TXOne Networks

2023
/Q1

# Achieving Energy Transformation:
## Building a Cyber Resilient Smart Grid

txOne networks

# Achieving Energy Transformation:

## Building a Cyber Resilient Smart Grid

txOne networks

# **Achieving Energy Transformation:** Building a Cyber Resilient Smart Grid

## Table of Contents

# Introduction

Electricity is closely linked to human daily life, and the applications of electricity can be seen everywhere, from household appliances to industrial power systems. However, in recent years, due to the impact of extreme weather conditions worldwide, experts from the Intergovernmental Panel on Climate Change (IPCC) believe that the danger of climate change has never been so dire.[1] Many countries, including the United States, Japan, South Korea, and the European Union, have pledged to achieve net-zero emissions by 2050 or soon thereafter, with the aim of limiting global warming to 1.5°C and avoiding catastrophic consequences for our planet. From 2021 to 2050, global electricity generation is expected to more than double under the NZE scenario. Global total electricity generation is expected to grow by 3.2% annually from 2021 to 2030, and then by 3.4% annually from 2030 to 2050, compared to a growth rate of 2.5% for global electricity generation from 2010 to 2021.[2] The impact of the Russian-Ukrainian conflict has only worsened the issue of energy shortages. Currently, power companies around the world are prioritizing the development of stronger grid resilience, ensuring stable power supply, energy conservation and carbon reduction, and accommodating more renewable energy sources as important development goals for the future. Advanced countries have proposed policies to transform their power grids so that their traditional power transmission system is enabled to cope with increasingly complex grid dispatch. To meet these needs, the smart grid that combines the power transmission system with information and communication technology has emerged.

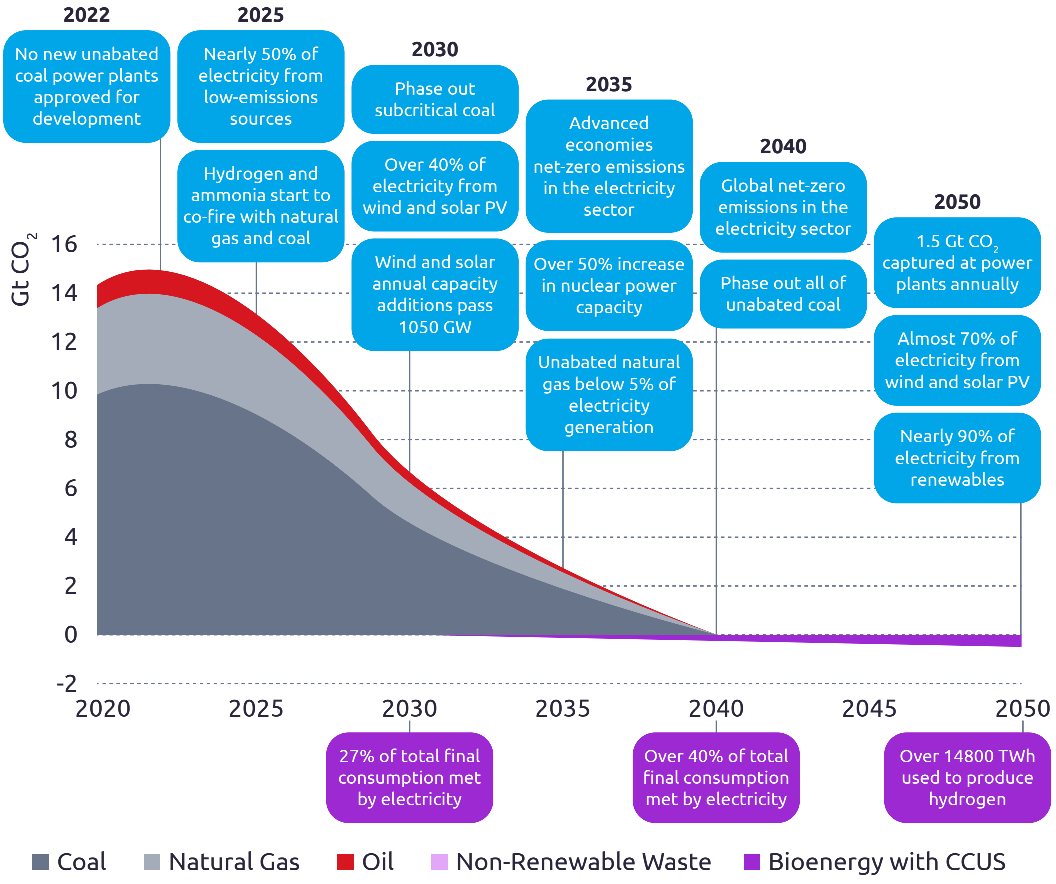
[1] *IPCC Working Group II report, Climate Change 2022: Impacts, Adaptation and Vulnerability, IPCC, February 28, 2022.*

[2] *IEA , "World Energy Outlook 2022", International Energy Agency, November 2022.*

# A Roadmap to Net-Zero Emissions by 2050

In the NZE scenario, low-emissions sources of electricity, such as renewables, nuclear power, hydrogen, ammonia, and fossil power plants with carbon capture, utilization, and storage (CCUS), are rapidly expanding. They are expected to overtake unabated fossil fuels just after 2025 and reach three-quarters of total generation by 2030, almost twice the amount reached in 2021.[2]

Under the NZE Scenario, the electricity sectors in advanced economies are expected to reach net-zero emissions by 2035, and globally by 2040. At that point, low-emissions sources are projected to provide nearly all electricity generation, as shown in Figure 1. This makes electricity the first energy sector to reach net-zero emissions in the NZE Scenario, and it helps to bring about emissions reductions in other sectors as they increasingly look to electricity to meet rising demand for energy services.



**2022**
No new unabated coal power plants approved for development

**2025**
Nearly 50% of electricity from low-emissions sources

Hydrogen and ammonia start to co-fire with natural gas and coal

**2030**
Phase out subcritical coal

Over 40% of electricity from wind and solar PV

Wind and solar annual capacity additions pass 1050 GW

**2035**
Advanced economies net-zero emissions in the electricity sector

Over 50% increase in nuclear power capacity

Unabated natural gas below 5% of electricity generation

**2040**
Global net-zero emissions in the electricity sector

Phase out all of unabated coal

**2050**
1.5 Gt $CO_2$ captured at power plants annually

Almost 70% of electricity from wind and solar PV

Nearly 90% of electricity from renewables

27% of total final consumption met by electricity

Over 40% of total final consumption met by electricity

Over 14800 TWh used to produce hydrogen

IEA.CC By 4.0.

Electricity is the first sector to reach net-zero emissions in 2040, tapping a wide set of low-emissions sources and enabling other sectors to cut emissions through electrification

*Figure 1: The Net-Zero Carbon Emission Blueprint for the Power Industry*[2]

[2] *IEA , "World Energy Outlook 2022", International Energy Agency, November 2022.*

# Key Factors for Achieving Net-Zero Emissions: Smart Grid, Renewable Energy, and Cybersecurity

## Smart Grid Technology

A smart grid is essential for maintaining a secure and stable power supply. Advanced countries have proposed policies to transform their power grids, allowing traditional power transmission systems to cope with increasingly complex grid dispatch. This has led to the development of a smart grid that combines the power transmission system with information and communication technology. As of now, the intermittent and unpredictable nature of renewable energy presents challenges in the development of renewable energy. Therefore, the collection and use of various data is crucial, and the challenges of renewable energy are transformed into opportunities through smart technology. In addition, the use of new energy storage systems can help transfer the demand for night-time peak power supply, resolving the pain points of renewable energy supply and driving energy storage opportunities.

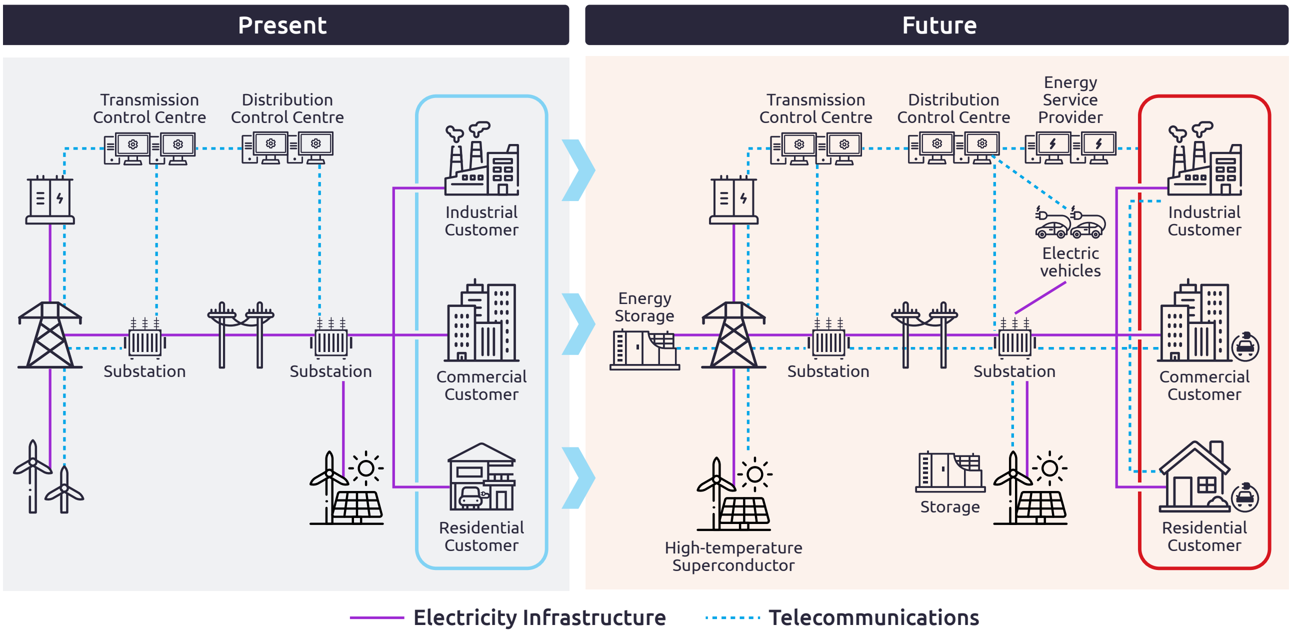


*Figure 2: Architectural Evolution of Smart Grid*[3]

## Renewable Energy

In the NZE Scenario, renewables become the dominant source in the global electricity sector. The share of renewables in electricity generation increases from 28% in 2021 to over 60% in 2030, and nearly 90% in 2050. The total installed capacity of renewables triples by 2030 and rises sevenfold by 2050. Annual additions to renewable capacity increase from 290 GW in 2021 to nearly 1,200 GW in 2030, and average above 1,050 GW from 2031 to 2050. This investment in renewables will drive a cumulative natural investment of $29.6 trillion globally from 2021 to 2050. The growth of renewables

[3] *IEA, "Technology Roadmap: Smart Grids", International Energy Agency, Paris, 2011.*

will vary depending on each country's natural resources (such as land, location, and terrain) and economic and social conditions. For instance, advanced countries like Europe and North America have maintained at least a 30% market share of renewable energy installations, supported by stable policies and economic incentives for decarbonization. This is expected to drive growth in energy storage and electric power infrastructure investment in the future.

