



Cybersecurity in Power Generation

Applying and Interpreting ISA/IEC 62443 Standards

Cybersecurity in Power Generation

Applying and Interpreting ISA/IEC 62443 Standards

» Introduction: Why Another 62443 Guide?

This document aims to serve as a valuable resource for understanding and applying the ISA/IEC 62443 family of standards¹ to power generation. It can be viewed as an informative appendix to the 62443 standards, specifically tailored for the power generation sector. Professionals who apply this document in professional practice can expect not only to adhere to the 62443 standards family, but to also maximize the standards' benefits while simplifying their work.

The 62443 standards are widely recognized as essential guidance for enhancing cybersecurity for Operational Technology (OT) across various industries, including water management, power generation, railway systems, and manufacturing. The value is undeniable, and aspects such as creating a risk assessment to properly segment the OT network into zones is a must-have for any security program. Today, most OT network representations use the "layered cake" Purdue model, with different zones from zero (0) to four (4), which comes from the application of these standards.

Applying the 62443 standards to a particular industry or specific site, however, may not be straightforward. The standards apply horizontally across industries, providing no guidance for specific verticals. The variety of choices, from risk assessments to zoning requirements and controls, can be daunting. Our approach is to narrow these choices to those most suitable for power generation.

Recently, the lack of industry-specific application guidance in 62443 has prompted certain industries to create new specifications to enhance or reevaluate the standards based on their distinct needs. An example is the Technical Specification 50701 (CLC TS-50701) in Europe, which is evolving into the IEC 63452 standard. This specification enhances and modifies the 62443 standards from the rail sector's perspective, addressing the unique cybersecurity challenges posed by signaling systems, moving vehicles, and other elements specific to rail systems.

In response to this need, the Securing Energy Infrastructure Executive Task Force (SEI ETF) created a set of profiles for power generation aligned with IEC 62443 in 2022. Furthermore, Working Group 14 within IEC 62443 is actively developing a series of vertical-oriented profiles. However, these profiles have yet to be released, leaving a gap in specialized guidance.



¹The full name of the ISA/IEC 62443 family of standards is quite long to type and say. It is abbreviated as "62443" or "the standards" throughout this document.

We hope to address power generation industry-specific gaps in this document by:

- » **Clarifying the certification procedures**, because certification against the standards is complicated, misunderstood, and often ineffective while evaluating power generation networks.
- » **Proposing a Consequence-Driven Risk Assessment as the initial risk assessment**, because the risk assessment examples provided in the standards do not account for high-impact, low-probability scenarios that are unacceptable in power generation.
- » **Proposing a zoning and interconnected structure for power generation**, addressing the unique needs of safety-critical and equipment protection sub-networks.
- » **Proposing engineering-grade controls to reduce the burden on cybersecurity controls**, because only 62443's highest Security Level 4 (SL4) addresses national-state attacks, and classifying all networks as SL4 is extraordinarily expensive.

» Overview of IEC 62443 for Power Generation

Applying and Interpreting ISA/IEC 62443 Standards

The 62443 family of standards includes a broad range of documents divided into four main parts: General, Policies & Procedures, System, and Components. Each document is identified by a unique number in the format 62443-x-y, where 'x' indicates the part and 'y' the specific document. Currently, there are 10 publicly available documents. Of these, two are technical reports (TR), which provide guidelines and two are technical specifications (TS), which may lead to standards but have not been ratified by the committees.

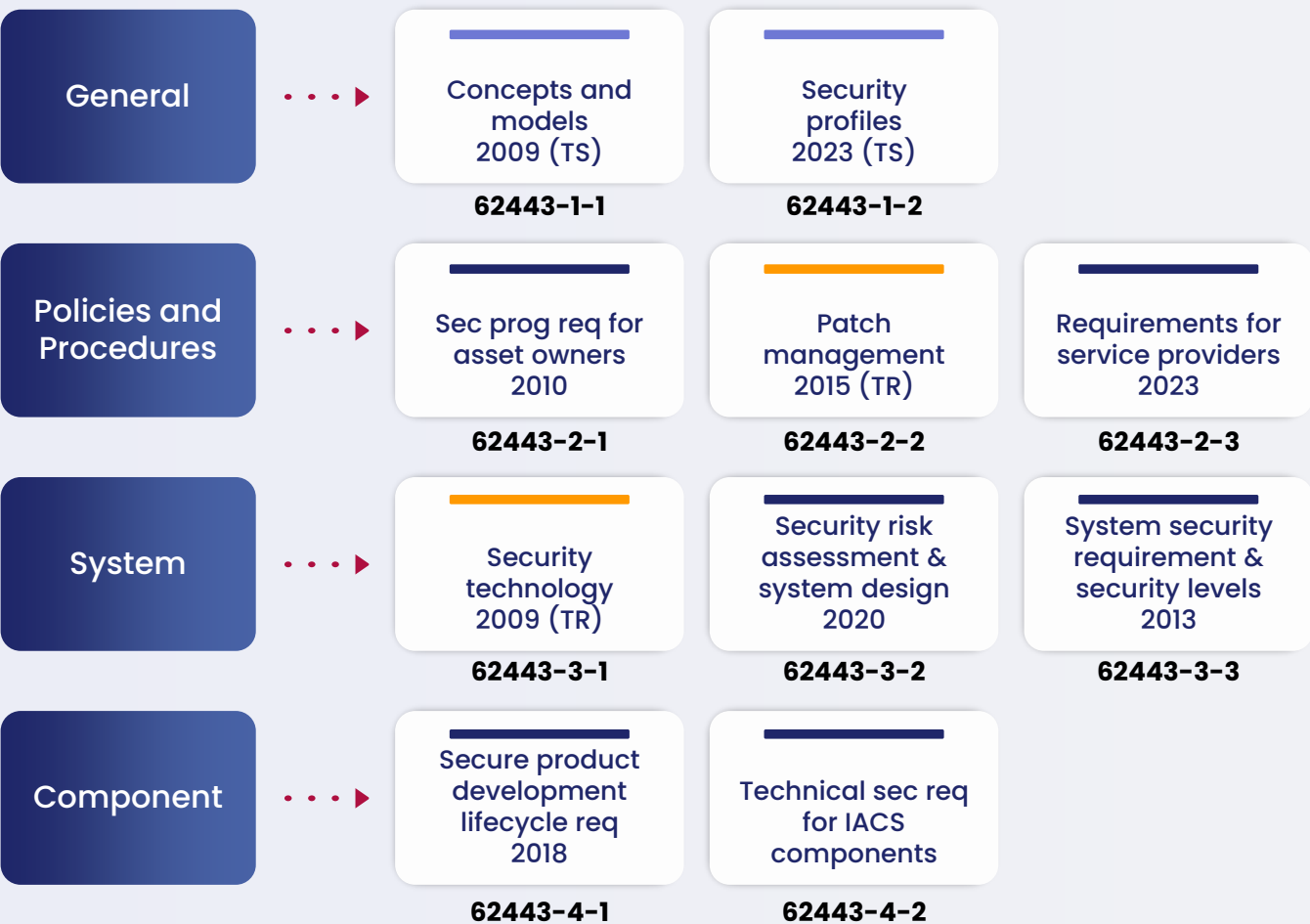


Figure 1 IEC 62443 Standards

Here is an explanation of each part, along with considerations for applying them to power generation:

General (62443 1-x):

This part lays the groundwork by defining terms and concepts. It recently added a document to create profiles for specific targets (as a technical specification) but none have been released.

