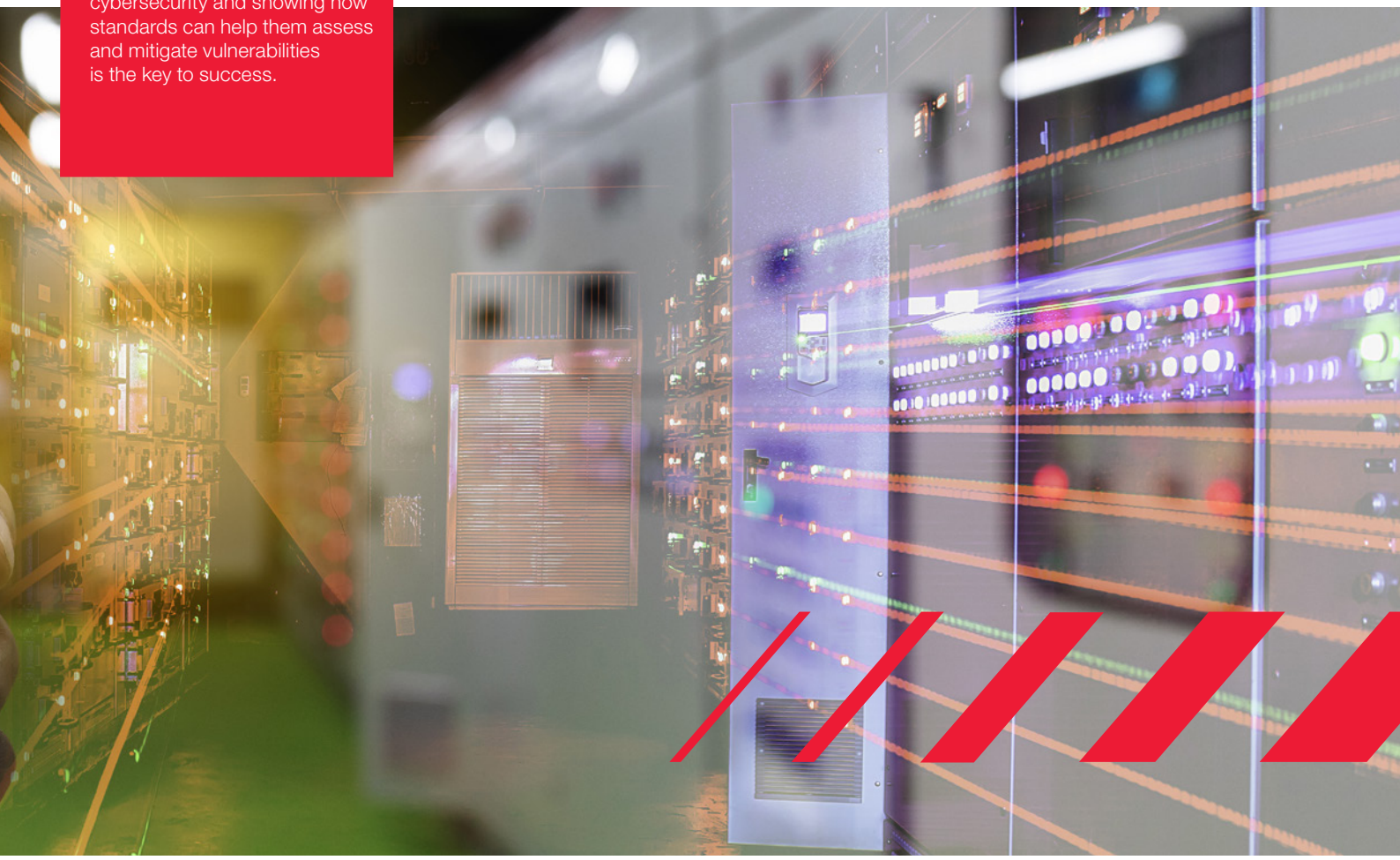
For the digital transformation of substations, educating utilities about the benefits of cybersecurity and showing how standards can help them assess and mitigate vulnerabilities is the key to success.

HITACHI
Inspire the Next



Cybersecurity compliance for digital substations

Hitachi Energy

Cybersecurity for electricity distribution is crucial because these systems link to other industries such as healthcare, communications, transportation, water treatment, and other critical infrastructure. Electricity transmission and generation control systems often interface with electricity distribution, especially in vertically integrated companies. This can create vulnerabilities. For example, attacks on gas supplies could affect combined heat and power generation, or downtime for a third-party datacenter could compromise utility operations.

When utilities develop cybersecurity for their own systems, it is important to collaborate with other industries and to understand the implications of emerging concepts and trends that can increase the attack surface, such as the Internet of Things (IoT).

Cybersecurity compliance for digital substations

Electric utilities are accelerating development of smart grids with sophisticated communications that give them a greater ability to monitor and control distribution systems by retrofitting existing infrastructure and adding intelligent electronic devices (IEDs). Digital substation communications are a key component of grid modernization plans because they improve reliability and availability for their mission critical application and help utilities adopt flexible, proactive practices, especially in support of wireless systems for remote areas and in harsh conditions.

However, digitalization and other new technologies make systems more vulnerable to cyberattacks. To defend against cyberattacks, utilities must incorporate increasingly robust and adaptable security measures into their modernization plans. This includes upgrading the automation and communication (A&C) systems installed over the last 20-30 years that were not designed around modern cybersecurity concepts. These systems can pose compliance challenges with rapidly changing cybersecurity requirements and the shifting regulatory environment, compromising their ability to securely operate and maintain the installed base.

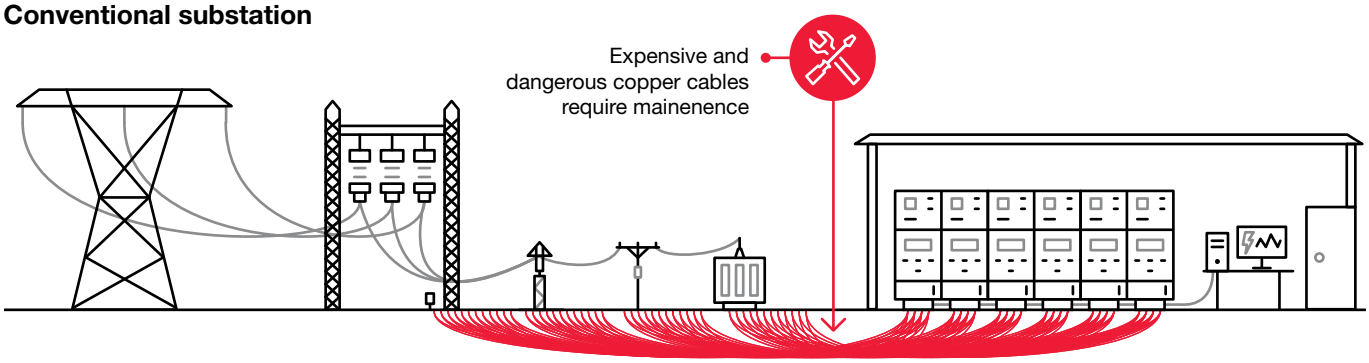
In 2015 and 2016, cyber attacks compromised information systems of three energy distribution companies in Ukraine and temporarily disrupted the electricity supply to consumers, driving home the importance of cybersecurity for digitalized infrastructure. Now, rather than an afterthought, cybersecurity programs are an inherent element of smart grids, and utilities need to fulfill regulatory requirements and provide optimal protection.