## Cybersecurity for Smart Grids

As the global economy increasingly relies on dependable and stable power supply, power security is critical in the NZE scenario. This is due to the expanding number of users and the evolution of natural sources of power supply coupled with the expansion of power usage. The smart grid enables bidirectional communication between the grid and the sensors installed in various locations. These sensors continuously transmit production data to the grid in the form of data packets. Although this is an advancement, this also demonstrates the need for robust cyber resilience. However, cyber resilience has posed a challenge for global organizations, particularly in the power industry. Over the years, we have seen the energy industry become a target for criminal purposes or other malicious reasons. The sophistication of attack methods is accelerating, and the capability of exploiting OT systems (such as Industry 4.0) is increasing, leading to a precipitous rise in cyber threats to the power industry. In the past, only cybersecurity professionals working for utility companies understood the vulnerable end products and protocols involved. However, we are now facing a series of threats executed by highly talented adversaries specialized in targeting the industrial sector. For instance, Taiwan Power Company's information system was attacked over 5.9 million times in a single day. Clearly, security is already crucial at this juncture and will only become more so in the future. Additionally, cybersecurity in the energy sector has been established around the need to increase efficiency by increasing connectivity within organizations. The security of many power utilities is based on the assumption of flexible operations in a trusted environment. However, as power utilities increasingly use digital technologies to improve efficiency and create system-level solutions to balance the grid, companies are inadvertently creating new cyber risks. The power system is one of the most complex and critical systems among all infrastructure types and serves as the backbone of economic activity. Large-scale events like blackouts may have social and economic impacts on households, businesses, and critical institutions. For example, a six-hour winter blackout in mainland France could result in total losses of over €1.5 billion ($1.7 billion).[4]

This report aims to explain the advanced cybersecurity challenges related to smart grid modernization, cybersecurity trends, and potential risks in the future power grid. It suggests incorporating the minimum requirements for best practices and deployment related to these cybersecurity challenges.

[4] *Rosa Kariger, Pierre-Alain Graf, "Hackers are causing blackouts. It's time to boost our cyber resilience", WEF, March 27, 2019.*

# A Perspective on Cybersecurity in Contemporary Smart Grids

The smart grid, which combines cyber and physical components, is essential for the effective transfer of electricity from power plants to consumers. It consists of a number of operations, including the production, distribution, transmission, and sale of electricity. The power grid serves as a direct route between power providers and consumers during the transmission and distribution stages. To put it simply, the power grid acts as a conduit for the delivery of electricity to homes, allowing users to get power quickly by flipping a switch.

While the traditional power grid lacks the resilience to integrate large amounts of renewable energy, resulting in unstable power supply, the smart grid has the capability to integrate various renewable energy sources and guarantee a stable supply of energy by using monitoring systems. With the increasing prioritization of environmental protection and sustainable development, the energy industry is transitioning from traditional power grids to smart grids, utilizing new technologies such as distributed architecture, two-way communication, and advanced control systems to collect information on power supply and usage, adjust power distribution, and achieve energy savings.

*Table 1: Differences Between Conventional and Smart Grids*

| Transformation of Power Grid | | Conventional power grid | Smart Grid |
|---|---|---|---|
| **Power Framework** | Power Generation Sources | Abuse of privileges by staff (insider attack) | The principle of least privilege is applied to production tools or equipment systems |
| | Methods of Power Generation | Centralized power generation | Concurrent use of centralized and decentralized power generation |
| | Energy Loss | High energy loss | Low energy loss |
| | Troubleshooting | • Slow and inaccurate fault localization<br>• Manual recovery<br>• Large-scale power outage | • Timely and accurate fault localization<br>• Self-recovery<br>• Localized power outage |
| | Device Inspection | Manual inspection/testing | Remote inspection/testing |
| **Network Connection** | Data Transmission | One-way communication | Two-way communication |
| | Connected Devices | Few sensors | Large-scale deployment of sensors, communication devices, and control systems |
| | Smart Meter | Electronic/mechanical metering vs manual reading | Digital, remotely readable meters |

| Transformation of Power Grid | | Conventional power grid | Smart Grid |
|---|---|---|---|
| **Data Management** | Processing Information Volume | Limited data | Complete and containing a large amount of user data from smart meter |
| | Electricity Usage Data Management | Difficult to manage electricity consumption | Access to real-time electricity pricing information<br>Changes in electricity consumption behavior to optimize energy usage and reduce costs<br>Reduces strain on power grid by reducing peak demand and overall electricity consumption |
| | Peak Electricity Usage | Difficult to assess and master | Real-time management of peak demand |

Due to fundamental differences in architecture and functionality between traditional and smart grids, smart grids are inherently more complex than traditional grids, which may affect the cyber risks they face. The following outlines the main differences between smart grids and traditional grids from a cybersecurity perspective:

## Architecture:

Traditional grids usually adopt a centralized architecture, where electricity is generated in large power plants and distributed to consumers through transmission and distribution networks. On the other hand, smart grids have a more distributed architecture, where electricity is generated from various sources, including renewable energy such as solar panels and wind turbines, and distributed through a network of sensors, communication devices, and control systems. However, the complexity of smart grids makes it more difficult to identify and address cyber risks, as more potential attack vectors and vulnerabilities need to be considered.

## Communication:

Traditional grids have a one-way power flow from centralized power generation, whereas smart grids have a two-way power flow, which allows for greater flexibility in distribution and the ability to exchange surplus and shortage of power between regions, reducing energy waste. Smart grids rely on bidirectional communication between various components of the power grid, including sensors, meters, and control systems. This allows for real-time monitoring of the power grid, which helps optimize power generation and even distribution.

## Data:

Traditional grids operate based on precedents stemming from historical experience, while smart grids have the ability to integrate current information, self-diagnose, and self-repair. This is primarily done through the collection of large amounts of data by smart grids, including energy use, power quality, and grid performance. While this data is valuable for optimizing the power grid, it also presents significant cyber risks, as attackers may attempt to access and steal this data for malicious purposes.

In summary, although both traditional and smart grids face cyber risks, the distributed architecture, bidirectional communication, and data-rich environment of smart grids present additional challenges and complexities as well as a larger potential payoff for hackers.

# Historical Overview of Cyberattacks in the Energy Sector

In this chapter, we have compiled real attack cases in the power industry from 2010 to 2022. By reviewing the history of cyber attacks in the power industry, organizations can gain a better understanding of attackers' infiltration paths and threat scenarios. It is noteworthy that many of the attack methods in these cases were compound attacks, which employ multiple infiltration paths and attack techniques to achieve their goals. This understanding can assist organizations in formulating more effective cybersecurity strategies and defense measures. It can also help them improve their incident response plans and develop better training and awareness programs to mitigate future attacks.

## 1. Portable media going uninspected can easily lead to threats breaching air-gapped environments

Electric grids are typically physically isolated from other networks, such as IT networks, to prevent lateral movement. However, hackers can still attempt to breach this physical isolation by infecting portable media. Some employees of power utilities may unknowingly connect infected portable media to the OT devices in the electric grid and thus disrupt the air-gapped system. For example, in 2010, the first worm virus targeting industrial control systems, Stuxnet, initially spread by infecting USB flash drives and then attacking other WinCC computers in the infected network.[5] Notably, APT attacks are typically highly targeted. Hackers spend a lot of time collecting information on the electric grid architecture, components, and vulnerabilities. As they lurk and try to remain hidden, they use various techniques to gain initial access, and then continue to evade defense mechanisms for as long as possible in order to prolong access to the target system. In recent years, with geopolitical conflicts, electric grids have become targets for nation-state actors or cybercriminals. Since attacks that introduce external malicious code through internal employees are the main vulnerability, the main weak points of defense are the absence of malicious program inspection for devices and zero-day vulnerability testing for industrial control systems.

## 2. Lateral movement from IT networks to power grid systems

Lateral movement from office networks is one of the most dangerous attack vectors for power system operators, as hackers mainly gain access to the electric grid system through lateral movement in the IT network. The most common method is to use spear-phishing emails and other social engineering techniques to trick employees into providing sensitive information or clicking on malicious links. For example, the first successful attack against an electric grid was carried out by BlackEnergy in 2015-2016 who launched a series of cyber attacks on the Ukraine power grid. The attackers used social engineering to send BlackEnergy to an employee's mailbox at a power

[5] *Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." White paper, symantec corp., security response 5.6 (2011): 29*

company in western Ukraine. When BlackEnergy was downloaded to the employee's computer, it activated the Windows OLE remote code execution vulnerability (CVE-2014-4114) and downloaded other attack tools to the compromised employee's computer.[6] As a result, the hackers were able to eavesdrop and collect user passwords, deploy remote desktops and, and VPN tunnels to the electric grid SCADA system, and finally gain control over the substation circuit breaker and SCADA system. This attack resulted in a power outage in the Ivano-Frankivsk region of Ukraine for up to six hours, directly affecting more than 200,000 residents.