Policies and Procedures (62443 2-x):

This part provides general guidance on procedures, such as patch management. However, it needs a fair bit of interpretation to apply effectively to networks and systems with safety and critical infrastructure reliability implications.

System (62443 3-x):

This part focuses on system-level cybersecurity evaluations. It revolves around conducting risk assessments and implementing controls to mitigate identified risks. It also introduces key concepts such as zones and conduits which are widely adopted in OT cyber security practice.

Components (62443 4-x):

This part focuses on certifications - evaluating the cybersecurity robustness of industrial control vendors and automation products. These standards assess the ability of these products to withstand cyberattacks.

Themes and terminology in 62443

There are recurrent themes across the standards:

Security Level (SL):

Measures a product's or system's protection against threats, defined in four levels (SL1 to SL4) with increasing protection requirements.

Foundational Requirements (FR):

Seven foundational cybersecurity requirements (e.g., identification and authentication control, use control, system integrity) form the basis for technical requirements, and each requirement can be evaluated by assigning it a SL.

Secure Development Lifecycle (SDL):

A process ensuring security is built into products from the start, addressing risks throughout the lifecycle.

Component:

An individual hardware or software product or subsystem within a larger industrial control system.

Zone:

A group of components within an industrial control system with similar security level (SL) requirements.

Conduit:

A communication pathway between zones, often demarcated and secured by firewalls or unidirectional gateways.

» Certification Against the Standards

Certification within the IEC 62443 framework is complex due to the standards' breadth. Certification is overseen by a testing organization independent of both the IEC and ISA, which licenses private entities to test and certify products on their behalf. A rated security level (SL) is assigned based on the outcome of the certification process. 62443 Certification covers three areas: the product development process, an actual product's resistance to attacks, and the security level of complete systems.

- » **Product Development or Secure Development Level Assessment (62443 4-1):** Vendors and other component and product developers must demonstrate maturity in their product development process with respect to security. This includes adhering to secure coding practices, performing regular security testing, and maintaining detailed documentation that shows compliance with SDLA 62443-4-1 standards. The goal is to ensure that the product is developed with a robust security foundation from the start
- » **Product Resistance Against Attackers (62443 4-2):** 62443 defines four security levels (SL1 to SL4). Achieving "resistance" against attackers involves following the evaluation process in 62443-4-2, which identifies seven foundational requirements for industrial automation products. Each requirement has specific system specifications that the product must meet to achieve a particular security level. The product must provide evidence that it meets every system specification for each foundational requirement at the desired security level.
- » **Products that are Systems (62443 3-x):** This certification applies when a product functions as a complete system, such as a vendor selling fully completed substations. Achieving a specific security level (SL) is detailed in 62443-3-3, while the process for determining the required security levels through a risk assessment is explained in 62443-3-2.

Important points:

- » A company can only certify their products if the company has already achieved a satisfactory SDLA certification (usually level 3), so a product provider needs to go through 4-1 certification before 4-2.
- » Achieving a certain security level under 4-2 for a cybersecurity product does not guarantee the cybersecurity capabilities of the entire system the product is part of; rather, it indicates that the product can withstand attacks directed at itself.
- » When certifying a complete system, the application of security levels often creates confusion among practitioners. The foundational requirements in 62443-3-3 mirror those in 62443-4-2 but are applied at the system level rather than at the component level for each zone in the system.

For evaluating the performance of cybersecurity tools, start with Common Criteria certification that assesses the intended functional requirements of security products, then focus on 62443-4-1 and 62443-4-2 to ensure the products do not contain glaring cybersecurity functionality omissions, and to prevent supply chain attacks.



» Implementing 62443 in Power Generation Systems

Are the Standards Suitable for Power Generation?

The IEC 62443 standards can significantly enhance the cybersecurity of power generation facilities, provided certain issues are understood:

- » **Horizontal Focus:** The standards are horizontal, meaning they are designed to apply across various industries. Therefore, careful interpretation is required when applying the proposed network models, threat assessments, and cybersecurity controls to the specific needs of power generation.
- » **Choice Creep and Complexity:** The flexibility within the standards can add difficulty, particularly at the beginning of the evaluation. Making practical choices can significantly increase the impact of cybersecurity measures while simplifying implementation.
- » **Aging Documents:** Some documents in the standard are over ten years old and may need to be interpreted or augmented to reflect today's technology and threat environments. For example, threats and consequences have changed dramatically since 62443-3-2 was published in 2020, with a tenfold annual increase in attacks with physical consequences compared to the previous decade.

As a result, the best way to apply 62443 to power generation is to create a modern engineering-driven assessment, accounting for the priorities in the sector, while being as consistent with 62443 as possible.

An Engineering Driven Cybersecurity Assessment for Power Generation

An engineering-focused cybersecurity program is built on a maturity model that prioritizes synchronization with engineering teams at every stage. This ensures that cybersecurity considerations are integrated into the engineering process from the outset, rather than being treated as an afterthought. The maturity model should include milestones and evaluation criteria that reflect the level of collaboration and integration between cybersecurity and engineering functions.

The following figure outlines a suggested process for integrating IEC 62443 standards into a standardized cybersecurity assessment for power generation:

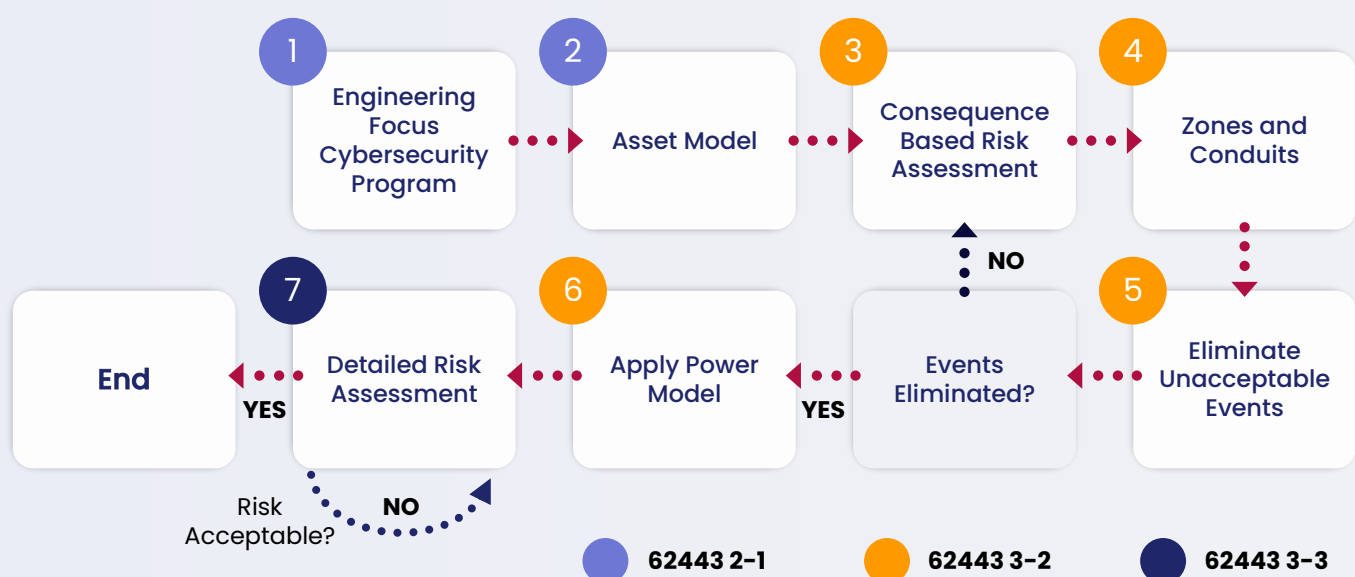


Figure 2 Steps in the Engineering-Driven Cybersecurity Assessment Process

1. **Create a Cybersecurity Program:** Establish an engineering-focused cybersecurity program that emphasizes collaboration with engineering teams throughout the lifecycle. The new Cyber-Informed Engineering (CIE)² perspective provides engineering focus to the cybersecurity program, tying the program closely to the engineering discipline and engineering approaches to risk management.
2. **Develop an Asset Model:** Create a detailed asset model of the power plant as an architectural reference, identifying critical components, their functions, and interdependencies with the help of the engineering team.
3. **Consequence-Based Risk Assessment:** Start by identifying unacceptable consequences related to safety and reliability. Then create a consequence-based risk assessment to determine priorities.
4. **Zones and Conduits:** Develop zoning strategies tailored to power generation, considering the unique characteristics of the plant. Define communication conduits between zones based on a connectivity matrix.
5. **Eliminate Unacceptable Events:** Prioritize the elimination of unacceptable events (Consequences/Attack vectors) identified in the risk assessment, then implementing engineering controls and/or security measures to achieve this. Iterate going back to step three (3) until either all unacceptable consequences are eliminated, or their impacts become reduced to an acceptable level and not requiring further mitigation.
6. **Apply Power Models:** Incorporate power-specific models and standards (e.g., NERC CIP) to further refine the cybersecurity assessment and ensure compliance with industry regulations. Evaluate if these power models reduce the risk to acceptable levels. If not, continue with a detailed risk assessment.
7. **Detailed Risk Assessment:** Conduct a more detailed risk assessment, taking into account the specific vulnerabilities and threats identified in previous steps. Implement additional security controls as needed to mitigate any remaining risks.

» Power Generation System Overview

Segregation of IT and OT

The main goal of cybersecurity in a power plant is to protect the plant's essential functions from cyber-sabotage attacks. These essential functions are automated by the plant's safety, protection and control (P&C) networks and must be preserved in the event of a cyberattack. Note that in modern cybersecurity parlance, a power plant's P&C network is considered to be an industry-specific form of Operational Technology (OT) network. The 62443 standards apply to the OT zone, while other IT standards can apply to both the business network and the OT network, as there may be IT elements in the OT network. However, we should first apply the 62443 standards and the zoning process before applying IT standards in OT networks, such as ISO 27001. If possible, we should integrate into 62443 any power generation specific guidance to enhance the evaluation.

The IT/OT interface (communications between IT and OT) and any OT dependencies on IT servers or services need to be closely evaluated. The impact of a cyberattack on the business network should not affect the essential functions of the OT networks. In practice, this means that the OT zones should contain any necessary functionality (e.g., active directory, time synchronization) needed to operate independently of IT networks, and inbound traffic from the IT network to the OT network must be minimized.

² <https://inl.gov/national-security/cie/>

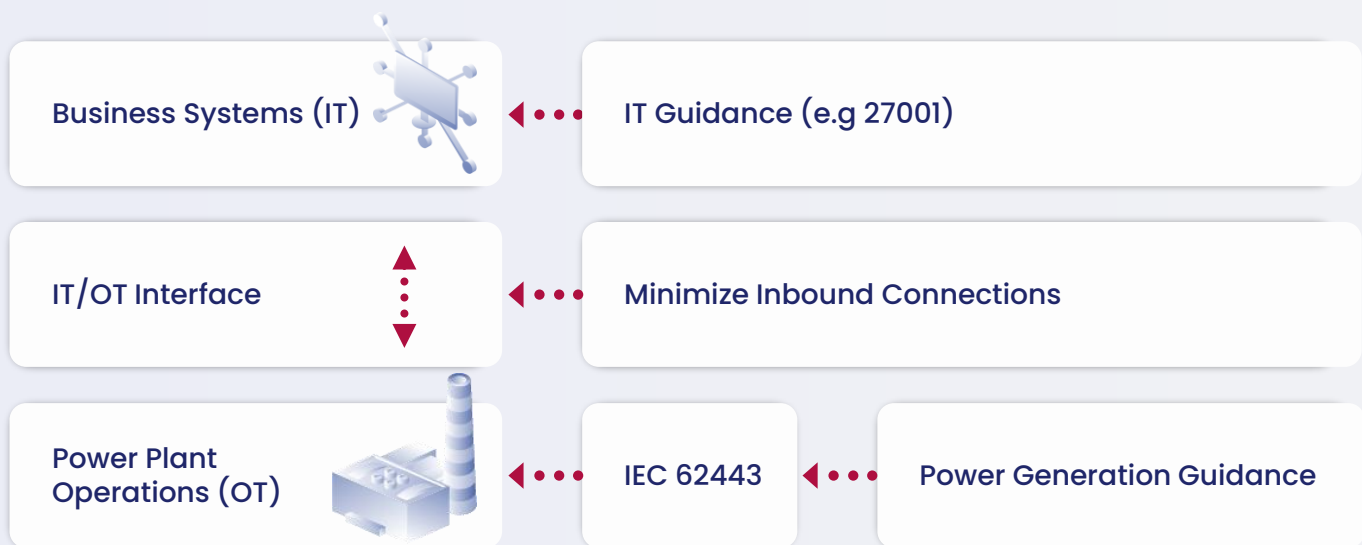


Figure 3 IT/OT Segmentation

Power Plant Architecture Modelling

A power plant model should be created as the first step before applying the standards. This model should include the subsystems of the plant, ideally displaying their physical location, criticality, ownership, and connectivity. This information will be utilized later to perform the risk assessment. Various methods can be used to provide this information, such as starting with the location of the assets and using color coding or other visual cues to indicate their criticality, ownership, and connectivity.

Common subsystems include:

Shared Plant Infrastructure: such as Historians, Active Directory servers, anti-malware (anti-virus) servers, remote access solutions, building automation systems, environmental control systems and other systems and servers that provide services to the entire OT network, and are shared across all generating units.

Operational: Houses the main operational systems of the plant, generally duplicated one set of systems per generating unit, including operator HMI workstations and automation for (where applicable) fuel handling, furnaces, boilers, turbines, generators and sometimes per-unit substations converting generating voltages to grid voltages.

