SHIELDWORKZ

IEC 62443 Foundational Guide

A Practitioner's Reference for Building and Maturing Industrial Cybersecurity Programs

This page has been intentionally left blank

About This Guide

This IEC 62443 Foundation Guide has been developed by Shieldworkz as a practitioner handbook for organizations implementing, assessing, or maturing OT cybersecurity programs using the IEC 62443 family of standards, across manufacturing, energy, oil & gas, utilities, water, chemicals, pharmaceuticals, food & beverage, mining, and transportation sectors.

The guide is intended for CISOs, CIOs, OT Security Managers, Plant Managers, Control System and SCADA Engineers, Industrial Automation Engineers, OT Architects, SOC Analysts, Risk Managers, Compliance Officers, Internal Auditors, System Integrators, Equipment Manufacturers, and Executive Leadership.

Scope and sourcing discipline: this document summarizes concepts from the IEC 62443 series, ISA guidance, NIST SP 800-82 Rev. 3, NIST CSF 2.0, NIST RMF, NERC CIP, ISO/IEC 27001, ISO/IEC 27019, CISA OT guidance, ENISA guidance, the EU NIS2 Directive, the EU Cyber Resilience Act, Saudi ECC/OTCC, and UAE Information Assurance Regulations. No clause numbers, mandatory controls, or compliance obligations have been invented; where IEC 62443 text could not be verified at the level of a specific clause number, this guide summarizes the general concept and scope instead of citing a fabricated reference. Throughout, requirements are labeled as follows:

Label	Meaning
NORMATIVE REQUIREMENT	A mandatory clause or requirement explicitly defined within the cited part of the IEC 62443 series, applicable within that part's stated scope and the organization's chosen Security Level target.
RECOMMENDED PRACTICE	A practice recommended by IEC 62443, ISA guidance, or a referenced standard body, but not universally mandatory across all conformance profiles.
INDUSTRY GUIDANCE	Widely accepted practice drawn from ISA, NIST, CISA, ENISA, or other recognized bodies, without a single binding source in IEC 62443 itself.
IMPLEMENTATION ADVICE	Shieldworkz practitioner guidance based on assessment and field experience; explicitly not a normative requirement of any standard.

Table of Contents

Executive Summary

Why IEC 62443 Matters

IEC 62443 is the leading international standard series specifically developed for securing Industrial Automation and Control Systems (IACS). Unlike general-purpose IT security standards, IEC 62443 was designed from the outset to accommodate the safety, availability, and real-time constraints unique to operational technology. For organizations seeking a defensible, internationally recognized reference framework for OT cybersecurity, IEC 62443 provides common vocabulary, structured risk methodology, and technical requirements applicable across asset owners, system integrators, and product suppliers alike.

The Evolution of Industrial Cybersecurity

Industrial cybersecurity has evolved from an assumption of air-gapped isolation, through a period where IT security controls were applied directly (and often unsuccessfully) to OT, toward today's recognition that OT requires its own risk-based, lifecycle-oriented security discipline. IEC 62443 (originally developed under the ISA99 committee) reflects this evolution, incorporating lessons from major publicly documented incidents and decades of industrial automation engineering practice.

Why IT Security Alone Is Insufficient for OT

IT security practice generally prioritizes confidentiality and assumes frequent patching, standardized endpoints, and tolerance for downtime during maintenance. OT environments generally prioritize safety and availability, run long-lived and often unsupported systems, and cannot tolerate the unpredictability that some IT security tools introduce. IEC 62443 directly addresses this gap by defining security requirements and a management system tailored to industrial automation and control system realities, rather than adapting IT frameworks after the fact.

Business Drivers for Adopting IEC 62443

- Reducing the likelihood and consequence of safety, environmental, and production-impacting cyber incidents.
- Meeting customer, insurer, or regulator expectations that increasingly reference IEC 62443 as a recognized baseline.
- Providing a common technical language between asset owners, system integrators, and equipment suppliers during procurement and contracting.
- Supporting merger, acquisition, and investment due diligence where OT cybersecurity posture is increasingly scrutinized.
- Establishing a structured, auditable security management system rather than ad hoc or inconsistent practices.

Regulatory Alignment

While IEC 62443 itself is a voluntary consensus standard rather than a law or regulation, it is increasingly referenced by regulatory and sector frameworks, including elements of the EU NIS2 Directive's risk-management expectations, the EU Cyber Resilience Act's essential requirements for products with digital elements, and various national critical-infrastructure programs including Saudi Arabia's OTCC. Organizations should confirm current regulatory text directly, as the degree of formal reference to IEC 62443 varies by jurisdiction and is subject to change.