Similar attack methods have also occurred in other countries. Researchers found that Dragonfly's earliest activity was a malicious email campaign that sent emails disguised as New Year's Eve party invitations to targets in the energy industry in December 2015. The organization further carried out targeted malicious email campaigns in 2016 and 2017. These emails contained highly specific content related to the energy industry, as well as some content related to general business issues, giving the false impression that these were authentic messages. Once opened, the attached malicious documents attempted to leak the victim's network credentials to a server outside the target organization.[7]

## 3. Vulnerabilities in remote services in connected devices are easily exploited

Remote access is a convenient and commonly used function in the electric grid, as it allows system administrators and engineers to remotely access power equipment and industrial control systems for maintenance, monitoring, and operation. However, because remote access can be established via the internet, it also makes it an easy target for attackers. Certain devices and systems may enable remote access by default, and these accounts and passwords are often left with their preset defaults and vulnerable to attacks. If administrators do not change the default password in a timely manner, attackers may easily gain entry to the system through brute force attacks. In 2022, the US CISA and DOE issued a warning that attackers often gain access to various networked uninterruptible power supply (UPS) devices through unchanged default usernames and passwords and suggested that organizations could remove management interfaces from the internet to reduce the chances of their UPS devices being attacked.[8]

## 4. Leakage of external remote service tool credentials

VPN access credentials include sensitive information such as usernames, passwords, and public and private keys used for remote access. They allow users to access internal networks from remote devices without directly connecting to the enterprise or organizational internal network. Attackers can gain access to an enterprise's internal network by obtaining sensitive information such as VPN access credentials and using this information to enter the network. In 2021, in the Colonial Pipeline incident, DarkSide was found to have used stolen employee VPN accounts for remote access to the internal network.[9]

[6] *Robert Lipovsky,"CVE-2014-4114: Details on August BlackEnergy PowerPoint Campaigns", ESET, October, 2014.*

[7] *CISA CYBERSECURITY ADVISORY, "Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector", CISA, March 24, 2022.*

[8] *U.S. Cybersecurity and Infrastructure Security Agency (CISA), "Mitigating Attacks Against Uninterruptable Power Supply Devices", CISA, March, 2022.*

[9] *Avertium, "The Top 5 Cyber Threats in the Energy Sector", Avertium, September 13, 2022.*

## 5. Attacks exploiting the weaknesses of public-facing applications

These vulnerabilities and weaknesses may be exploited by hackers to gain access to the system. For example, in March 2019, attackers exploited a web interface vulnerability in a firewall device to launch a denial-of-service (DoS) attack, triggering an unexpected reboot of on-site equipment. As the firewall management center communicated with multiple remote power stations, the communication between the control center and a large wind and solar power generation operator in Utah was simultaneously disrupted.[10] This cybersecurity incident was recorded as caused by an unauthorized attacker triggering an unexpected equipment reboot and was the first case of an interruption in wind power generation.

## 6. Supply chain attacks on the power company

The smart grid is one of the most complex CPS systems, making it vulnerable to cyber attacks, with supply chain attacks being one of the most insidious and difficult to detect forms of cyber attack. Attackers may target the supplier of key components, such as smart meters or other sensors, and then use that access to control a wider network. There are several reasons why the smart grid is particularly vulnerable to supply chain attacks:

- ### Dependence on supplier controls and services:

  The smart grid often relies on a wide range of interconnected devices and systems, which creates a huge attack surface that is difficult to protect. In addition, smart grid components are often manufactured by third-party suppliers who may not have the same level of cybersecurity expertise or resources as the utilities that deploy their products, making remote-controlled systems more vulnerable to attack. For example, in March to April 2022, three wind power companies in Germany were hit by ransomware attacks. First, Enercon GmbH, a wind turbine manufacturer, lost control of 5,800 turbines due to the interruption of satellite communications services by a supplier, causing the company to lose control of the turbines.[11] Second, Nordex SE was hit by ransomware attacks and, in order to protect customer assets, remote access to wind turbines was prohibited from Nordex Group IT infrastructure under contract.[12] Third, Deutsche Windtechnik lost control of about 2,000 turbines during an attack,[13] which affected the stability of power supply for power grid operators.

- ### Unpatched software from the software supply chain:

  Because electrical grid systems have a long lifespan, and many smart grid components are difficult or impossible to replace once deployed, vulnerabilities may persist in the system for a long time. For example, smart grid components may continue to be used for decades, during which time they may become outdated or no longer have software vulnerability patching support from suppliers, exposing them to greater likelihood of attack. Researchers found serious

[10] *Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. stuxnet dossier." White paper, symantec corp., security response 5.6 (2011): 29*

[11] *Maria Sheahan, Christoph Steitz and Andreas Rinke, Miranda Murray, Bernadette Baum, "Satellite outage knocks out thousands of Enercon's wind turbines", Reuters, March 1, 2022.*

[12] *Vilius Petkauskas, "Conti claims responsibility for an attack on wind turbine giant Nordex", Cybernews, April 2022.*

[13] *Catherine Stupp, "European Wind-Energy Sector Hit in Wave of Hacks", WSJ Pro, April, 2022.*

vulnerabilities (including information disclosure vulnerability CVE-2021-33558, arbitrary file access vulnerability CVE-2017-9833, and remote code execution vulnerability CVE-2009-4496) in the Boa network server.[14] Since this software was discontinued in 2005, the nascent high-risk vulnerabilities in old systems allowed attackers to collect information about network assets and obtain valid credentials before successfully gaining access to the network undetected. The Boa vulnerability led to the recent attack on Tata Power in October 2022. At the same time, this vulnerability also led to the release of data stolen from this Indian energy giant by the Hive ransomware group.[15]

# Emerging Vulnerabilities in Contemporary Smart Grids

The original smart grid architecture was based on the traditional power grid structure (generation, transmission, distribution, and consumption) and was constructed with a focus on power technology. In the future, the smart grid will place greater emphasis on the integration of information and communication technologies and will be oriented toward solving demand-side issues. When examining the new revised architecture of CPS systems for power, we can summarize the major cybersecurity risks into four important areas:

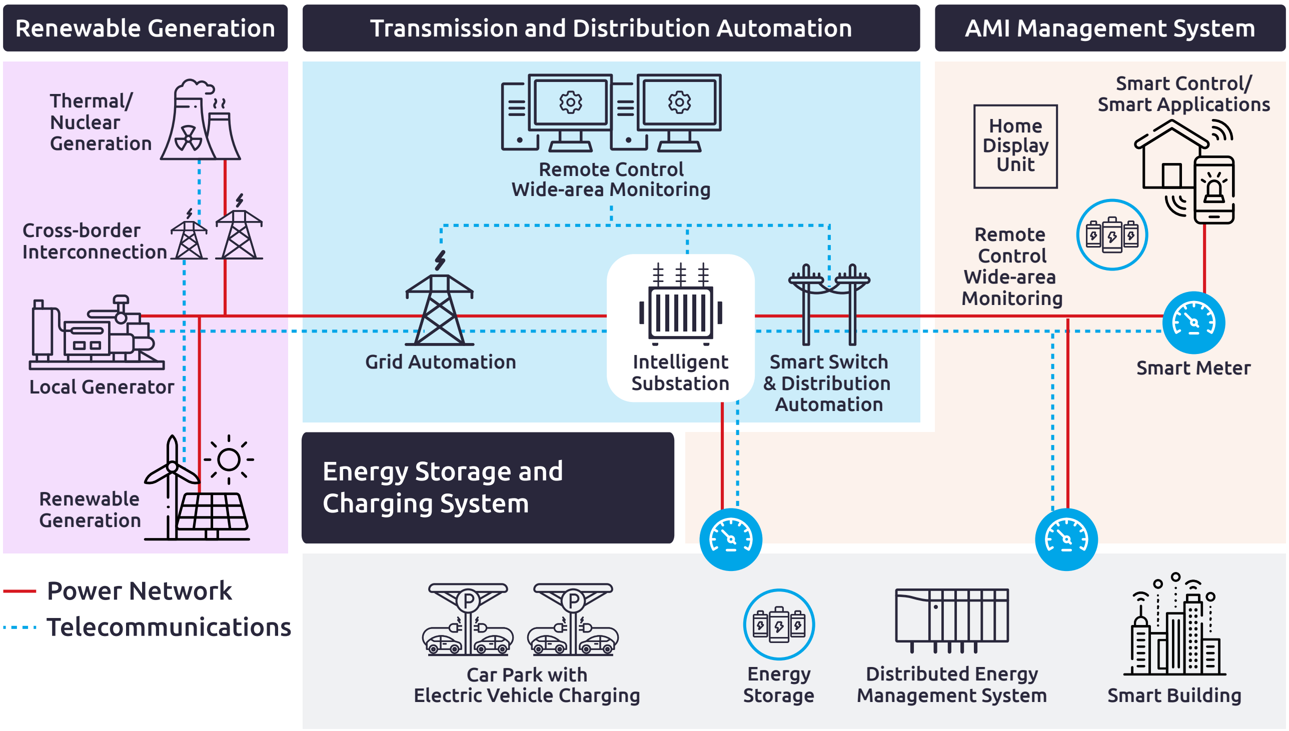

Renewable Generation
Transmission and Distribution Automation
AMI Management System
Thermal/ Nuclear Generation
Cross-border Interconnection
Local Generator
Renewable Generation
Remote Control Wide-area Monitoring
Grid Automation
Intelligent Substation
Smart Switch & Distribution Automation
Home Display Unit
Smart Control/ Smart Applications
Remote Control Wide-area Monitoring
Smart Meter
Energy Storage and Charging System
Car Park with Electric Vehicle Charging
Energy Storage
Distributed Energy Management System
Smart Building
Power Network
Telecommunications

*Figure 3: Important Subsystems of the Smart Grid*

[14] *Microsoft Security Blog, "Vulnerable SDK components lead to supply chain risks in IoT and OT environments", Microsoft, December 2022.*
[15] *Carly Page, "Microsoft says attackers are hacking energy grids by exploiting decades-old software", TechCrunch, November 2022.*

# 1. Renewable Power Generation

In recent years, due to environmental and green energy concerns, power generation has shifted towards renewable energy sources such as solar and wind. Renewable energy facilities are often located in remote areas, so power plants must be more flexible in utilizing these energy resources. Thus, the concept of "virtual power plants" has emerged, aggregating distributed small and medium-sized energy sources through decentralized energy management technology to become a reliable source of power supply, like a controllable power plant. Power companies need to flexibly dispatch power generation units in order to meet the fluctuating electricity demand, maintaining a stable dynamic balance of supply and demand in the power system. Generally, power companies consider the different characteristics and costs of various units and carry out power source and grid dispatch according to three criteria: a) ensuring the reliability of power supply, b) power quality, and c) minimum operating costs of the power system.