Safety Subsystems: Ensure the plant operates safely and include protective relays, fire suppression systems, and emergency shutdown systems.

Cloud: Enables remote monitoring, data analysis, remote file storage, and integration with advanced technologies such as AI and machine learning.

Business: Manages administrative and business functions, including Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), and financial systems.

IoT, Fire & Security Alarm, and Public Announcement: These systems are isolated from the plant operational subsystems and may include cameras, fire suppression, speaker systems, and other sensor systems that do not interact with the main operational systems.

Different systems within the power plant should be assigned criticality levels to prioritize their security and operational importance.

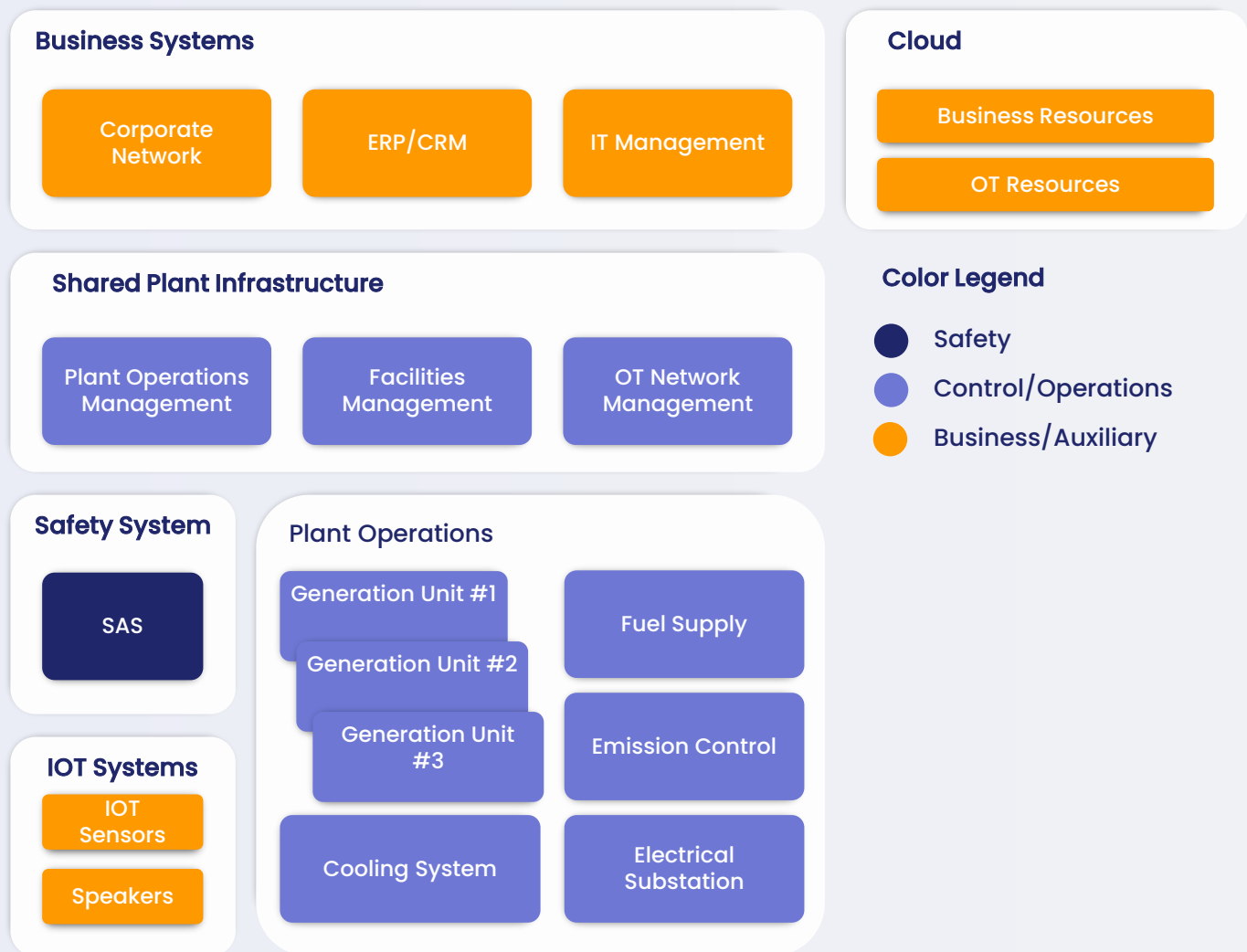


Figure 4 Power Plant Asset Model

» Consequence Based Risk Assessment

Risk Assessments in 62443

By design, 62443 describes a process for conducting risk assessments and leaves the selection of specific risk assessment methodologies or criteria to the practitioner. Large power plants are inevitably critical industrial infrastructure and hence critical to national security. As a result, they must always be considered credible targets of nation-state attacks. The risk assessment criteria we use for power generation must therefore focus on, to the greatest extent practical, eliminating unacceptable consequences of nation-state attacks. We focus on likelihood only secondarily, for only acceptable consequences.

This may seem unusual to practitioners accustomed to using risk matrices. Therefore, let's explore why risk matrices should not be used for an initial risk assessment, and what should be used instead.

Often, risk assessments use a matrix where risk is determined by the product of the severity of potential consequences and the likelihood of an event. This approach is common for assessing health and safety risk and has now made its way into cyber security practice. This is partly because of examples such as the one provided in IEC 62443-3-2, which includes a risk matrix.

The problem with this approach is that, while safety incidents due to human error and equipment failures are correctly modeled as independent random events, the same is not true for cyber attacks. If a specific attack against a specific target brings about an unacceptable consequence, then most often, exactly the same attack against exactly the same target will bring about exactly the same consequences. In safety engineering terminology, cyber attacks are more accurately modeled design flaws, not independent random events that can be modelled statistically with “likelihood.”

				Focus of a Consequence Based Risk Assessment		
Likelihood (treat occurs and result in adverse impact)	Very high	Very Low	Low	Mode rate	high	Very high
	high	Very Low	Low	Mode rate	high	Very high
	Mode rate	Very Low	Low	Mode rate	Mode rate	high
	Low	Very Low	Low	Low	Low	Mode rate
	Very Low	Very Low	Very Low	Very Low	Low	Low
		Very Low	Low	Mode rate	high	Very high
Level of Impact						

When assessing risk, the only reliably quantifiable aspect is the consequence of a successful attack under different scenarios. Thus, for power generation, it makes sense to start with a scenario-based, consequence-driven evaluation of unacceptable outcomes. After doing so, remaining scenarios with tolerable outcomes (such as purely business or financial consequences) can be considered by factoring in likelihood.

Consequence-Driven Risk Assessments

For power generation we evaluate risk in a consequence-driven way, guided by engineering knowledge. This reflects modern approaches to managing unacceptable consequences, for example:

» **Cyber-Informed Engineering (CIE)**³

Developed by the U.S. Department of Energy, CIE integrates cybersecurity considerations into the engineering lifecycle of industrial control systems from an engineering perspective. It uses both engineering controls and cybersecurity controls – making small changes to the design of systems to eliminate risk, and using cybersecurity to mitigate residual risks.