Those regulatory requirements and standards are constantly evolving, which can pose compliance challenges to utilities and equipment suppliers. The standards generally take two forms, regulatory and technical, and sometimes conflict. From an operations standpoint, utilities may see standards as restrictive, especially maintaining regulatory compliance through organizations like the North American Electric Reliability Corporation (NERC) in the US. For example, under NERC-CIP (Critical Infrastructure Protection) guidelines, communications extending digital substation cyber assets into the switchyard can be securely implemented while satisfying compliance standards. The information gained from digitalized substations is essential for improving system performance, allowing proactive control, and supporting predictive maintenance and asset management. This type scenario presents a potential conflict between what is best for operating the utility (e.g., capabilities for gathering information to improve performance and reliability) and what is required to maintain compliance.

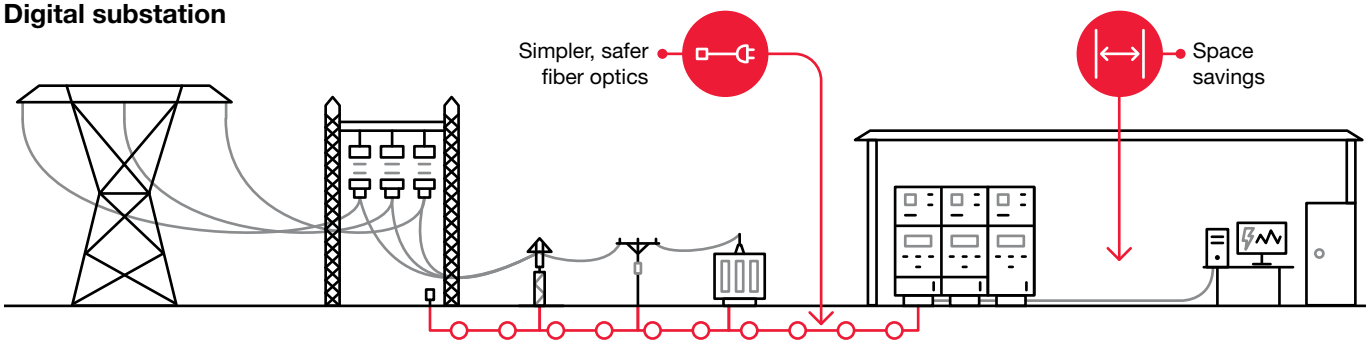
Interconnectivity, based upon open standards, has improved reliability, but also increased the number of vulnerabilities. Rather than restricting grid modernization programs, standards provide a framework for finding the balance between improved reliability and managing cybersecurity risks. For the digital transformation of substations, educating utilities about the benefits of cybersecurity and showing how standards can help them assess and mitigate vulnerabilities is the key to success.

Digital substations

Conventional substation



Digital substation



Smaller, safer and more efficient
Digital substations replace many point-to-point copper cables with a single fiber optic process bus.

As part of upgrading substations, many utilities are moving away from conventional hardwired designs with standalone components and toward digital substations that utilize modern communication systems connected to a utility's central control systems. This "digitalization" process usually involves replacing copper wiring and installing wireless systems or fiber optic communications as new components are retrofit into existing layouts.

As enterprise, automation, and control systems become increasingly interconnected and digitalized, the risk of exposing operational and confidential data increases. New technical standards must support a utility's compliance with regulations and maintain cybersecurity levels as substations move from electro-mechanical systems to digital controls.

Substation communications layout

A typical large substation (as depicted in the figure above) includes a control building and a communication system with copper wires connecting assets to the building. In a digitalized substation, the control building includes automation, protection, and control systems, alongside a communications bus using IEC 61850 standards (see discussion below for details on IEC 61850). Control for a digitalized substation uses the Generic Object-Oriented Substation Events (GOOSE) peer-to-peer multicast messaging, contained within IEC 61850.

Communications extend outside the control house into the switchyard and connect all devices digitally. A single optical fiber line, the digital process bus, replaces the multiple copper connections. The new line can carry current and voltage measurements and send commands between the protection and control system and high voltage assets. It also collects asset information and monitoring data from digital transformers and breakers.

Advantages of digitalization

One of the main reasons utilities are digitalizing substations is to gain access to additional data which allows them to take advantage of new smart grid technologies, making it easier to build, operate, and maintain these critical facilities. Digital substations increase the responsiveness of distribution and transmission grids, using near real-time data to react to asset conditions and enhance grid stability. Digitalization also enables utilities to increase the supervised area of physical and electronic perimeters which improves visibility of cybersecurity incidents and attacks. Enhanced visibility supports wider monitoring and ensures that systems can identify and proactively mitigate with issues more quickly before they escalate and become difficult to neutralize.

Another important advantage of digitalization is the significant reduction in the amount of copper wiring in a substation, which is costly to install, maintain, and replace. Fiber optic cables are cost-effective and require fewer labor hours for trenching, installation, maintenance, and testing to ensure a higher quality system.

In summary, digital substations provide a range of potential benefits that would be difficult to achieve with traditional electro-mechanical or first generation microprocessor relay systems.

Digitalization and asset performance management

Asset management performance shows how digitalized substations provide measurable benefits and can make a difference in the ways utilities operate. Increased connectivity and digitalized systems allow utilities to monitor the condition of transformers, tracking performance and monitoring health at the breakers. The system can track assets and send the information to an asset health center for a performance analysis.

A risk-based application determines the condition of assets and uses a traffic light system to depict when an asset needs closer monitoring or give a red warning when imminent failure is likely. This risk-based optimization supports a proactive maintenance philosophy for substations, which is the main goal of utility asset management. Of course, successful asset management needs the protection of cybersecurity because it helps utilities understand any inherent vulnerabilities of digital assets and their system. In turn, this understanding of potential weaknesses supports detailed risk evaluation during asset performance management.

Challenges of digitalization

Despite the obvious advantages of digitalization, some utilities are reluctant to adopt the technology because it also brings some challenges. One issue involves legacy technology: utilities must decide whether to update, upgrade, or replace existing systems. Some may opt for a flexible solution that interfaces with legacy systems and supports an incremental approach. Accordingly, their cybersecurity program will need to cope with utility-specific approaches, and the applicable standards need to be flexible.