Due to the instability of renewable energy sources, sensors and networks need to be used for timely scheduling, so the distributed generation system has begun moving towards the smart grid. The smart grid can incorporate renewable energy sources such as solar and wind more easily. However, that means more power electronics equipment needs to be integrated into the grid system (such as advanced inverters, energy management systems, and intelligent controllers) in order to facilitate the conversion between high voltage and low voltage, regulate power flow, or convert between direct current (DC) and alternating current (AC). Ensuring the cybersecurity of these devices is even more critical. On top of that, renewable energy sources such as solar and wind farms are distributed over a larger area and system, which also increases the demand for networks and increases the number of individual devices connected to each other. For hackers, this is a boon because renewable energy systems expose more vulnerabilities. However, fossil fuel facilities have different weaknesses than renewable energy sources. Since most coal, oil, and gas plants are much older than renewable energy sources, systems from decades ago were not really prepared to resist modern cyber attacks, so protecting these legacy assets is currently the priority when it comes to traditional power grids.

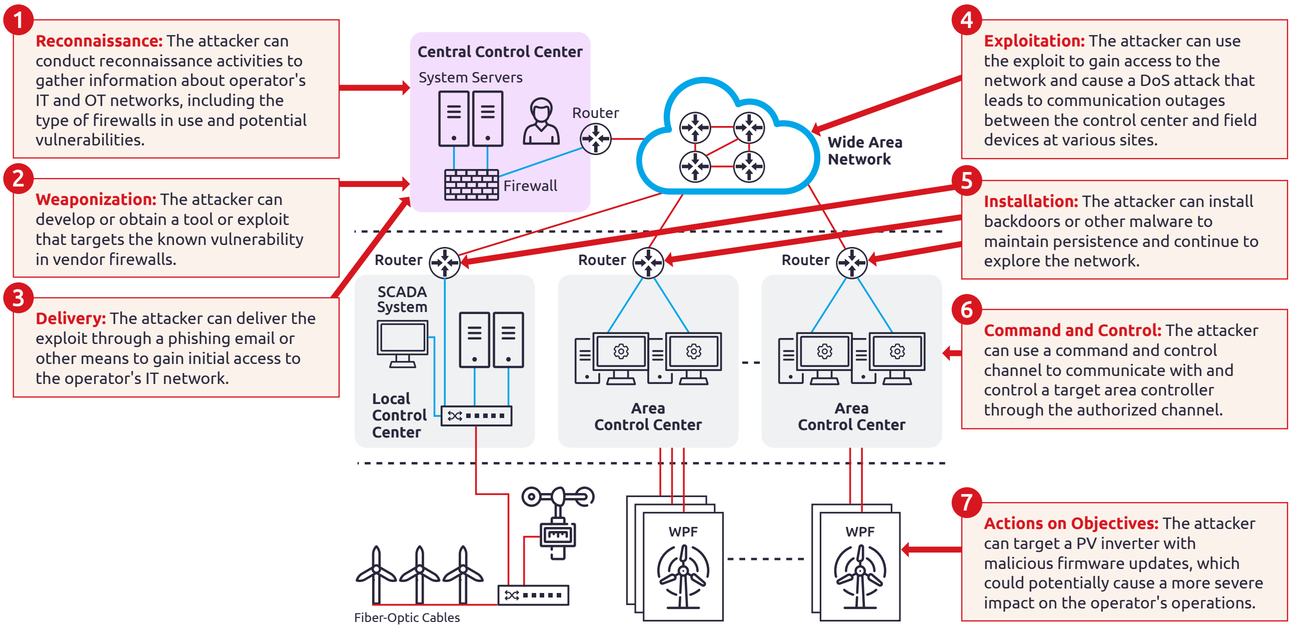
## • Vulnerabilities in Wind Power Control Equipment:

Wind turbines do not operate as isolated entities. As a natural generator within smart grids, wind farms rely on information and communication technology (ICT) that supports bidirectional communication, remote control, automation, and monitoring under certain circumstances. In 2015, a cybersecurity researcher discovered vulnerabilities in two wind turbine systems. The XZERES 442SR wind turbine uses a web-based interface, which was found to be vulnerable to cross-site request forgery attacks that allowed retrieval and modification of default user passwords, thereby granting administrative privileges over the entire system. This vulnerability exploit could lead to power outages across connected systems.[16] In addition, researchers found HMI vulnerabilities in the company producing wind turbines, in which credentials listed in plaintext could be used to gain unauthorized remote access to devices, allowing attackers to modify all configurations and settings.[17]

[16] *ICS-CERT. "XZERES 442SR Wind Turbine Vulnerability", CISA, Last modified August 27, 2018.*

[17] *ICS-CERT. "RLE Nova-Wind Turbine HMI Unsecure Credentials Vulnerability (Update A)", CISA, Last modified August 27, 2018.*

Similarly, in 2017, researchers at the University of Tulsa described a scenario combining cyber and physical attacks, focusing on wind turbine control, turbine damage, wind power plant interruption and damage, and substation interruption and damage in an unmanned turbine gate. Researchers used a Raspberry Pi mini-machine connected to a programmable automation controller, a microwave-sized computer that controls the turbine. They showed that attackers can unlock the turbine in less than a minute and access every connected wind turbine through the network. This research demonstrated that attackers can use custom tools to craft and replicate turbine control messages, use worms to propagate malicious and harmful commands within the turbine or entire wind power plant network, or "arbitrarily block, modify, and forge control messages" using the flat wind power plant network topology.[18]


1 **Reconnaissance:** The attacker can conduct reconnaissance activities to gather information about operator's IT and OT networks, including the type of firewalls in use and potential vulnerabilities.

2 **Weaponization:** The attacker can develop or obtain a tool or exploit that targets the known vulnerability in vendor firewalls.

3 **Delivery:** The attacker can deliver the exploit through a phishing email or other means to gain initial access to the operator's IT network.

4 **Exploitation:** The attacker can use the exploit to gain access to the network and cause a DoS attack that leads to communication outages between the control center and field devices at various sites.

5 **Installation:** The attacker can install backdoors or other malware to maintain persistence and continue to explore the network.

6 **Command and Control:** The attacker can use a command and control channel to communicate with and control a target area controller through the authorized channel.

7 **Actions on Objectives:** The attacker can target a PV inverter with malicious firmware updates, which could potentially cause a more severe impact on the operator's operations.

*Figure 4: Wind Farm Attack Scenarios*[19]

## • Vulnerabilities in Solar Power Generation:

Solar power units also have the characteristic of being placed in external areas, making the components easily accessible to attackers. In addition to solar panels, inverters that can be connected to the network (as shown in Figure 5) are also targeted for attack. Inverters act as the interface between the solar panels and the power grid, providing functions such as changing power delivery schedules and shutting down power. In 2017, security researcher Willem Westerhof discovered several security vulnerabilities in products,[20 21] such as CVE-2017-9852, where default passwords for users and installers were reused among inverters installed by the same installation company, making passwords easily guessable or predictable by attackers. This could endanger the affected devices and their functions. If one system can be compromised, it is possible that all systems can be compromised. However, in a highly interconnected power generation environment, if there is poor network segmentation between inverters, attackers could potentially first attack one group of inverters and then use them to connect to other areas of inverters, threatening the interruption of a large number of power-generating units.