» **Consequence-driven Cyber-informed Engineering (CCE)**

Developed by Idaho National Laboratories, CCE builds upon CIE by emphasizing a consequence driven approach. It systematically analyzes potential consequences and develops security controls to mitigate them.

» **Network Engineering and Cyber Design Basis Threat (cDBT)**⁴

Network engineering is focused on small design changes to automation networks to eliminate or dramatically reduce the risk of cyber-sabotage attacks pivoting across criticality boundaries. Cyber design basis threat is a way to communicate acceptable residual risk to project teams – drawing a line between attacks and attack vectors that are reliably defeated, and those that are not.

» **Security Process Hazard Analysis Review (SPR)**⁵

SPR extends traditional process hazard analysis (PHA) to include cybersecurity considerations. It looks for opportunities to dramatically reduce cyber risk through the use of electro-mechanical and procedural mitigations, rather than only “hackable” cyber mitigations.

Complexity/Focus	System-Specific	Framework-Based
Streamlined	SPR	cDBT
Comprehensive	CCE	CIE

Focus:

Ranges from “System-Specific” (narrowly tailored to a particular system’s assets and processes) to “Framework-Based” (offering a broader, more generalizable approach).

Complexity:

Ranges from “Streamlined” (emphasizing ease of use and rapid assessment) to “Comprehensive” (providing a more in-depth analysis with greater detail).

These consequence-driven approaches provide a structured framework for identifying and mitigating the most significant cybersecurity risks in power generation systems. By prioritizing the protection of critical functions and assets, these methods help ensure the resilience of essential infrastructure against cyber threats.

³ <https://inl.gov/national-security/cie/>

⁴ <https://waterfall-security.com/engineering-grade-ot-security>

⁵ <https://www.isa.org/products/security-pha-review-for-consequence-based-cybe-1>

Cyber Design Basis Threat Example

Cyber Design Basis Threat (cDBT) is a powerful tool for addressing unacceptable cybersecurity events in high-stakes environments like power generation. cDBT focuses on identifying threats that must be reliably defeated to avoid severe consequences for critical infrastructure.

cDBT is closely related to the concept of Design Basis Threat (DBT) that is used in counter-terrorism, which defines the characteristics of potential threats that a site's physical security measures must be designed to reliably address. Similarly, cDBT focuses on identifying and reliably mitigating cyber threats that could have severe consequences for critical infrastructure.

The cDBT process begins with defining "directives" -- unacceptable events and associated attack vectors. Then we evaluate which attack vectors are applicable and credible. Finally, we express security priorities in terms of consequences and types of attacks that must be defeated reliably by our engineering and cybersecurity designs.

Examples of cDBT Directives:

- » No cyberattack operating exclusively across the internet, without insider assistance, should cause a material operational disruption.
- » Logs must be maintained to ensure insiders committing sabotage can be identified and prosecuted.
- » Safety-critical items' functionality must be protected from manipulation by both adversaries over the internet and unauthorized insiders.
- » No wirelessly connected IoT devices shall become an attack vector for the power plant.

Unacceptable Cybersecurity Event	Attack Vector (Outside Zone)	Attack Vector (Inside Zone)	Attack Vector (Supply Chain)	Suggested Approach
Remote operational disruption from the internet	Not Acceptable	Not Applicable	Not Applicable	Physically restrict traffic from the internet and IT network with unidirectional technology
Erasure of critical logs	Not Acceptable	Not Acceptable	Not Credible	Implementing physically non-writable logs in reliability critical and safety critical zones
Unauthorized manipulation to damage turbines	Not Acceptable	Not Acceptable	Not Acceptable	Protect networks of protective relays unidirectionally, to prevent manipulation of relay settings
Counterfeit components create a cyber incident	Not Applicable	Not Applicable	Not Acceptable	Supply chain security: Perform rigorous vendor vetting and component inspection
IoT devices used to attack the plant	Not Acceptable	Not Acceptable	Not Acceptable	Create a specific zone for IoT devices, and forbid data exchange with other zones except to the cloud





Example cDBT Matrix

Attack Vector Classifications:

- » Not Acceptable: The consequence is unacceptable, and mitigation is insufficient. Prevention is the primary goal.
- » Not Applicable: The attack vector is irrelevant to the specific consequence.
- » Not Credible: While the attack vector is possible, it is not reasonable for an adversary to invest enough effort to bring about the consequence reliably, e.g., because of existing controls or inherent limitations, such as an insider modifying systems in front of peers.

The action items from this cDBT exercise directly inform the implementation of zoning (e.g., reliability, safety, IoT), conduit selection (e.g., firewalls, unidirectional gateways), and engineering controls (e.g., overpressure valves). cDBT also facilitates discussions with management about necessary cybersecurity focus areas, helping prioritize resources and investments.

After addressing the most critical risks with cDBT, organizations can leverage more complex consequence-driven evaluations, such as CCE, to quantitatively assess the potential impacts of tolerable events and further refine mitigation strategies. This iterative approach ensures that the most critical risks are addressed first, while also allowing for a comprehensive evaluation of the overall risk landscape.

	Security Level	Description
	SL1	Protects against casual or coincidental violation of cybersecurity policies. Eg: errors & omissions
	SL2	Protects against intentional violation using simple means with low resources, generic skills, and low motivation. Eg: disgruntled insiders, "script kiddies", curious teenagers
	SL3	Protects against intentional violation using sophisticated means with moderate resources, IACS-specific knowledge, and moderate motivation. Eg: politically-motivated hackers
	SL4	Protects against intentional violation using sophisticated means with extended resources, IACS-specific knowledge, and high motivation. Eg: ransomware criminals & nation-states

» Zones and Conduits in Power Generation

Establishing a Modified Zoning Strategy

One of the most widely-utilized aspects of the 62443 standards is the creation of zones and conduits. This zoning strategy must be tailored to the asset model and risk assessment.

The first step is to create a zoning strategy for the power plant. 62443 defines Security Levels zero (SL0) through four (SL4) based on adversarial capability. Various 62443 drafting committees are debating this definition of security levels, because the current definition does not take consequence or criticality into account. Power plants should adopt a zoning strategy based on criticality, not on adversary capability levels. For example, "Safety-related assets shall be grouped in dedicated zones. If non-safety assets are in such a zone, those assets must be secured as if they were safety-critical." A good system to standardize zones based on criticality is proposed in TS-50701, which creates different zone criticality levels and assigns them numbers zero (ZC-0) through five (ZC-5).

The following criticality matrix utilizes a similar zoning strategy as TS-50701 but is specially adapted for power generation. It assigns criticality 5 to any zones that may incur equipment damage and 5s to zones that are safety-related, such as Safety Automation Systems (SAS).

Zone criticality (ZC)	Zone Criticality	Example
ZC-5s	Safety Zone	Automatic Shutdown, SAS
ZC-5	Reliability Critical/Damage	Protective Relays
ZC-4	Reliability Critical	DCS, Substation SCADA System, Historians, Automation
ZC-3	Business Critical	Internal Network, Office and Business Network
ZC-2	Business	Gateway Area
ZC-1	External Business	External Companies, Cloud
ZC-0	None	Internet

Other strategies that may be considered when applying network engineering and cDBT concepts include separating systems into zones based on physical location, legacy systems, temporarily connected devices such as roaming devices, and wireless systems.