Another issue with legacy Ethernet and TCP/IP-based communications is that, while they promote interoperability, they also increase the attack surface and increase vulnerabilities to malware and viruses. In 2008, when NERC-CIP was first enforceable, the organization (NERC) felt that Ethernet technology left too many vulnerabilities and banned routable protocols, instead supporting non-routable protocols for mission-critical applications. Even with these regulations in place, the applications and protocols using Ethernet did not always provide a sufficiently strong security mechanism to protect against common attack vectors. Today, utilities are increasingly moving to communications systems that routinely use GOOSE and Sampled Values (SV) protocols as non-routable communications offering real-time operation.

Due to these challenges, some utilities perceive that the disadvantages of substation digitalization outweigh the benefits. Because the NERC-CIP standards carried large penalties for utilities who failed to comply, many substation engineers felt these restrictions prevented them from creating reliable substations. Standards organizations need to overcome this perception through promoting the benefits of substation automation.

The digital advantage
Digital substations offer several key benefits over traditional substations.

Perceived challenges of adopting standards

To combat the misperceptions about standards, regulating organizations need to promote the advantages of how digitalization improves system performance. Information supports proactive control, and facilitates operations and maintenance, while cybersecurity enables digitalization and system improvements. Standards should not be viewed as restrictive but should be seen as providing a framework for compliance and achieving the best practices from a technical perspective.

Substation automation, protection, and control technologies have evolved significantly over the past few years and will continue to change as new technologies emerge. Interconnected systems provide utilities with the information they need to improve reliability, and standards promote interoperability between different products. Fostering interoperability through a combination of open standards and commercial technologies helps ensure that utilities do not end up backing the wrong technology and end up with unsupported systems or stranded assets.

"Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."

US Cybersecurity and Infrastructure Security Agency

Increased connectivity can create vulnerabilities, but open standards are intended to achieve interoperability while ensuring the availability of cybersecurity options. Open standards can be seen as primer elements designed to reduce vulnerabilities and display the intent of the power industry to reduce the risk of cyberattacks. Interoperable standards like IEC 62351 ensure that vendors implement and integrate cybersecurity measures in a way that supports a defense-in-depth approach in which a series of defensive mechanisms are layered to protect valuable data. However, the idea that it is "impossible" to implement IEC 61850 solutions and move digital technology into the switchyard, while complying with NERC-CIP, endures.

Cybersecurity

Two considerations shape definitions of cybersecurity and affect the standards and approaches used to develop solutions. On one hand, there is the software side of cybersecurity that refers to maintaining control of IT systems and data, and on the other hand is the need to protect physical access.

The Institute of Electrical and Electronics Engineers (IEEE) Power System Communications and Cybersecurity Committee (PSCC) includes defense against physical intrusions in its definition[1] to acknowledge the need to defend against physical access to sensitive information. IEEE uses the term 'cybersecurity' rather than 'cyber security,' which is more common with IT organizations focused on electronic intrusions.

Physical cybersecurity does not just mean protecting against things like drone attacks or terrorism which may affect the physical integrity of a substation. Physical cybersecurity can include a variety of measures designed to prevent someone from breaking into an installation, accessing a port on a protective relay, or downloading information onto a USB drive.

Digitalization and security

Developing a digitalized substation usually requires fiber optics, and Ethernet has attracted a reputation for insecure communications that allow external actors to access systems and compromise information. It is important to demonstrate that the benefits of digitalization far outweigh any potential disadvantages by educating everybody involved in the process, showing how to mitigate risk, and suggesting how cybersecurity can offer the necessary protection. Digitalization is a natural byproduct of implementing cybersecurity measures at the device and system level and supports the monitoring and identification of threats. For utilities, it is important to select trusted partners that provide a combination of available high-performance, mission-critical applications with the latest cybersecurity standards.

1 IEEE, PSCC S1 SG: IEEE 1686 Standard for Intelligent Electronic Devices Cyber Security Capabilities, Summary Minutes for Subcommittee Report, Dec. 2017, https://site.ieee.org/pes-pscc/files/2019/01/IEEE-PSCC-S1-WG-Minutes-Jan-2019.pdf

Accordingly, when developing substation protection and control systems, cybersecurity should form an inherent part of digitalization plans, with a roadmap showing the steps needed to make the entire system secure. Industry standards provide a robust framework for developing cybersecurity roadmaps, especially when integrated with best practices from other electric utilities. Cybersecurity systems need to be monitored, maintained, and upgraded which costs time and resources. However, the cost of not implementing cybersecurity could be far higher, so cybersecurity should not be viewed as an additional expense but an inherent part of the digitalization process.

While regulatory requirements can provide useful foundations, focusing only on the regulations pertinent to the power sector can cause useful lessons from other industries to be overlooked. As an example, financial institutions have relied on cybersecurity for a much longer time than most utilities and have valuable lessons to share about protecting systems and data. Utilities should try to institutionalize best practices from other industries and utilities and develop an optimal approach to cybersecurity built upon managing and mitigating risk.

When digitalizing substations, simply adding cybersecurity onto a wider grid modernization program as an afterthought is unlikely to succeed. It is important to cultivate a cybersecurity culture throughout an organization through education and training to raise awareness. Compliance with regulations should be a goal, because it allows a utility to take incremental steps by working from the basics, but utilities should actively pursue cybersecurity best practices from all sources.

The need for a layered defense

A fundamental reality of cybersecurity is that 100% security is impossible to attain. Technology is constantly changing and hackers constantly improve their techniques to discover and exploit vulnerabilities. Accordingly, the most effective security systems evolve with the technology landscape and include a layered defense approach to reduce risk.

The best OT and IT cybersecurity systems offer a flexible, multifaceted approach that is adaptable over time and promotes defense-in-depth. This allows utilities to cope with a range of different threats and allow systems to continue operating with minimal disruption and recover quickly if affected.

For electronic and physical defense, the system should be focused on preventing unauthorized access by developing a system of access rights by monitoring and detecting intrusions, creating alerts and reports, and should include procedural measures such as a system for reviewing access rights and log files.