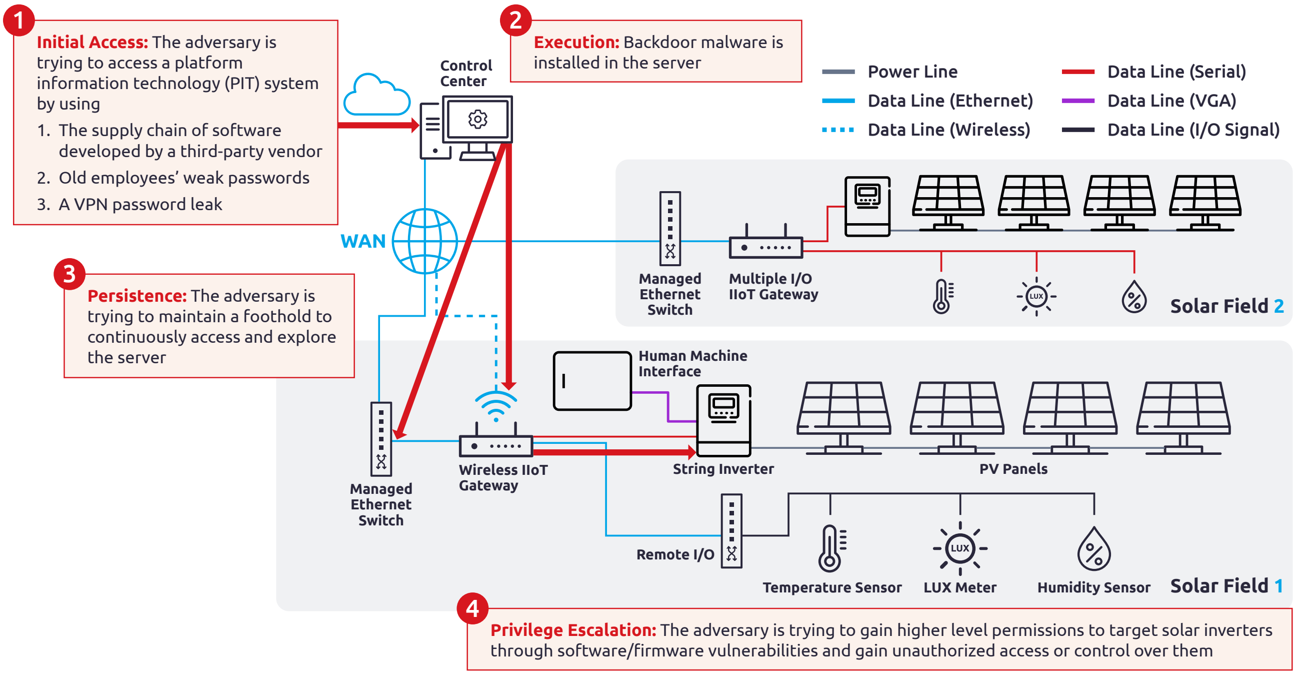
[18] *Staggs, Jason, David Ferlemann, and Sujeet Shenoi. "Wind Farm Security: Attack Surface, Targets, Scenarios and Mitigation", International Journal of Critical Infrastructure Protection, March, 2017.*

[19] *Ahmed, M. H., Kang, Y. S., & Kim, Y. "Modeling and simulation of communication networks for use in integrating high wind power generation into a power grid", Journal of Renewable and Sustainable Energy, August 2015.*

[20] *Swati Khandelwal, "Critical Flaws Found in Solar Panels Could Shut Down Power Grids", The Hacker News, August 08, 2017.*

[21] *SMA, "Statement By Sma Solar Technology Ag On The Cyber Security Of PV Inverters (Horus Scenario)" SMA, August, 2017.*

Furthermore, in their 2022 IEEE paper, Jin Ye et al. mentioned several attack scenarios against smart inverters.[22] Attackers can launch cyberattacks on solar inverters using software/firmware update events. The attack surface for software/firmware in solar power plant control centers and smart inverters includes three fronts: remote vendor access, operator access, and physical access. Advanced attackers such as APT groups and insider threats can masquerade as vendors or authorized users to modify software. Figure 5 illustrates a cyber attack scenario aimed at disrupting photovoltaic inverters, explained based on the Cyber Kill Chain (CKC) model. In this scenario, an adversary gains initial access to the platform information technology (PIT) system by using the supply chain of software developed by a third-party vendor, old employee's weak passwords, or a VPN password leak (1. Initial Access). Backdoor malware is installed in the server (2. Execution). The adversary tries to maintain a foothold to continuously access and explore the server (3. Persistence). The adversary tries to gain higher-level permission (4. Privilege Escalation).[22]



1 **Initial Access:** The adversary is trying to access a platform information technology (PIT) system by using

1. The supply chain of software developed by a third-party vendor
2. Old employees' weak passwords
3. A VPN password leak

2 **Execution:** Backdoor malware is installed in the server

3 **Persistence:** The adversary is trying to maintain a foothold to continuously access and explore the server

4 **Privilege Escalation:** The adversary is trying to gain higher level permissions to target solar inverters through software/firmware vulnerabilities and gain unauthorized access or control over them

*Figure 5: Solar Farm Attack Scenarios*

## 2. Distribution Automation (DA) and Feeder Automation (FA):

Smart grid management includes Distribution Automation (DA) and Feeder Automation (FA). DA is an electric information management system established on the basis of distribution networks and equipment. It is mainly based on wired or wireless communication networks, distribution or feeder terminal equipment, and backend computer management. DA enables precise fault location during outages and provides information on the operation of adjacent distribution terminal equipment, thus allowing for monitoring and quick fault isolation and elimination in distribution networks. FA is an important branch of DA and refers to the automation between the substation circuit and the user's transformer equipment, including automatic recovery and isolation of feeder faults. In the past, distribution network protection circuits only had rudimentary overcurrent and overvoltage

[22] *Jin Ye , Sudip K. Mazumder, Taesic Kim…, "A Review of Cyber–Physical Security for Photovoltaic Systems", IEEE Journals & Magazine, August 2022.*

protection circuit designs, without communication networks and backend computer management systems, making it difficult to achieve segmentation isolation. Whenever there was a power outage, the affected area was extremely large, and fault power outages would take hours to resolve. With the help of communication networks and backend computer management systems, fault isolation time can now be shortened to milliseconds to ensure uninterrupted power supply. Therefore, the availability of DA and FA must be kept at a high level and made secure.

## • Insecure Industrial Control Protocols:

The concept and design of substation automation systems was proposed by Working Group 10 of Technical Committee 57 of the International Electrotechnical Commission (IEC). However, the main design purpose of IEC 61850, released by IEC TC 57, was not for cybersecurity, but for (1) reducing configuration and installation costs, (2) multi-vendor interoperability, (3) long-term stability, and (4) minimizing the impact on existing systems. Therefore, many industrial protocols do not include cybersecurity functions, including important industrial communication protocols for the power grid, such as DNP 3.0, IEC 61850, IEC 60870-5, and Internal Control Center Communication Protocol (ICCP). For example, many grid communication protocols adopt multicast schemes that have potential network vulnerabilities. In addition, most delayed transmission time encryption schemes or other cybersecurity functions are not applicable to these protocols, as the performance requirements for GOOSE and SMV messages are within 4 milliseconds, making it difficult to implement data encryption measures. The lack of encryption may provide attackers with the opportunity to execute attacks such as man-in-the-middle or deception.[23]

**Typical Communication Protocols Used in a Power System**

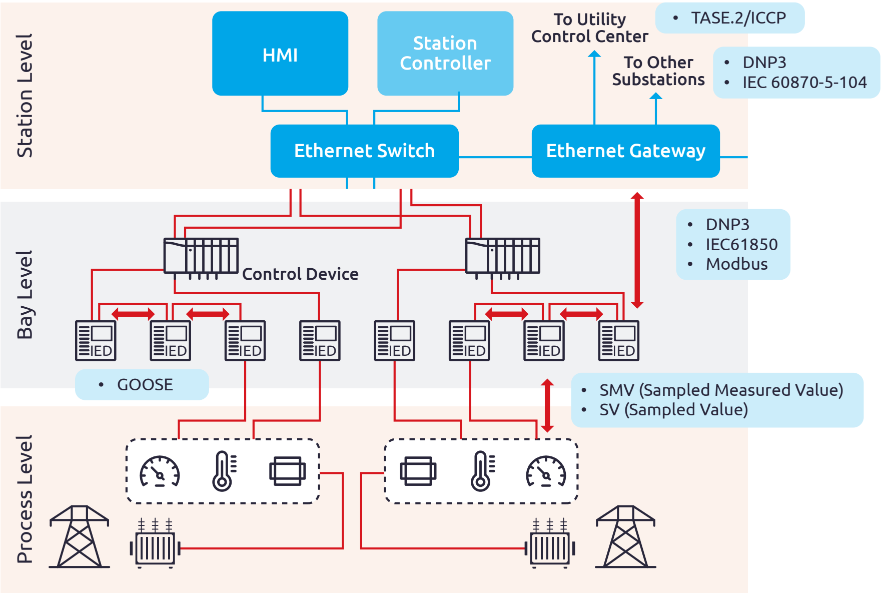


*Figure 6: Vulnerabilities in IEC 61850 Protocols*

**Examples of Vulnerable Protocols**

- **DNP3:** The Stuxnet worm, discovered in 2010, was a sophisticated cyberattack that targeted industrial control systems, including those using DNP3. Some of the vulnerabilities, including CVE-2015-5374, CVE-2015-5375, CVE-2019-9569, allow an attacker to execute arbitrary code or cause a DoS attack on IEC 60870-5-104 devices.
- **IEC 60870-5-104:** In December 2015, a cyberattack on the Ukrainian power grid caused widespread power outages. The attack was carried out using a variant of the BlackEnergy malware, which targeted IEC 60870-5-104 devices. Some of the vulnerabilities allowed attackers to perform man-in-the-middle (MitM) attacks on IEC 60870-5-104 devices.
- **IEC61850:** Take GOOSE as an example; GOOSE messages are transmitted in clear text, which means that they are vulnerable to interception and eavesdropping. If an attacker can intercept the GOOSE message, they can launch a man-in-the-middle attack and they can potentially tamper with the message, leading to false data or even physical damage to equipment.
- **SV/SVM**：SV/SVM are also vulnerable to replay attacks, where an attacker can intercept and replay a message, leading to incorrect data or even physical damage to equipment.

[23] *Junho Hong, "Cyber Security Of Substation Automation Systems", Washington State University, August 2014.*

- **Risk of Remote Service Vulerabilities:**

  Distribution and transmission systems may be widely distributed and remote, leading to the use of virtual private networks (VPNs), dial-up, or wireless remote access to substations for monitoring and maintenance purposes. However, the main risk of remote access is the lack of sufficient security measures, such as improperly configured firewalls, weak ID and password policies, and poor management of encryption keys, which leads to the possibility of remote intrusion.

  A typical substation may have many intelligent electronic devices (IEDs), and these devices may have credential storage vulnerabilities. For example, according to CISA's advisory on CVE-2022-2513, IED credentials from a device vendor were stored in plaintext in a database. If successfully exploited, attackers may gain access to sensitive credentials and load incorrect configurations, restart IEDs, or cause denial of service situations.