Simplifying Countermeasures for Zones and Conduits

Conduits are the communication pathways between zones in the power plant network. They control and monitor data flow, prevent unauthorized access, and prevent data breaches. Specific assets in zones may provide some additional security capabilities, and when assets cannot be secured as needed, for example because engineering change-control imperatives prevent prompt patching, security controls in conduits provide important “compensating measures” – preventing cyber attacks from reaching vulnerable targets, especially at security level / criticality boundaries.

The best approach to choosing the right countermeasures between zones is to simplify by being practical: in practice, nearly all critical and credible threats originate in lower-level criticality zones and reach higher criticality zones over modern ethernet (internet/IP) conduits. Also, nearly all modern cyber-security countermeasures deployed between zones are either unidirectional technology or firewalls.

- » **Firewalls:** Software-based solutions that filter, monitor and route network traffic based on predefined rules. They are versatile and suitable for bidirectional communication between zones with similar criticality. Some possess advanced “next-gen” features like deep packet inspection or intrusion detection and response. Despite having the appearance of hardware elements, all firewall functionalities are provided by software.
- » **Unidirectional technology:** Combine a hardware element that can physically send information only one way, and a software element that replicates data and data sources via the unidirectional hardware. Unidirectional technology features at least one unidirectional gateway element and may also incorporate additional features such as another unidirectional gateway in the reverse direction, a reversible feature, or a temporary bypass.

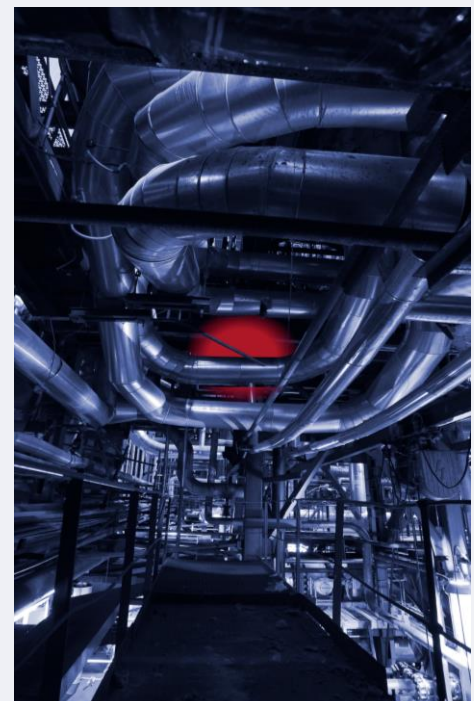
When choosing between unidirectional technologies or firewall countermeasures between connected zones, consider the following two questions:

1. **Zone Criticality:** Do the connected zones differ significantly in criticality level? (e.g., safety ZC-5 vs. business ZC-3)
2. **Information Flow:** Is the information flow primarily asymmetric between zones?

If the answer to both questions is yes, then unidirectional technologies are often a better choice than firewalls, as the hardware is immune to software vulnerabilities that could be exploited by attackers. If not, firewalls may be a better option, but the type of firewall should be carefully evaluated, especially between zones of different criticality. Prudent network designs deploy unidirectional protections at criticality boundaries.

Next, a connectivity matrix is created that documents the standard countermeasure choice for each combination of zone criticality level and considering information-flow requirements. This matrix can be organized purely by zone criticality or by more granular categories. Don't forget to ensure that any deviations from the connectivity matrix are thoroughly documented and their impact on the zone's risk profile carefully evaluated.

This table provides an example of a connectivity matrix for a typical power generation plant.



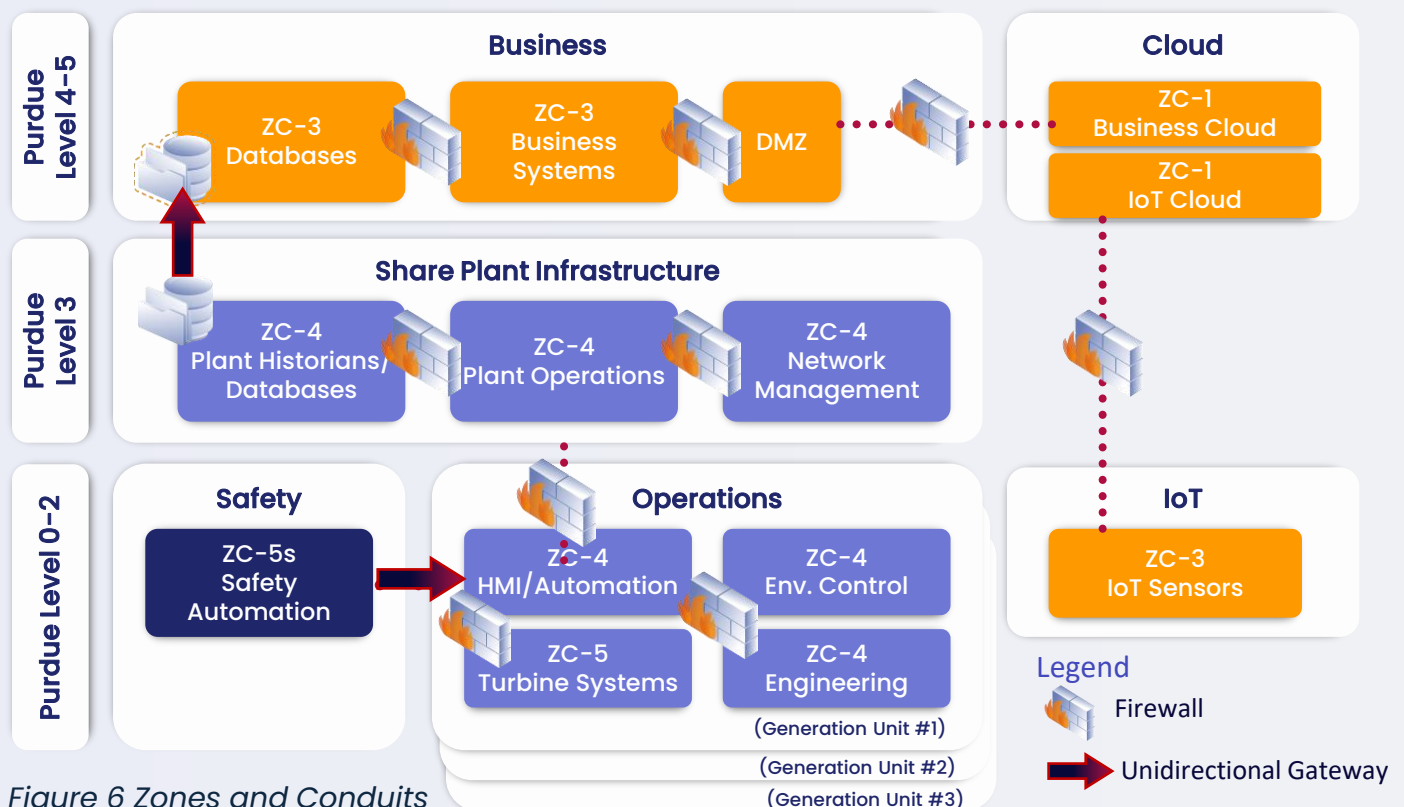
From/ To	ZC-5s (Safety)	ZC-5 (Reliability Critical/ Damage)	ZC-4 (Reliability Critical)	ZC-3 (Business Critical)	ZC-2 (Business)	ZC-1 (External Business)	ZC-0 (Untrusted)
ZC-5s	FW	UGW	UGW	UGW	UGW	UGW	NO
ZC-5	NO	FW	FW	UGW	UGW	UGW	NO
ZC-4	NO	FW	FW	UGW	UGW	UGW	NO
ZC-3	NO	NO	UGW*	FW	FW	FW	NO
ZC-2	NO	NO	NO	FW	FW	FW	NO
ZC-1	NO	NO	NO	NO	FW	FW	FW
ZC-0	NO	NO	NO	NO	FW	FW	N/A