The convergence of OT and IT

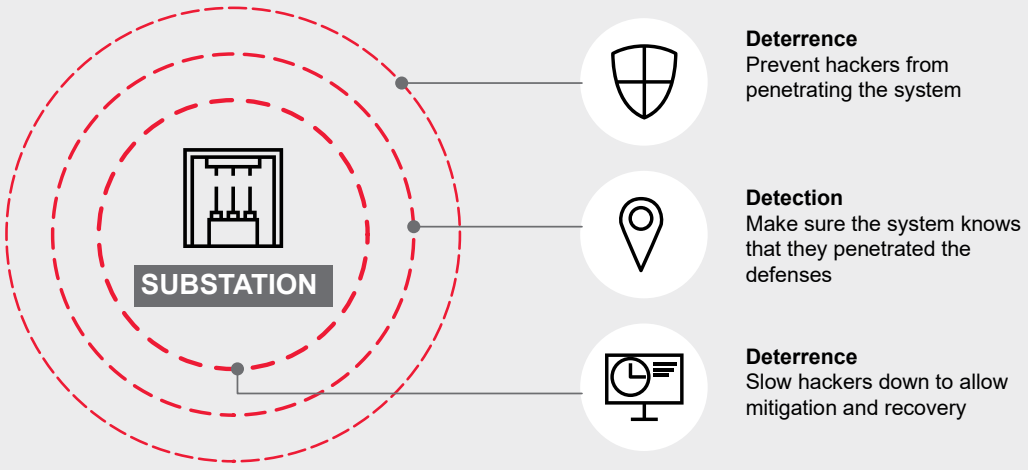
Operational Technology (OT) comprises the devices, sensors and software necessary to control and monitor the means of production – the physical equipment. Information Technology (IT) combines all necessary technologies for information processing. As OT is increasingly digitalized, the data generated by the equipment can be ingested into IT systems where it can be analyzed and visualized to help organizations gain new insights and see their operations in new ways.

With these measures in place, key cybersecurity capabilities include:

- Secure communications
- Zoning and perimeter protection
- Malware protection
- Patch management
- Backup and recovery
- Account management
- Security logging and monitoring
- Product and system hardening

These different elements provide a highly integrated approach that extends to cover all of the vulnerabilities in a digital substation, encompassing IT and OT to ensure maximum protection of the entire system.

Three layers of defense
Utilities need a flexible approach to cybersecurity that maximizes continuous operation while delivering defense-in-depth.



IT vs. OT: a difference in philosophy

One challenge to overcome is the variation between IT and OT in an organization, because they often have very different priorities when it comes to cybersecurity. For most IT departments, the main priority involves protecting sensitive personal, legal and financial information, largely due to cross-fertilization of ideas from other industries. Conversely, OT and industrial control systems emphasize continuity of physical processes and protection of components.

While they share many of the same basic objectives, approaches for protecting OT infrastructure are different from the ways IT systems are protected. A major difference is that the OT environment can affect the management of the cyber-physical power system which can directly affect power system safety and reliability.

From the industrial control perspective, protecting health, the environment, and systems in order to mitigate the financial cost of disruptions is more important than protecting the data itself. In this respect, there is a difference between system availability and system reliability. An OT department is usually only concerned with computer problems if they affect the utility's protection and control system and have a negative impact on system reliability.

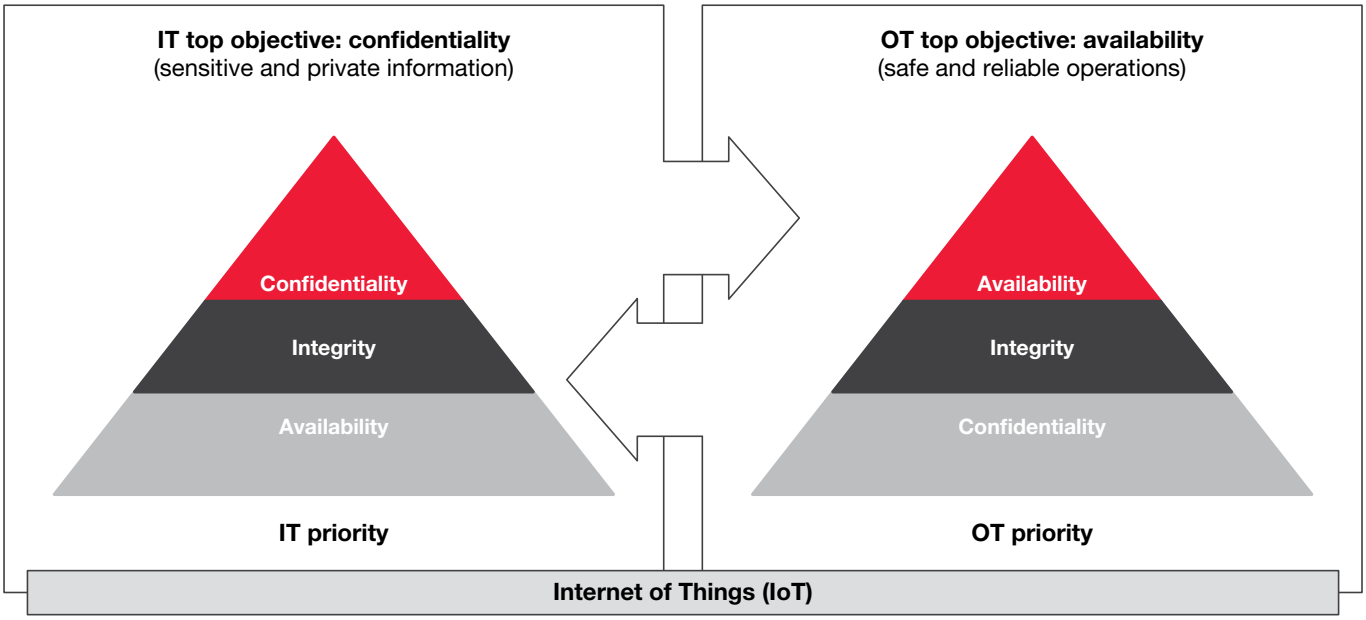
Consider an example of an attempted distributed denial of service (DDoS) attack on a substation. While IT and OT departments would likely agree that swift and decisive action is necessary, they may have different responses and solutions. An IT department would likely be inclined to create an "airgap" to isolate the problem and stop the threat, whatever the cost. In contrast, the OT approach would be to attempt to keep the system active while trying to investigate the problem.

Given a substation's critical importance in an electrical system, striking a balance between cybersecurity and reliability is the goal. During an attack, isolating only the compromised sections while keeping the rest of the equipment operational is preferred. Isolation should not affect mission critical functions of the system that allow the intrusion prevention system (IPS) to minimize impacts of an attack. It should be noted that establishing this type of protection requires deep domain knowledge of power systems and automation/protection and may be beyond the realm of many IT system security providers.

Although a silo mentality between IT and OT security departments often exists, the barriers are falling as OT systems become more digitalized and both sides recognize the benefits of the other's philosophy. This cultural change encourages unified approaches that provide a more thorough level of protection across both ecosystems. To help bring the sides together, IEEE has developed a working group to create a language that unites the two perspectives and emphasizes common utility goals such as delivering secure power to customers.

In December 2015, information systems of three energy distribution companies in Ukraine were compromised in what is considered to be the first known successful cyberattack on a power grid. While the attack temporarily disrupted the electricity supply to consumers, it was also a wakeup call to the entire electrical industry and provided an opportunity for utilities to learn and adapt to the threats as part of developing a mature approach to cybersecurity based on standards.

