Industrial_Control_Systems_Assessment_Summary_Report_S508C.pdf

http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx

https://www.pandasecurity.com/mediacenter/press-releases/all-recorded-malware-appeared-in-2015/

https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

https://www.krypsys.com/hacking-2/cyber-attacks-becoming-increasingly-costly-can-business-really-afford-protect-attacks


Kalkitech


Corporate Headquarters: **Bangalore, India**

U.S. Headquarters: **Campbell, California**

Sales Office: **United Arab Emirates**

www.kalkitech.com

sales@kalkitech.com



Version: 1.01.012019