Connectivity Matrix Legend:

- » **FW:** Zones with nearly the same criticality send or receive data utilizing Firewalls. Note that firewalls are bidirectional, so the send/receive is reciprocal.
- » **UGW:** Zones of different criticality are connected whenever possible with Unidirectional Gateways. Note that Unidirectional Gateways may be used to send but not receive. For example, in this matrix sending data from ZC-3 to ZC-4 (noted with an asterisk) is allowed utilizing a reversible Unidirectional Gateway (e.g., Waterfall FLIP).
- » **NO:** Transmission is completely prohibited in this zoning pair-combination
- » **N/A:** countermeasures do not apply to untrusted networks

Example: Zoning and Conduits in a Power Generation Plant

The diagram illustrates a strategy for a power management plant, aligning with the IEC 62443 standard and applying the principles of Cyber Design Basis Threat (cDBT). The conduits shown are derived from the plant's asset model to identify the subsystems shown. A connectivity matrix was created to select appropriate countermeasures. The model identifies four subsystems, each containing zones of different criticality.



To fulfill the cDBT requirements and adhere to the connectivity matrix, unidirectional gateways (UGWs) are strategically positioned at critical boundaries. Specifically, a UGW is placed between the ZC-4 (Reliability Critical) and ZC-3 (Business Critical) zones, creating a secure IT/OT interface. The UGW acts as an impenetrable physical barrier by preventing any internet-initiated attack from directly impacting operational systems. Necessary protocols and databases required by the business subsystem are replicated in real-time through the UGW, ensuring data availability without compromising security.

Another UGW is implemented as a conduit between the safety/protection systems (ZC-5s) and the HMI/automation systems (ZC-4). This crucial separation ensures that an attack or malfunction originating in any other zone cannot directly compromise the safety or protection systems, safeguarding critical safety and equipment protection functions.

Within the operational subsystem, the environmental control and engineering zones (ZC-4) are created on separate networks. While they share the same criticality level, their segregation enhances security by limiting attack propagation, such as by ICS insiders. A firewall (FW) serves as a conduit between these zones and the HMI/automation zone (ZC-5), facilitating controlled communication and data exchange.

Additionally, the shared plant infrastructure zone (ZC-4) connects with the plant operations zone (ZC-4) through an OT firewall, as they share the same criticality level. This firewall enables secure bidirectional communication for essential operational data and commands while maintaining network segmentation and impairing at least somewhat the propagation of attacks, should any of the connected networks/zones be compromised. The shared plant infrastructure also communicates with the plant operations and network management zones (ZC-4) using firewalls.

The IoT sensor subsystem is not connected to the main plant network, and the sensors cannot modify operations. The data is sent directly to the cloud, and the cybersecurity of this subsystem is managed as an IT system, with a focus on confidentiality.



» Applying Cybersecurity Controls

Engineering-Grade Controls, Hardware Controls, and Software Controls

In power generation, achieving high confidence in mitigating unacceptable consequences requires a multi-layered approach to cybersecurity. Priority is given to controls that reliably defeat attacks and prevent consequences, especially controls not easily subverted by attackers. Controls such as these are so-called "engineering-grade" controls, to differentiate them from less reliable, and often IT-centric, controls.

Engineering-grade controls are the cornerstone of reliable cybersecurity in power generation. They rely on immutable hardware or physical principles to enforce security policies, making them highly resistant to subversion, regardless of their certified or designated Security Level.

Physical Controls: The Absolute Zero Trust

- » Rely solely on physics for cybersecurity control. They may use software for operation but not for enforcing security policies.

Examples:

- » **Unidirectional Gateways:** Ensure one-way data flow, physically preventing reverse data transmission even if software is compromised.
- » **Physical Relays:** Isolate critical systems and prevent unauthorized commands from reaching them.
- » **Non-Writable Media:** Protect data integrity by preventing unauthorized modifications or deletions, such as of critical device firmware.
- » **Write-Once Media:** Protect data integrity, for example of security logs, preventing unauthorized modifications or deletions
- » **Over pressure relief valves:** Automatically release pressure when it exceeds safe levels, preventing system damage or failure. These valves operate purely on mechanical engineering principles, ensuring they function regardless of software or control system status.
- » **Manual Operations:** Practiced ability for personnel to operate critical physical functions manually during emergency conditions, such as during clean-up of a cyber attack.



Hardware Controls: Strengthening the Defense

- » Incorporate cyber hardware components to enhance cybersecurity, with the security function relying on hardware, making it more difficult for attackers to bypass.

Examples:

- » **Trusted Platform Modules (TPMs):** Securely store cryptographic keys and perform platform integrity checks.
- » **Security Tokens:** Provide hardware-based authentication and authorization.
- » **Secure Boot:** Ensures that only authorized firmware and software can be loaded onto a device.



Software Controls: An Essential Layer, But Not Foolproof

- » Essential for a defense-in-depth strategy but more vulnerable due to potential software flaws.

Examples:

- » **Firewalls:** Monitor and control network traffic based on predefined rules, though software-based and breachable.
- » **Intrusion Detection Systems (IDS):** Monitor network traffic and system activities for suspicious patterns, relying on software algorithms.
- » **Antivirus Software:** Detects and removes malware but needs regular updates and reliable evidence collection.