Convergence of priorities
Cybersecurity priorities have traditionally been inverse for IT and OT organizations. The accelerating adoption of IoT is changing the needs of IT and OT, bringing them closer together and shifting priorities towards one another.



The importance of standards

Over the past few decades, a number of government agencies and industry associations recognized the mounting vulnerability of electrical grids and issued standards intended to help utilities and product vendors shape their cybersecurity strategies. Given the severe consequences of failure, a number of organizations developed cybersecurity regulations and technical standards for electrical systems in general and for substations in particular.

In 2008 and 2009, the US Federal Government's recession stimulus packages included provisions intended to help utilities develop smart grids and emphasized development of relevant technology, but few strategies or requirements covered cybersecurity. In response, the US Department of Energy Smart Grid funding mandated cybersecurity. This prompted creation of the National Institute of Standards and Technology (NIST) Interagency/Internal Report, NISTIR 7628, which defined the important interconnections on a utility system and highlighted the main areas security standards should cover.

Other standards organizations, such as IEC and IEEE, quickly followed suit and began developing technical standards to document best practices. At the time, IEEE emphasized the security of power system relays and did not really focus on substations. As a result, the first real standard for cybersecurity was IEEE C37.240, which defined the requirements for power system automation, protection, and control. This standard is presently undergoing revision.

Another particularly important set of standards is NERC-CIP, which focuses on the security of electronic perimeters and the protection of critical cyber assets as well as personnel and training, security management and disaster recovery planning.

While NIST focused on overall smart grid architecture, IEEE committees started developing cybersecurity standards for power systems and, in 2017, they developed cybersecurity standards that covered substation digitalization, including:

- Physical layer
- Protocols
- Interoperability
- Profiles and mapping
- Architecture
- Security – both physical and cyber

Because of its demand for regulatory compliance, NERC-CIP, in many ways, came to dominate standards for digital substations and were adopted by organizations outside North America.

NERC-CIP and non-routable communications

One important distinction for cybersecurity is the difference between routable and non-routable protocols. Routable protocols, in an Ethernet system, can pass through different areas of the system which makes them attractive to hackers and other "bad actors" with malicious intent. In contrast, non-routable protocols do not leave the area in which they operate, so it is difficult to forward the protocol and access systems, making them more secure.

When IEC 61850 first emerged, NERC assessed the standard and argued that routable protocols in substations were creating vulnerabilities. Accordingly, they advocated non-routable communication as an alternative. However, in 2007, NERC accepted that it also had to promote reliability as part of its organizational philosophy. This created a conflict between promoting reliability by the CIP organization, and cybersecurity as emphasized by the Protection Relay and Control (PRC) organization. Finding the right balance became crucial for future development of smart substations.

Ultimately, increasing reliability means generating more information, which requires digitalization. The idea of leaving an air gap within communications systems does not support this and, as a result, NERC adopted IEC 61850, as have many utilities. Now, open standards have promoted compatibility and a willingness among utilities, vendors, and research institutions to develop common solutions.

It is important to note that even non-routable protocols need a level of cybersecurity, because any serial communications outside the system still face threats, especially through direct message protocols. Attackers can intercept communication if unencrypted and they can "spoof" it so that incorrect information reaches the control center. It may also be possible to intercept commands from the control center and send trip commands. Therefore, non-routable communications are still subject to NERC-CIP compliance. Now, there is greater collaboration between the NERC and IEEE PSCC, and a move towards balancing reliability with cybersecurity, building this around routable communications and ensuring that regulatory and technical standards work together.

Applicable standards and best practices for substations

A number of standards are applicable to substations, some covering communications for the wider power system, while others focus on digitalized substations.

Standard	Description
NISTIR 7628	NIST's Smart Grid Interoperability Panel (SGIP), responding to the Energy Independence and Security Act, coordinated standards for smart grid communications. NISTIR 7628 includes protocols for managing information and interoperability for smart grid solutions. It encourages the use of digital information and control technology to improve reliability and efficiency, while optimizing cybersecurity.
NERC-CIP	The NERC-CIP standards protect critical infrastructure and transmission, including cyber assets, and compliance is mandatory for the bulk energy system (BES). The standard covers control centers and systems using a high category for transmission control centers, while substations tend to fall under the low or medium categorization, making compliance less stringent. Product vendors and system integrators do not provide certification for NERC-CIP compliance and utilities are responsible, although many vendors include technical features to support compliance.
IEEE C37.240 Standard Cybersecurity Requirements for Power System Automation, Protection and Control Systems	The C37.240 standard covers the suitability and technical implementation of NERC-CIP and NIST smart grid security standards for digital substations. It covers substation automation, protection, and control systems, and it applies engineering principles independent of voltage or the critical nature of particular cyber assets. IEEE published the standard in 2014, and it is presently under review.
IEEE 1686 - IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities	The IEEE 1686 standard defines the essential security capabilities of intelligent electronic devices (IEDs), including protective relays installed in digital substations. Some requirements do not apply to substation IEDs, but help a utility understand their cybersecurity measures and capabilities. The standard covers user authentication and security event logging, and leaves room for tailored solutions such as interfaces with legacy software. The standard allows manufacturers/vendors to state the security capabilities of their device, and helps utilities consider cybersecurity consistently.
IEC 62351	The important IEC 62351 standard focuses on security management functions and the overall requirements for the management of data and communications. This technical security standard intends to secure communication protocols designed for power systems, such as IEC 61850 or IEC 60870-5-104. Presently under development, the standard uses digital signatures and authorized access, and supports intrusion detection.
IEC 62443 (Former ISA S99)	This newly introduced standard, derived from ISA S99, covers security for all aspects of the control system, and probably includes substations. The standard defines requirements for the value chain, the supply side, and the system integrator. The ISA Security Compliance Institute (ISCA) program assesses whether devices conform to this standard, while other IEC 62443 certification programs confirm the cybersecurity capabilities of a device.
IEC 61869	This standard is not cybersecurity-related and focuses on instrument transformers, but it can support interoperability of substation components. While many utilities still refer to the process bus as 61850, many are transitioning to 61869. The standard covers the instrument values on non-conventional instrument transformers, so it will have an effect on interoperability.
IEC 61850 9 2 – Process Bus	IEC 61850 defines communications protocols for IEDs in substations, and supports a number of protocols, including GOOSE, Manufacturing Message Specification (MMS), and Sampled Measured Values (SMV). The protocols can use TCPIP or substation LAN using Ethernet, and the standard defines the communications architecture for station and process buses to enhance interoperability in substations using Ethernet.

Example substation standards

With a number of standards covering cybersecurity for digitalized substations, it is useful to show how to implement them in practice. In the figure below, the network control center is at the top, with the communication infrastructure entering the substation. For this typical layout, IEC 62443 covers almost all aspects, including product security standards, products development, and system integration, showing how it is a very comprehensive standard. In a similar way, IEEE 1711.2 protects the communications leaving the substation to the control center.