## 3. Energy Storage System Management:

To mitigate the impact of intermittent renewable energy generation on power quality, Battery Energy Storage System (BESS) is becoming an important part of the power grid. Currently, lithium-ion battery energy storage systems are the mainstream technology in the power grid. They play an important role in the integration of renewable energy sources (RES) in the energy system, helping to achieve stable and resilient supply of renewable energy, and improve the efficiency of the power system. Data integrity is one of the primary requirements for ensuring secure operation of grid networks. Integrity attacks aim to modify data, delay its transmission, or replay previously stolen data to undermine the observability of the system and manipulate its parameters. Data integrity is associated with FDIA because this attack involves the modification of data.[24][25] In addition, researchers discovered in 2022 that the Combined Charging System (a common fast charging technology) has weaknesses that can be exploited to perform disruption attacks. Attackers can use these weaknesses to interrupt charging services at EV charging stations through wireless signals. If multiple charging stations are terminated without warning, the voltage may become unstable and affect the entire power grid.[26]

## 4. Advanced Metering Infrastructure (AMI) Management System:

This is a system built on smart metering systems that collects energy usage data and transmits it back to utility companies. AMI allows for more accurate demand response plans that incentivize customers to reduce energy usage during peak demand periods. This can be achieved through pricing signals, rebates, or other incentives, as well as better load management and outage detection to improve the resilience and efficiency of the power system. AMI is an intermediate system between smart grid end-users and utility companies, mainly for electricity pricing and demand management purposes. The common components of AMI include smart meters, data concentrators, and utility centers, which communicate bidirectionally over a network. For example,

[24] *ICS-CERT. "Hitachi Energy IED Connectivity Packages and PCM600 Products", CISA, Last modified November 29, 2022.*

[25] *S. Kumbhar, T. Faika, D. Makwana, T. Kim and Y. Lee, "Cybersecurity for Battery Management Systems in Cyber-Physical Environments," 2018 IEEE Transportation Electrification Conference and Expo (ITEC), Long Beach, CA, USA, 2018.*

[26] *Sebastian Köhler, Richard Baker, Martin Strohmeier, and Ivan Martinovic, "Vulnerability in the Combined Charging System for Electric Vehicles", Brokenwire, Accessed Sep 23, 2022.*

a smart meter can transmit user power usage data through a data concentrator to the control center, and the control center can also transmit control commands through a data concentrator back to the smart meter. Due to the distance between devices, wireless technology is often used for data transmission in AMI, which gives attackers the opportunity to falsify power data using corresponding radio frequency tools and even gain control of endpoint devices.[27] [28] [29]

# Cybersecurity Standards Development for the Smart Grid

The increasing threat of cyber attacks on critical energy infrastructure has highlighted the need for robust cybersecurity measures in the power grid. Power grid operators and governments around the world are implementing a range of cybersecurity measures, including network segmentation, multi-factor authentication, and regular security training for employees, to address these threats. In addition, regulatory frameworks are being developed to ensure that power grid operators have robust cybersecurity plans in place. Therefore, it is important to have a detailed understanding of the current best practices and standards for securing the infrastructure of smart grids. We focus on several areas to assess existing standards and identify gaps between current standards and future requirements.

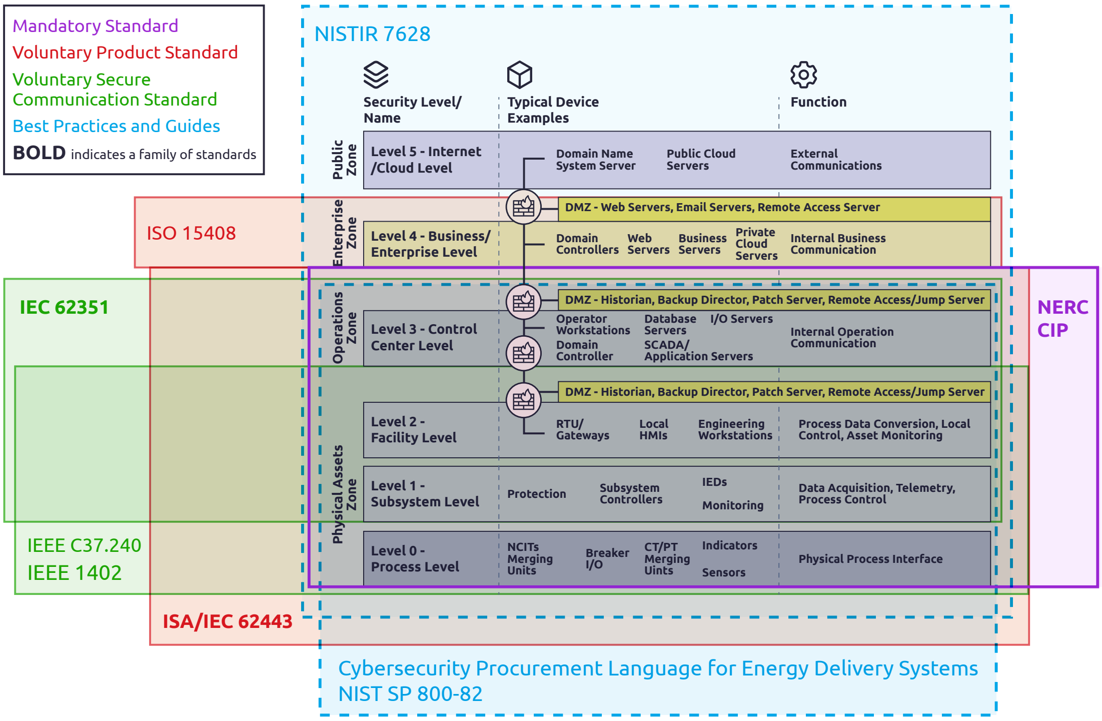

Mandatory Standard
Voluntary Product Standard
Voluntary Secure Communication Standard
Best Practices and Guides
BOLD indicates a family of standards
NISTIR 7628
Security Level/ Name
Typical Device Examples
Function
Public Zone
Level 5 - Internet /Cloud Level
Domain Name System Server
Public Cloud Servers
External Communications
Enterprise Zone
DMZ - Web Servers, Email Servers, Remote Access Server
Level 4 - Business/ Enterprise Level
Domain Controllers
Web Servers
Business Servers
Private Cloud Servers
Internal Business Communication
ISO 15408
Operations Zone
DMZ - Historian, Backup Director, Patch Server, Remote Access/Jump Server
Level 3 - Control Center Level
Operator Workstations
Database Servers
I/O Servers
Domain Controller
SCADA/ Application Servers
Internal Operation Communication
IEC 62351
NERC CIP
DMZ - Historian, Backup Director, Patch Server, Remote Access/Jump Server
Level 2 - Facility Level
RTU/ Gateways
Local HMIs
Engineering Workstations
Process Data Conversion, Local Control, Asset Monitoring
Physical Assets Zone
Level 1 - Subsystem Level
Protection
Subsystem Controllers
IEDs
Monitoring
Data Acquisition, Telemetry, Process Control
Level 0 - Process Level
NCITs Merging Units
Breaker I/O
CT/PT Merging Uints
Indicators
Sensors
Physical Process Interface
IEEE C37.240
IEEE 1402
ISA/IEC 62443
Cybersecurity Procurement Language for Energy Delivery Systems
NIST SP 800-82

*Figure 7: Example Mapping of Standards onto the Reference Architecture*[30]

[27] *Mostafa Shokry, Ali Ismail Awad, Mahmoud Khaled Abd-Ellah, Ashraf A.M. Khalaf, "Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision", ScienceDirect, Nov 2022.*

[28] *Elias Bou-Harb, Claude Fachkha, Makan Pourzandi, Mourad Debbabi, Chadi Assi, "Communication Security for Smart Grid Distribution Networks", ResearchGate, Jan 2013, Accessed September 23, 2022.*

[29] *Ding, J.; Qammar, A.; Zhang, Z.; Karim, A.; Ning, H. "Cyber Threats to Smart Grids: Review,Taxonomy, Potential Solutions, and Future Directions", Energies 2022.*

[30] *Maurice Martin, Samuel Chanoski, Steve Granda, Steven Kunsman, Marcus Sachs, "Reference Architectures as a Means of Influencing Electric Energy Operational Technology/Industrial Control System Security Outcomes", SEI ETF, March 2022.*

# 1. Secure Policy and Management in the Smart Grid

## • NERC CIP Cybersecurity Standards

The NERC CIP (currently in its fifth iteration) is a mandatory cybersecurity standard that covers access control, personnel safety, physical security, network security incident response, and disaster recovery for large-scale power systems with a voltage of 100 kV or higher, including physical and network assets for power generation, transmission, and distribution (>20 MW). However, it only partially applies to renewable energy generation systems. The NERC CIP standard is mandatory for all entities responsible for operating large-scale power systems in North America, including utilities, power generators, and transmission and distribution companies. NERC and its regional entities enforce these standards through audits and other oversight protocols. The structure of the NERC CIP standard includes nine specific standards (CIP-002 through CIP-010), which require power system operators to develop and implement various security plans, controls, and risk management processes.[31] [32]

In addition, FERC has issued an order to modify the reliability standard for supply chain risk management within the NERC CIP standards. Multiple CIPs came into effect on October 1st, 2022, including electronic access control or monitoring systems (EACMS) associated with bulk electric system cyber systems with medium to high impact. Furthermore, Chapter 2 of the NERC - Cyber Supply Chain Risk Document calls for further expansion to protect physical access control systems (PACS). Supply chain risk management requirements first include the following NERC CIP standards:

a. CIP-005-6: CIP-005-6 introduces Requirements 2.4 and 2.5 for identifying and disabling vendor remote access sessions used for high and medium impact BCS Cyber Systems (BCS).

b. CIP-010-3: CIP-010-3 introduces Requirement R1, Section 1.6 to enforce entity authentication of software sources (R1.6.1) and to verify the integrity of software obtained from the software source (R1.6.2) for all BCS used for high or medium impact. These measures aim to address potential supply chain risks associated with threat actors deceiving vendor sites or inserting/injecting malicious code into software between their legitimate supplier source location and customer downloads.

c. CIP-013-1: CIP-013-1 is the first revision of a risk-based CIP reliability standard for cyber supply chain risk management (CSCRM).