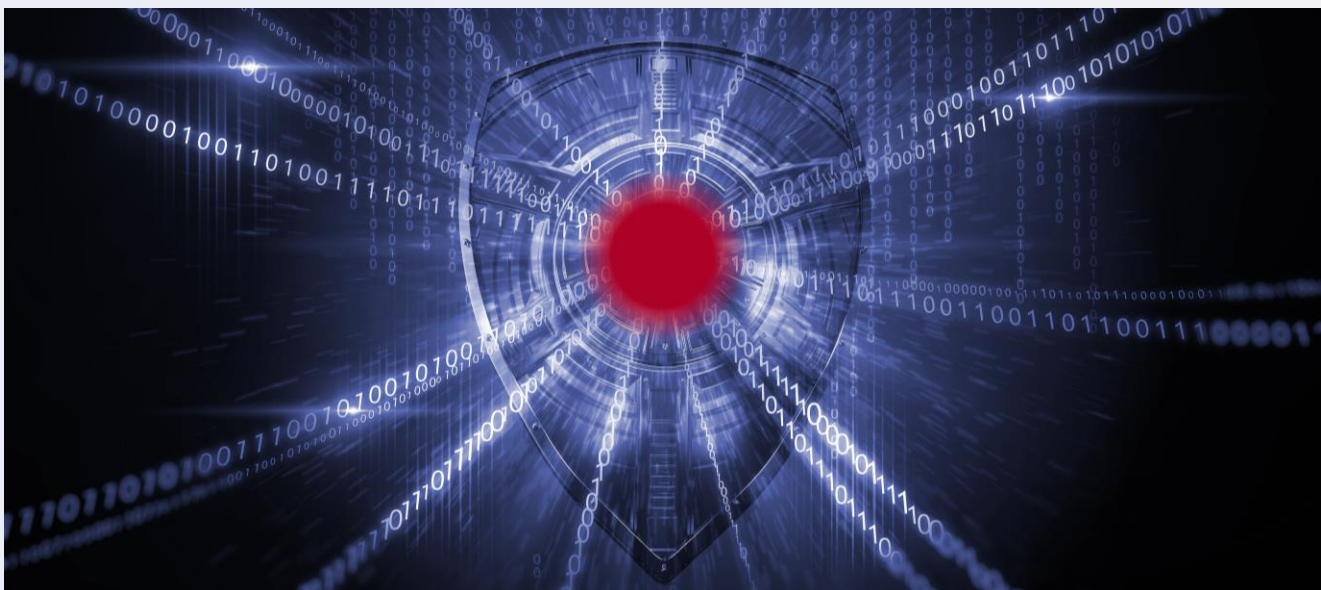
Applying Power Generation Models

After addressing unacceptable consequences with engineering controls, the next step is to mitigate remaining risks using current power generation models. Consider IEC 62443 3-3 controls: while they are not specific to power generation and may be outdated, most are still relevant. Augment these controls with other power-generation-specific best practices, such as:

- » **Internal Best Practices:** Many companies have their own models to address cyberattack risks in power generation.
- » **NERC-CIP:** The North American Electric Reliability Corporation Critical Infrastructure Protection standards are mandatory for infrastructure essential to the stability of the Bulk Electric System (BES) in North America. Note that NERC CIP is focused by law on the reliability of the North American BES, and unlike IEC 62443, cannot say anything about safety systems, or power generation business requirements other than BES reliability
- » **Energy Network Codes of Cybersecurity:** The European Commission has adopted the first EU network code on cybersecurity for the electricity sector, aiming to improve the cyber resilience of critical energy infrastructure and services. This code establishes a process for recurrent cybersecurity risk assessments in the electricity sector. It aligns with existing EU legislation, such as the revised Network and Information Security Directive (NIS2) and includes mechanisms for reporting cyberattacks and coordinating responses to large-scale events. The code seeks to promote a common cybersecurity baseline while respecting existing practices and investment. Like NERC CIP, the code is focused on the reliability of critical industrial infrastructure that is essential to the nation or the union, not on worker safety, public safety, or power generation business requirements not related to reliability.

Detailed Risk Assessment

For all zones and conduits that carry unmitigated risk, or that cannot be easily evaluated utilizing an existing cybersecurity model for power generation, we conduct a detailed risk assessment (DRA). DRA involves a detailed time-consuming examination of each zone and conduit identified in the initial risk assessment and whose risk still is not satisfactorily mitigated. The goal is to gain a deeper understanding of the specific assets, threats, and vulnerabilities within each zone and conduit, enabling us to fine-tune security measures. This process is described in 62443 3-2 and uses the Foundational requirements existing in 62443 3-3, but simplified as many unacceptable consequences will have been ruled out, and power models will have been applied.



» New Cybersecurity Paradigms and 62443

The Industrial Cloud

Cloud technologies have challenged the layered Purdue model, requiring a more flexible approach to connectivity and data flow. By implementing connectivity matrices, zones at different levels of the Purdue Model can be securely connected, standardizing the flow of data between these zones. This method allows for the safe integration of cloud services without compromising the security of critical OT systems and being consistent with 62443 requirements.

We can differentiate two types of cloud communications: **open loops** and **closed loops**.

Open loops, which involve sending information to the cloud without requiring a return flow, are generally safer and easier to implement when breaking the Purdue Model, by utilizing at least a Unidirectional Gateway to push OT information out to cloud systems.

Closed loops, which involve sending information back from the cloud to the OT systems, are less common and more challenging but can be managed with careful design using unidirectional architectures⁶. This hybrid approach leverages the strengths of both the Purdue Model and modern cloud technologies, ensuring a secure and efficient industrial operation.

Remote Connectivity: Zero Trust and Hardware Enforced Remote Access

While remote access is less common in power generation, it may be necessary for accessing certain systems. A recent multi-national report⁷ highlights two modern approaches to remote access: Zero Trust and Hardware-Enforced Remote Connectivity.

Zero Trust operates under the assumption that essentially all networks are compromised, requiring strict encryption, authentication and access authorization for every endpoint. In practice, zero trust cybersecurity products validate authentication evidence at the endpoint such as the user, location or intent. Zero Trust is the natural solution for internet-based remote access, but poses challenges when used deeper into OT network architectures, challenges such as creating authentication entities, evaluating endpoint integrity, and managing non-homogeneous systems like PLCs and HMIs.

Hardware-Enforced Remote Connectivity adds a layer of hardware protection to remote access security, addressing vulnerabilities in software-based security solutions. Hardware-enforced segmentation, using unidirectional technologies and architectures, is deployed to provide secure remote access. Examples of hardware-enforced remote connectivity include:

- » **Unidirectional Remote Screen View**, which Transmits real-time screen images to remote technicians, allowing them to provide real-time advice to on-site personnel,
- » **Time-limited hardware switches** that enable temporary bidirectional remote access, providing physical control over the duration of software-based remote access, and
- » **Hardware-Enforced Remote Access (HERA⁸)** that uses unidirectional technology to enable interactive remote access while preventing attacks that exploit vulnerabilities from pivoting through remote access gateways into protected OT networks.

⁶<https://aws.amazon.com/blogs/iot/securely-sending-industrial-data-to-aws-iot-services-using-unidirectional-gateways/>

⁷<https://www.cisa.gov/resources-tools/resources/modern-approaches-network-access-security>

⁸<https://waterfall-security.com/technology-and-products/hera/>

» Power Generation-Specific 62443 Application Guidance

The unique challenges and criticality of power generation demand a tailored approach to cybersecurity that prioritizes the protection of essential infrastructure and services. This document provides guidance for interpreting and applying 62443 and modern cybersecurity techniques for power generation applications.

This guidance aims to reduce complexity while improving the resilience of power generation systems by addressing events that could produce unacceptable consequences from the onset. This is achieved through a consequence-based risk assessment, creating zones according to that assessment, and mitigating these events using engineered controls. Residual risk is then evaluated and mitigated using 62443, NERC CIP and other power-generation-specific advice.

• • • • •