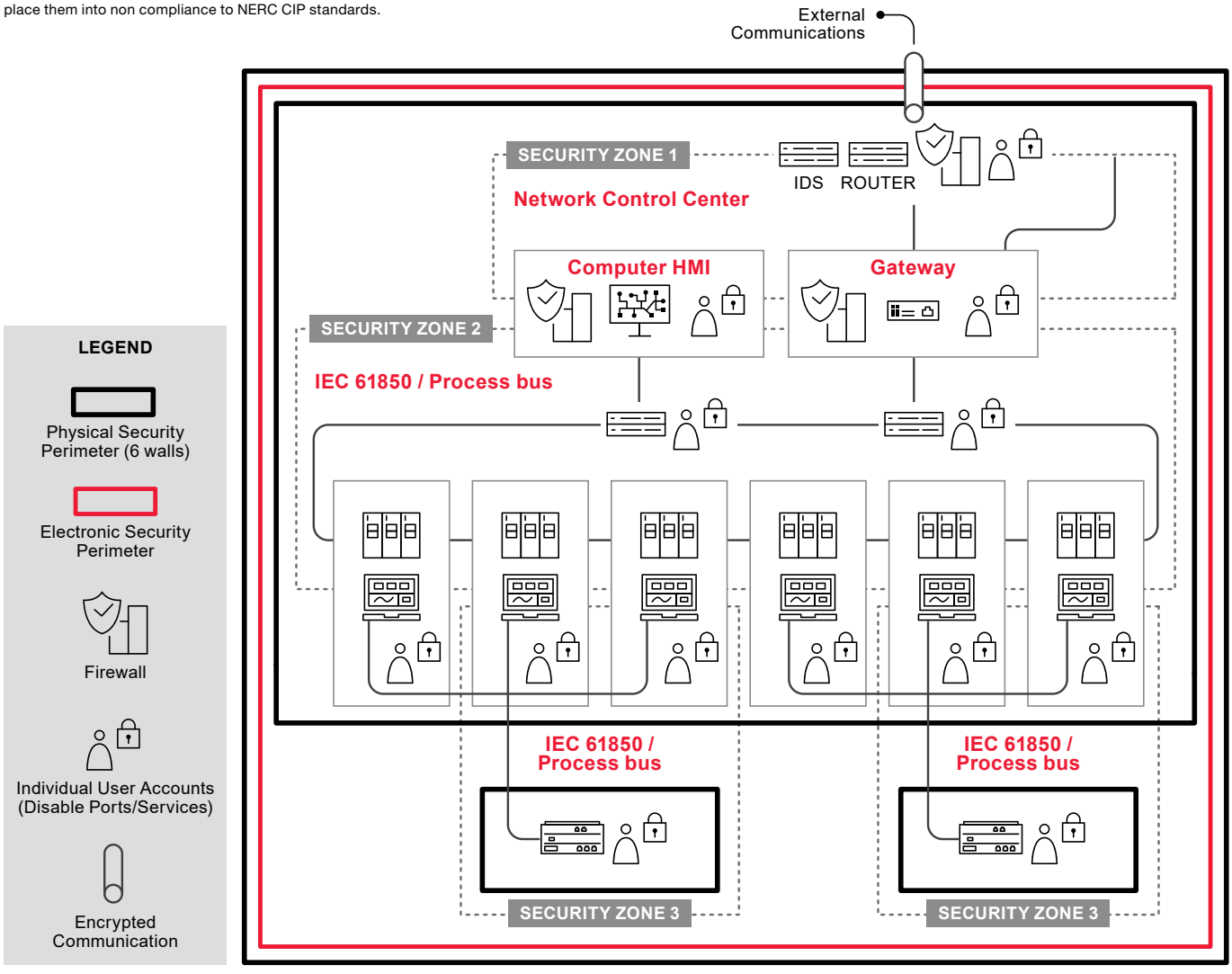
In the center, the NERC-CIP, the IEEE C37.240 standard and IEC 62351 all apply. Importantly, NERC-CIP differs from the IEEE and IEC standards in that it is performance based, not technical, so it tells utilities what they need to do but not how they should do it. This leaves scope for a companion set of technical standards, which draw from industry best practices and technical expertise. These technical standards can provide a blueprint and help utilities achieve their desired cybersecurity goals.

One example is IEC 61850-9-2, which covers the process bus in the form of the connection replacing the copper wires. When this bus leaves the control house and enters the physical substation, does it create a NERC-CIP violation? The concern with process bus and monitoring/control station bus applications in the switchyard was that it would break the electronic security perimeter (ESP) and would thereby violate NERC-CIP. Only point-to-point, non-routable interfaces fulfill the regulatory requirements and maintain compliance, according to this belief.

The system is covered by various technical standards and failing to follow these can lead to violations of NERC-CIP. In other words, failing to protect a system can inevitably lead to a violation of the CIP standards, which is difficult to avoid under current guidance. However, the new version of the technical standards in Version 5, promoted by the PSCC and presently underway, will allow the process bus to become a viable solution without violating the NERC-CIP standards.

Another change to the standards process involved the working group covering IEC 61850 working with the Utility Communications users group (UCA), which covers operations outside the substation. In the diagram, the inner black line depicts the electronic security perimeter. Before Version 5, the electronic security perimeter had to be contained within “six walls,” which essentially defined the perimeter as the control house. However, Version 5 removed this requirement, making it possible to have routable protocols running outside the control house into the switchyard and reflecting the availability of suitable modern technologies. Within the substation, single password protection is permitted, and the standards support routable protocols.

Substation automation and NERC CIP
In the US, some utilities believe routable protocols and configurable IEDs in the substation switchyard (outside of the control building) will place them into non compliance to NERC CIP standards.



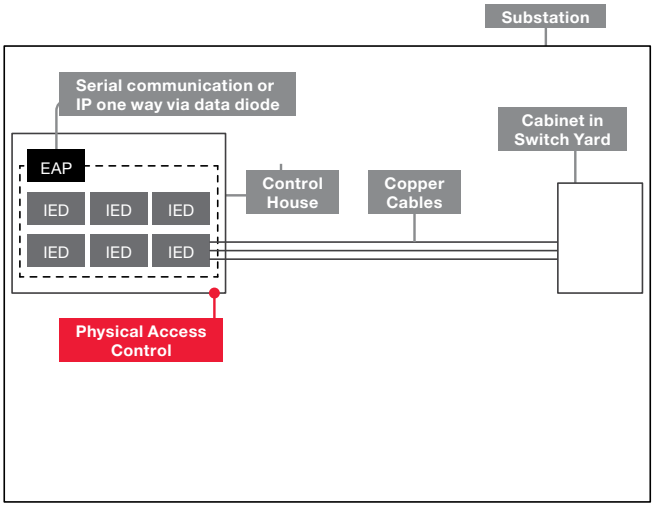
EXAMPLE 1

AIS Conventional substation (medium impact) with hardwired connections

The substation perimeter lies inside the outer box, at the chain link fence. Inside the substation switchyard are a number of kiosks where the copper control cables for the breaker open/close with feedback from the breaker. The current transformer (CT) and potential transformer (PT) inputs also return to the protection system.