[31] *Awati, R., Cole, B., "North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)", TechTarget, March 2022.*

[32] *AMI-SEC Task Force, "Security Profile for Advanced Metering Infrastructure. Technical report", AMI-SEC Task Force, 2010.*

*Table 2. NERC CIP Standards*

| Standard Number | Standard Title | Purpose | Effective Date of Standard |
|---|---|---|---|
| CIP-002-5.1a | BES Cyber System Categorization | To identify and categorize BES Cyber Systems and their associated BES Cyber Assets for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those BES Cyber Systems could have on the reliable operation of the BES. Identification and categorization of BES Cyber Systems support appropriate protection against compromises that could lead to misoperation or instability in the BES. | 12/27/2016 |
| CIP-003-8 | Security Management Controls | 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 Bulk Electric System (BES). | 4/1/2020 |
| CIP-004-6 | Personnel & Training | To minimize the risk against compromise that could lead to misoperation or instability in the Bulk Electric System (BES) from individuals accessing BES Cyber Systems by requiring an appropriate level of personnel risk assessment, training, and security awareness in support of protecting BES Cyber Systems. | 7/1/2016 |
| CIP-005-7 | Electronic Security Perimeter(s) | To manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter in support of protecting BES Cyber Systems against compromise that could lead to misoperation or instability in the BES. | 10/1/2022 |
| CIP-006-6 | Physical Security of BES Cyber Systems | To manage physical access to Bulk Electric System (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. | 7/1/2016 |
| CIP-007-6 | System Security Management | 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 Bulk Electric System (BES). | 7/1/2016 |
| CIP-008-6 | Incident Reporting and Response Planning | To mitigate the risk to the reliable operation of the BES as the result of a Cyber Security Incident by specifying incident response requirements. | 1/1/2021 |
| CIP-009-6 | Recovery Plans for BES Cyber Systems | 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. | 7/1/2016 |
| CIP-010-4 | Configuration Change Management and Vulnerability Assessments | 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 Bulk Electric System (BES). | 10/1/2022 |
| CIP-011-2 | Information Protection | 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 Bulk Electric System (BES). | 7/1/2016 |
| CIP-012-1 | Communications Between Control Centers | To protect the confidentiality and integrity of real-time assessment and real-time monitoring data transmitted betwen control centers. | 7/1/2022 |
| CIP-013-2 | Supply Chain Risk Management | To mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES) by implementing security controls for supply chain risk management of BES Cyber Systems. | 10/1/2022 |
| CIP-014-3 | Physical Security | 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. | 6/16/2022 |

### • NIST Cybersecurity Standards for the Power Grid:

The US National Institute of Standards and Technology (NIST) has published NISTIR 7628, a general cybersecurity standard for the power grid, which is applicable from Level 0-Level 5. It provides guidelines for identifying and mitigating cyber risks in smart grid systems, including recommendations for security controls and risk management processes. In addition, NIST has published the SP800-82 guide for security controls for OT/ICS systems, which is not specific to the power industry but is applicable to the cybersecurity management of automated industrial control systems. However, since NIST's cybersecurity standards are voluntary, they are mainly used for self-assessment (such as cybersecurity maturity assessment) rather than cybersecurity compliance certification.

## 2. Secure Equipment in the Smart Grid

### • ICS/OT Zone Equipment Security Standards

IEC 62443 is one of the most critical cybersecurity standards to ensure the security of smart grid systems and devices. Developed by the International Electrotechnical Commission (IEC), it provides a framework for protecting industrial automation and control systems, including those used in smart grid systems. Specifically, IEC 62443-4-1 and 4-2 provide software security development and component definition security standards for reference in the development of power system automation and control systems, such as grid control center equipment, substation equipment, and intelligent electronic devices (IEDs).[33]

### • Enterprise Zone Equipment Security Standards

ISO 15408 can be used to evaluate the security of a wide range of products, including those used in smart grid systems, for information technology (IT) operations. It provides a set of requirements and guidelines for implementing security controls, including access control, identity authentication, data confidentiality, and data integrity. It also provides guidance for the evaluation of security products and systems, including testing and certification, to make sure that cybersecurity is considered in their design, development, and implementation. This helps to fend off cyber threats and vulnerabilities and ensures that Layer 4 devices in smart grid systems operate reliably and securely.[33]

### • Security Profile for Advanced Metering Infrastructure

The AMI-SEC Task Force, also known as the Advanced Metering Infrastructure Security Task Force, is a public-private partnership established by the US Department of Energy (DOE) and the National Institute of Standards and Technology (NIST) in collaboration with the Electric Power Research Institute (EPRI) and the utilities industry. The task force is responsible for promoting and developing best practices and standards for the secure deployment of advanced metering infrastructure (AMI) and other smart grid technologies. The AMI-SEC Task Force was formed

[33] *Leszczyna, R., "Standards on cyber security assessment of smart grid. International Journal of Critical Infrastructure Protection", International Journal of Critical Infrastructure Protection, 2018.*

in response to the increasing cybersecurity threats facing the electric power industry and the need to protect the integrity and security of the nation's energy infrastructure. The task force consists of representatives from various government agencies, utility companies, equipment manufacturers, and other stakeholders in the electric power industry. The AMI-SEC Task Force's main goal is to develop a comprehensive and effective security framework for AMI and other smart grid technologies. This framework includes guidelines, standards, and best practices for securing communication networks, data management systems, and other critical components of the smart grid.

The Security Profile for Advanced Metering Infrastructure is a guideline developed by the AMI-SEC Task Force to provide guidance on implementing security in the AMI infrastructure. The majority of security controls presented in the guideline are adapted from the DHS Catalog of Control Systems Security, which advises regular evaluations of all components of the AMI system for security vulnerabilities and compliance with maintenance and security policies. The guideline recommends analyzing all cryptographic modules against the requirements of FIPS 140-2 and suggests using cryptographic modules validated by the Cryptographic Module Validation Program. Any vulnerabilities or incompatibilities with security requirements identified during the analyses should result in updates or replacements of the relevant AMI system components.[34]

## 3. Secure Communication in the Smart Grid

### • IEC 62351 Cybersecurity Standards for Grid Equipment:

IEC 62351 is one of the essential cybersecurity standards for ensuring the security of intelligent grid systems and equipment. Developed by the International Electrotechnical Commission (IEC), it provides a framework for protecting industrial automation and control systems, including those used in intelligent grid systems. IEC 62443 4-1 and 4-2 respectively cover software security development and component definition security standards, which can be used as a reference for the development of power system automation and control systems, such as grid control center equipment, substation equipment, and Intelligent Electronic Devices (IEDs).[35]

### • IEEE Cybersecurity Standards for DER Energy Storage Systems:

For the security of DER energy storage systems (such as solar panels and wind turbines), IEEE 2030 has established a set of standards for interoperability and communication between energy storage systems and the power grid to achieve a more reliable, efficient, and sustainable power system. IEEE 2030 plays an important role in modernizing and transforming the power grid, facilitating the integration of DERs, and transitioning to a more sustainable and flexible power system. In addition, the IEEE C37.240 standard addresses communication security issues in power system automation and control, where IEDs are used to protect, monitor, and control power system equipment. The standard defines a set of requirements and guidelines for implementing security communication protocols that are compatible with IEDs. The standard

[34] *AMI-SEC Task Force, "Security Profile for Advanced Metering Infrastructure. Technical report" AMI-SEC Task Force, 2010.*

[35] *Rodriguez, M., Lazaro, J., Bidarte, U., Jiménez, J., & Astarloa, A., "A Fixed-Latency Architecture to Secure GOOSE and Sampled Value Messages in Substation Systems", IEEE Access, 2021.*

includes recommendations for security message formats, data types, data encoding, and data transmission. It also provides guidance on security management, such as access control, user authentication, and data confidentiality. IEEE C37.240 plays a critical role in ensuring the reliable and secure operation of the power grid. It helps to mitigate cyber risks and threats in power system automation and control and prevent cyber attacks and other security threats.[36]

## 4. Certification of Standards

Although creating a list of standards to address cybersecurity issues is a good starting point, there must be a certification process to ensure that governance, software, networks, and devices in the power grid system have at least the minimum level of protection. If established standards are not adopted and implemented by power grid systems, hackers may exploit these vulnerabilities to pivot and attack other systems. The power industry places special emphasis on implementing cybersecurity-related standards due to government regulation and policy. For example, in the case of large-scale power generation systems, a specific organization responsible for certifying and implementing standards (such as NERC maintaining an organizational certification program) can execute the certification program through industry alliances representing the government, corporations, owners and operators, as well as research and academic institutions. However, to nail down the cybersecurity of emerging power grid systems, stakeholders are beginning to implement basic cybersecurity best practices in wind energy systems.[37]

[36] *Dong, S., Cao, J., Flynn, D., & Fan, Z., "Cybersecurity in smart local energy systems: requirements, challenges, and standards", Energy Informatics, 2022.*

[37] *Office of Energy Efficiency And Renewable Energy "Roadmap For Wind Cybersecurity", U.S Department of Energy, July 2020.*

# Countermeasures to Address Smart Grid Cybersecurity Threats

In order to address these threats, power grid operators and governments around the world are implementing a range of cybersecurity measures, including network segmentation, multi-factor authentication, and regular security training for employees. Additionally, regulatory frameworks are being developed to ensure that power grid operators have robust cybersecurity plans in place.