Inside lies the control house with six walls, and the electronic security perimeter signified by the dotted line. The electronic access point (EAP) allows any routable communications or communications that break the electronic security perimeter to enter. This is either serial, non-routable, or communication with a data diode to allow only information outflow, with no inflow of internet protocol (IP) information.

This is, therefore, a medium impact station due to the voltage level and because it only has non-external routable connectivity. Because there is no two-way IP, it is possible to use copper wires, no protection is needed in the switchyard, and the system is contained. From a CIP perspective, the only thing required is to ensure that physical access into the control room is restricted, and that everything essential is contained by the ESP, inside the control house.



PSP (Physical Security Perimeter)

ESP (Electronic Security Perimeter)

EAP (Electronic Access Point)

BCA (BES Cyber Asset)
IED: Protection/control device
MU: Merging unit/process bus IO

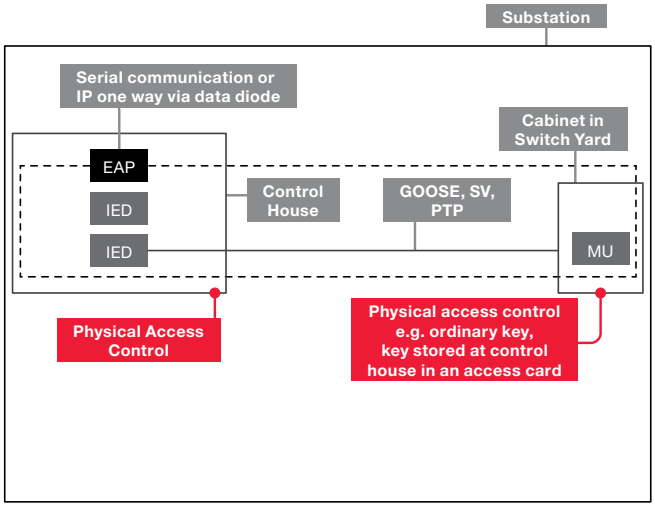
... Cyber Security Measures

EXAMPLE 2

AIS Digital substation (medium impact) – layer two traffic

For Layer Two traffic, the system includes hardwire connections between the current transformers and potential transformers in the switchyard and the control house. Layer Two traffic uses GOOSE, which is able to multitask with sample values, which are process bus calculations of the digital sensors connected to the relays. The merging unit is a device for converting the CT and PT outputs to the digital sample values in the switchyard. This process is still non-routable or one-way IP leaving the substation.

This scenario is still medium impact because it uses non-routable connectivity and the system needs the same physical controls on the control house, but it also needs a system to restrict physical access to the kiosk housing the merging unit. Ideally, anyone with permission to enter the control house and signed in should also be able to access the merging unit. From a NERC perspective, because the system is non-routable, it needs no further requirements for compliance.



PSP (Physical Security Perimeter)

ESP (Electronic Security Perimeter)

EAP (Electronic Access Point)

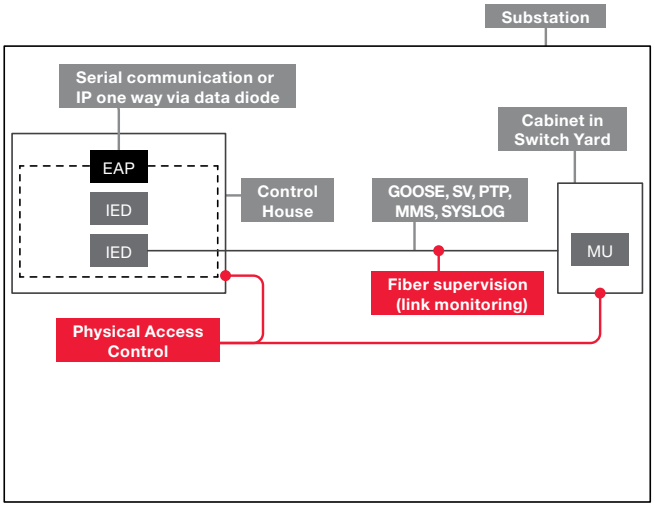
BCA (BES Cyber Asset)
IED: Protection/control device
MU: Merging unit/process bus IO

... Cyber Security Measures

EXAMPLE 3

AIS digital substation (medium impact) – layer three traffic

Layer Three traffic brings another layer of communication between the control house, protection system, and merging unit. Examples of this could include Manufacturing Method Specification (MMS) or IP SYSLOG information from devices. This layout can take advantage of the new approach contained within CIP Version 5, which allows the ESP to extend outside the control house as long as it is still within the substation. In other words, the perimeter now includes the merging unit located in the kiosk, so there is still no external routable connectivity outside, with only serial and one-way communication present. The only important protocol restricts physical access in the merging unit kiosk and control house. It is also easy to monitor the link supervision of the Ethernet fiber communication.



PSP (Physical Security Perimeter)

ESP (Electronic Security Perimeter)

EAP (Electronic Access Point)

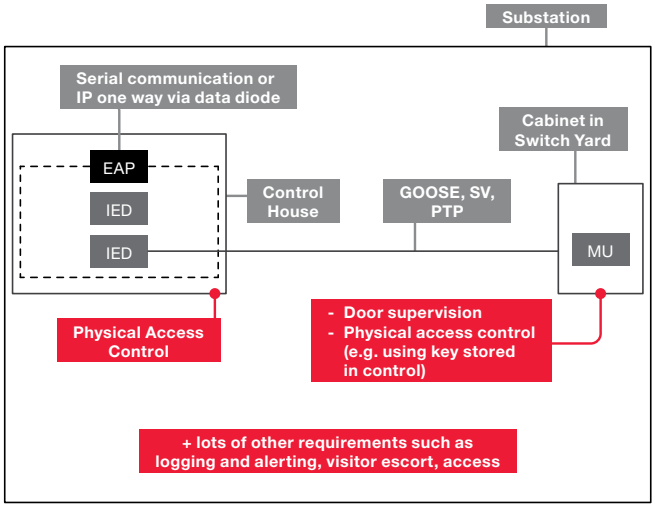
BCA (BES Cyber Asset)
IED: Protection/control device
MU: Merging unit/process bus IO

... Cyber Security Measures

EXAMPLE 4

Routable connectivity

Another example occurs if a utility installs routable connectivity. With Layer Two traffic, only GOOSE and sample values travel between the control house and the merging unit, but IP now travels outside the substation. The system will still need physical access restrictions on the merging unit kiosk and control house, but door supervision becomes necessary. The system needs to indicate when somebody accessed the BES fiber asset, making the system a medium impact categorization with external routable connectivity. This brings a range of additional NERC-CIP compliance requirements.