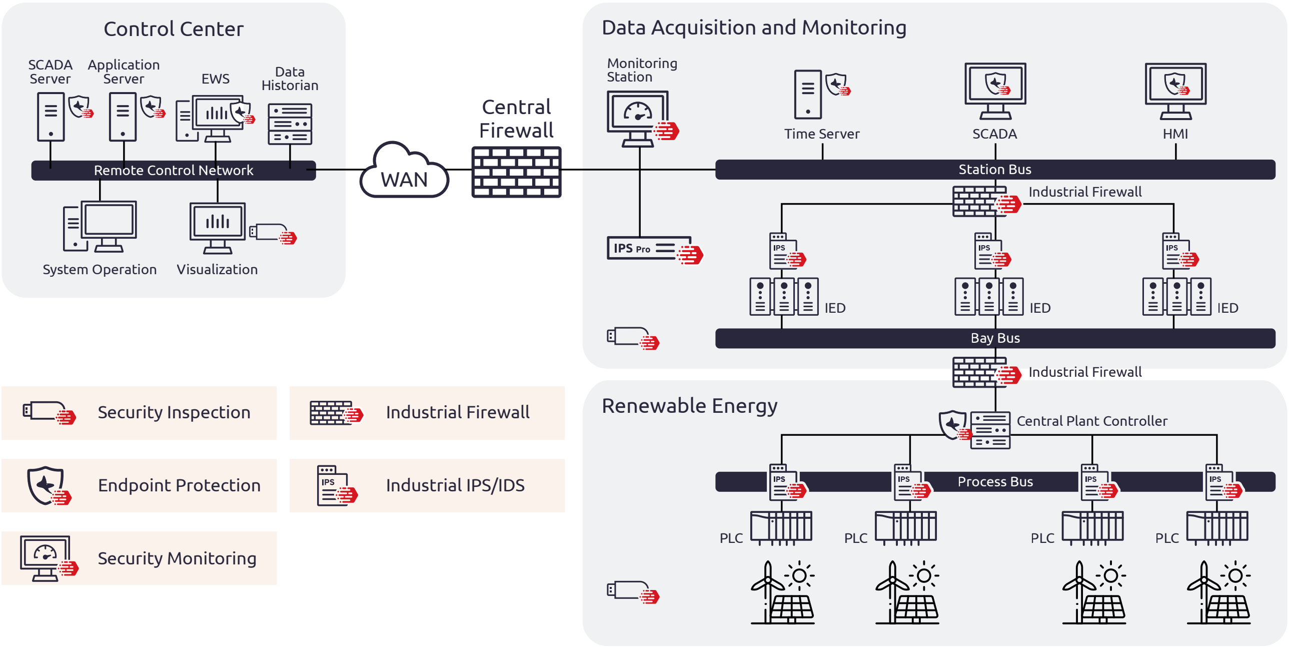


*Figure 8: A Reference Architecture with Cybersecurity Approaches for Smart Grid Environments*

## 1. Establish Good Cyber Hygiene Practices for Vulnerability and Threat Management

Implementing cyber hygiene practices is critical for ensuring the security of smart grids. Before deployment, it is important to proactively check new equipment to ensure that it does not introduce new security risks to the organization's cyber posture. When introducing new equipment into the organization's system, it is important to actively inspect the equipment to identify whether there are any serious vulnerabilities or malicious code present. This process is essential as it enables the organization to ensure that the new equipment is secure, and that vulnerability remediation has been properly completed. One way to proactively check equipment is to conduct vulnerability assessments and threat scanning. These technologies allow organizations to identify potential vulnerabilities and threats in the system and conirm whether suppliers are effectively mitigating these vulnerabilities.

Initial attacks may come from equipment suppliers before power plant equipment enters the factory facilities, so power grid operators should conduct malicious software scans on each asset entering factory facilities and establish health records to ensure that equipment does not contain malicious software or critical vulnerabilities. To mitigate supply chain attacks, Portable Inspector can be used to automatically scan for malicious software, vulnerabilities, and system configurations without connecting to the network. By using Portable Inspector, asset owners can avoid violating warranty terms and detect malicious software without having to replace complex equipment. This will help power plants ensure the integrity of their equipment while also complying with specific industry regulatory compliance requirements, such as NERC CIP standards, IEC 62443, and NISTIR 7628.

## 2. Network Segmentation, Trust Lists and Detection

### • Network Segmentation

To reduce the risk of cyber threats and maintain the reliability of the power grid, it is recommended to divide the smart grid network into the smallest possible areas. However, to achieve the minimum area, network segmentation technology is needed to divide the network. Segmentation methods can be roughly categorized as two types: physical segmentation involving the use of hardware such as routers and switches to create separate networks, and logical segmentation using virtualization and network security policies to separate traffic between different areas of the network. By separating the network, access to critical parts of the system can be prohibited, and potential threats moving laterally between IT and ICS networks can be stopped in their tracks. At the same time, a network trust list can prevent unauthorized network access, i.e., trusted addresses are added to the trusted list, while any requests received from unknown sources are discarded.[38] TXOne Networks' OT native EdgeIPS and EdgeFire can implement network segmentation and boundary security defense, dividing power grid ICS/OT networks into the smallest zone in an effective way to improve network security. The implementation of these measures can prevent threats from moving laterally between IT and ICS networks and prevent network attacks.

### • Automated Intrusion Detection:

As described in the previous sections discussing attack cases, many threats are related to data integrity (e.g., DoS and FDIA attack vectors). In addition to network segmentation, detecting malicious behavior on electric grid OT/ICS networks is necessary.[39] The grid needs to transmit widely scoped measurement and configuration information, which can be used for anomaly identification and classification by inspecting communication metadata or correlating and comparing with out-of-band data sources (e.g., SCADA, AMI). The development of IDS may consider detection of specific ICS protocols and automatically block the source address when detecting specific attack scenarios. TXOne Networks' EdgeIPS can analyze multiple grid communication protocols and perform network intrusion detection based on unique specifications, such as abnormal detection of substation GOOSE.

[38] *Zografopoulos, I., Konstantinou, C., & Hatziargyriou, N., "Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations", December 2022.*

[39] *Boeding, M.; Boswell, K.; Hempel, M.; Sharif, H.; Lopez, J. Jr.; Perumalla, K., "Survey of Cybersecurity Governance, Threats, and Countermeasures for the Power Grid", MDPI, November 2022.*

- ### Virtual Patches:

Virtual patching technology can help isolate critical assets and provide an additional layer of protection. By implementing these practices, the grid helps provide protection measures for some older assets, such as using vulnerable communication protocols, to maintain grid reliability and maintain continued power supply to homes and businesses. TXOne Networks' EdgeIPS or EdgeFire has specially designed packet filtering network policies aimed at resisting attacks that exploit known vulnerabilities in communication protocols without requiring endpoint system updates, meaning this technology can be used without restarting or stopping the power system.

## 3. Provide Reduced Attack Surfaces and Strong Endpoint Protection

- ### Ransomware Protection:

Limiting file access can help organizations mitigate the impact of ransomware. File access restriction refers to allowing only trusted applications to access protected files on ICS/OT endpoints. Applications are added to the trusted application list based on their ICS signature, and enterprises can also add or remove applications from the trusted application list.

- ### Software Process Chain Lockdown:

System hardening measures are necessary during device software activation to eliminate or reduce attack vectors, including deploying antivirus software, disabling unnecessary software services, disabling high-risk network protocols, restricting user privileges, and managing physical ports (such as USB connections). By securing assets, technicians can significantly reduce the chances of attackers gaining access to critical systems and prevent the execution of malicious programs. For example, using Stellar Application Control technology, certain risky software behaviors can be restricted, including launching executable files and scripts that attempt to download or run other files, or launching applications that do not normally run during standard operations.

- ### Device Control:

As described in the previous attack scenarios, many threats can enter the OT environment through portable media. In particular, in physically isolated environments, hackers can use removable drives (such as USB drives) to launch attacks. Stellar helps prevent unauthorized peripheral devices from compromising your devices. You can configure it to block or allow removable devices and files on removable devices, providing an added layer of protection.

# Conclusion

The power grid is undergoing an unprecedented shift towards the deployment of distributed energy resources (DER), enabling customers to have more energy choices and control. This transformation is driven by technological advancements and environmental goals, resulting in market forces for critical infrastructure investments. Emerging renewable energy sources such as wind and solar power are leading the energy transition, fundamentally changing the planning and operation of the grid, as well as the power load itself (e.g., power transportation). At the same time, this energy transition can diversify the energy resources of the grid and make the power system more resilient through microgrids to maintain critical power during grid failures, extreme weather, and even cyber attacks.

During the power grid transformation, cyber attacks within the economic scope have steadily increased over the past two decades. Today, attackers are developing their practices and capabilities faster to target new technologies, and hackers can easily infiltrate smart grid systems. Smart grid threats cover two core areas: inherent system vulnerabilities and external cyber attacks. Vulnerabilities in smart grids have been discussed in various aspects and are constantly evolving in complexity. In addition, we have also conducted a global review of cyber attacks against smart grids between 2010 and 2022, which have different characteristics, such as internal threats, lateral movement from IT networks, remote service vulnerabilities, web application interface vulnerabilities, and supply chain threats, among others.

Ensuring the security of the smart grid is crucial to maintaining the reliability and safety of our power systems. Implementing effective cybersecurity measures, such as network segmentation, intrusion detection, and endpoint protection, helps prevent potential threats and reduce system risk. Proactively checking new equipment before deployment and closely monitoring vendor patches are also critical to maintaining a strong cybersecurity posture. Adopting TXOne's OT Zero Trust is one way to address this challenge and reliably protect facilities from present day and future cyberattacks. These practices enable power grid operators to enhance the cybersecurity and resilience of their systems and ensure critical assets are protected from cyberattacks.

**txone.com**