PSP (Physical Security Perimeter)

ESP (Electronic Security Perimeter)

EAP (Electronic Access Point)

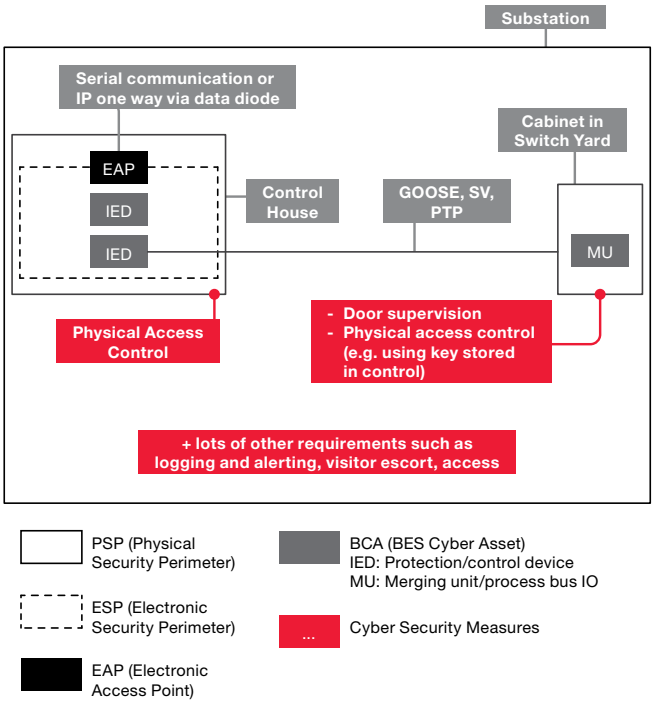
BCA (BES Cyber Asset)
IED: Protection/control device
MU: Merging unit/process bus IO

... Cyber Security Measures

EXAMPLE 5

Layer three traffic

With Layer Three traffic with routable protocols entering and exiting the control house, the system still has link supervision, door supervision, and access control so that the system is aware of anyone entering the merging unit kiosk. The CIP requirements for logging, alerting, and access control remain. The process bus solution now also needs to include the ESP outside the control house and fulfill the NERC-CIP requirements.



Advanced architecture

For advanced architecture, IEC 62443 begins to define the different layers and boundaries between the layers, which form the security zones, so the protection and control system for the process bus could be extended into the switchyard. For security, the utility needs to know which ports and services various devices use as part of NERC-CIP and disable those not needed by the system.

For any port used, the utility must document its use and note why it is being used. This makes it possible to locate and disable unused ports, protecting against the use of USBs or other portable devices. Although most utilities restrict USBs in sensitive areas, NERC-CIP also covers portable computers such as laptops.

Overall, the system includes an ESP, a firewall on the boundary of the ESP, and an intrusion detection system (IDS) located just inside the firewall. The firewalls protect the ESP and block any suspicious or unnecessary communication entering the substation. An intrusion prevention/detection system is equally crucial, ideally located just inside the firewall.

For NERC-CIP compliance, traffic blocked by the firewall does not need reporting. The IDS is the most important aspect, and any intrusion blocked by the IDS should be reported. Utilities need to protect any data exiting the substation and implement central account security logging and account management.

Enterprise programs and/or local programs inside the substation can monitor and manage user accounts and collect information from every device. An example of this could be a CIS log that feeds into the system and is added automatically to every security management system for that type of application. If someone tried to log into a device three times and failed, then it creates an entry on the CIS log, which the event management system reads and sends to the security management system. For the medium and low impact categories, there is single factor authentication throughout the substation. If a user enters via remote service, there needs to be a DMX (digital multiplex) for two-factor authentication to gain the credentials for entry, creating another layer.

Overall, this builds a defense strategy that is robust and flexible. For a substation, the protector relay connects to the breaker, so a good strategy makes this the most difficult aspect to access, because an external attacker able to close and open breakers could cause serious damage.

Finally, the system needs patches, which must be coordinated and managed across the entire system to deal with new threats as they emerge. Vulnerabilities are normal, and patch modifications are common, so the entire fleet needs updating with the right security patches. This forms part of the CIP compliant patch management process, which addresses a vulnerability or security issue.

Summary

The idea of standards is to oversee the entire digital transformation process and help utilities offer higher levels of availability. Using standards to shape the course of substation digitalization can help utilities shift towards proactive maintenance to reduce costs and help them understand the health of the system. With respect to security, it is important to ensure that this process proceeds incrementally, with a defense-in-depth approach that uses layers to deter intruders and report issues, maximizing effectiveness.

This involves moving the entire digital fleet forward and embracing standards to remove the perception that digitalization is not possible due to cybersecurity concerns. It is important to focus on why digitalization is needed and suggest what security requirements support the process. This should happen from the very beginning of the process and should be incorporated into modernization roadmaps and designs. Utilities should ingrain cybersecurity into the business culture as institutionalized policies and processes.

It is important to note that most of the fears around NERC-CIP are unfounded and the standards intend to bring reliable and safe power to consumers, leaving scope for the technical standards to guide modernization plans. Now, Version 5 ensures that CIP and the technical standards coexist much more closely, especially the changes to ESPs, allowing more substations to undergo digitalization safely. The various standards promote interoperability and let utilities build up a portfolio of solutions from multiple vendors to deliver a communications system with robust cybersecurity that suits their own infrastructure.

NERC-CIP is an important performance-based standard, not a technical standard, so there is no certification. However, going forward, the IEEE 3374 standard will include a conformity assessment program and information that provides NERC auditors with a technical blueprint to promote better levels of security within digital substations. In other words, IEEE and CIP are working together to create common goals and benefit the industry, although there are no NERC-CIP certified integrators or certified programs.

In conclusion, utility control centers will rely upon useful flows of information from substations, and serial communications cannot handle the volume of data needed to drive improved reliability. IEC 61850 is a platform that enables substation digitalization by giving technical guidance and supporting interoperability, allowing choice between vendors, solutions, and architecture. This reinforces the need for open standard based applications that will engage industry and help parties develop systems around cybersecurity. Open, consistent standards support training, and provide a common platform that allows utilities to share best practices.

Hitachi Energy is one of few companies that offer a complete suite of digital substation hardware and software. They help utilities develop communications systems that streamline operations and improve reliability without compromising on cybersecurity. Almost any substation can be transformed, usually without replacing primary equipment. Hitachi Energy can help utilities improve asset health, adopt proactive maintenance, streamline operations, reduce costs, and create safe systems.

To learn more about how Hitachi Energy can help utilities use standards to move toward a smarter, digital future, click here.

Hitachi Energy
marketing-update@hitachienergy.com
hitachienergy.com

9AKK107991A5495