Benefits of Implementation

- A structured, risk-based approach to segmenting and protecting OT environments (zones and conduits).
- A common Security Level vocabulary (SL1–SL4) for expressing and comparing protection targets across zones, systems, and components.
- Supplier-facing requirements (secure development lifecycle, component security) that raise the baseline security of procured OT products over time.
- A management-system foundation (policies, risk assessment, patch management) that supports continuous improvement rather than a one-time project.

Key Takeaways for Executives

1. IEC 62443 is a voluntary, internationally recognized standard, not a single monolithic certification — organizations should determine which parts and Security Level targets are relevant to their risk profile.
2. Full conformance is a multi-year journey; most organizations should begin with foundational asset visibility, governance, and zone/conduit architecture before pursuing formal certification.
3. IEC 62443 complements, rather than replaces, other frameworks the organization may already be subject to (ISO/IEC 27001, NIST CSF, sector regulation) — see Section 4 for detailed mapping.
4. Meaningful risk reduction depends on genuine engineering and operations engagement, not policy documentation alone.

> **IMPLEMENTATION ADVICE**
>
> Shieldworkz recommends that executive sponsors treat IEC 62443 adoption as a multi-year capability-building program measured through the KPIs in Section 11, rather than a pass/fail compliance exercise completed once and then set aside.

Section 1 — Understanding Operational Technology (OT)

This section provides the shared technical vocabulary used throughout the guide before introducing IEC 62443's own terminology and models in Section 2.

1.1 Operational Technology (OT)

Operational Technology is hardware and software that detects or causes changes in physical processes through direct monitoring and control of physical devices — distinct from Information Technology, which primarily processes, stores, and transmits data.

1.2 Industrial Control Systems (ICS)

ICS is the umbrella term for the control system types found across industrial environments — SCADA, DCS, and PLC-based systems — together with associated instrumentation. IEC 62443 uses the closely related term Industrial Automation and Control System (IACS) to describe broadly the same scope: personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.

SCADA Systems

Supervisory Control and Data Acquisition systems provide centralized monitoring and control over geographically dispersed assets such as pipelines, transmission networks, and water distribution systems.

Distributed Control Systems (DCS)

DCS architectures distribute control functions across controllers close to the process, typically within a single site, coordinated through a common supervisory layer.

Programmable Logic Controllers (PLCs)

PLCs are ruggedized industrial computers executing control logic to directly operate field devices based on sensor input, and are a primary asset class addressed by IEC 62443-4-2 component requirements.

Remote Terminal Units (RTUs)

RTUs interface with field sensors and actuators, converting physical signals into data communicated to a SCADA master, common in geographically distributed environments.

Human-Machine Interfaces (HMIs)

HMIs provide the graphical interface through which operators monitor process status and issue commands, and represent a frequent target given their direct path to process manipulation.

Engineering Workstations

Engineering workstations run vendor configuration software used to program PLCs, DCS controllers, and safety systems, making them among the highest-consequence assets to protect.

Historians

Historians log process data over time for trending, reporting, and regulatory purposes, and often sit at the OT/IT boundary.

Safety Instrumented Systems (SIS)

SIS are independent systems designed to bring a process to a safe state when unsafe conditions are detected. IEC 62443 addresses SIS protection as a distinct consideration given the safety consequence of compromise.

Industrial Internet of Things (IIoT)

IIoT refers to internet-connected sensors, actuators, and edge devices used for condition monitoring, predictive maintenance, and process optimization, introducing new attack surface at the OT/cloud boundary.

Industrial Ethernet

Industrial Ethernet refers to Ethernet-based protocols adapted for deterministic, real-time industrial communication (e.g., PROFINET, EtherNet/IP, Modbus TCP), increasingly displacing legacy serial fieldbus in modern deployments while introducing IT-style network attack surface into OT.

Cyber-Physical Systems (CPS)

Cyber-Physical Systems is a broader engineering term describing systems where computational elements are tightly integrated with physical processes — a superset that includes ICS/OT alongside robotics, autonomous vehicles, and building automation. This guide uses OT/ICS as the primary scope, consistent with IEC 62443's IACS focus, while noting CPS as the wider academic and engineering context.

1.3 The Purdue Enterprise Reference Architecture (PERA)

PERA is a widely used conceptual model for segmenting industrial environments into logical levels. IEC 62443's zone and conduit model (introduced in Section 2) is compatible with, but not identical to, PERA — zones can be drawn along PERA level boundaries or according to other risk-based groupings such as process area or criticality.

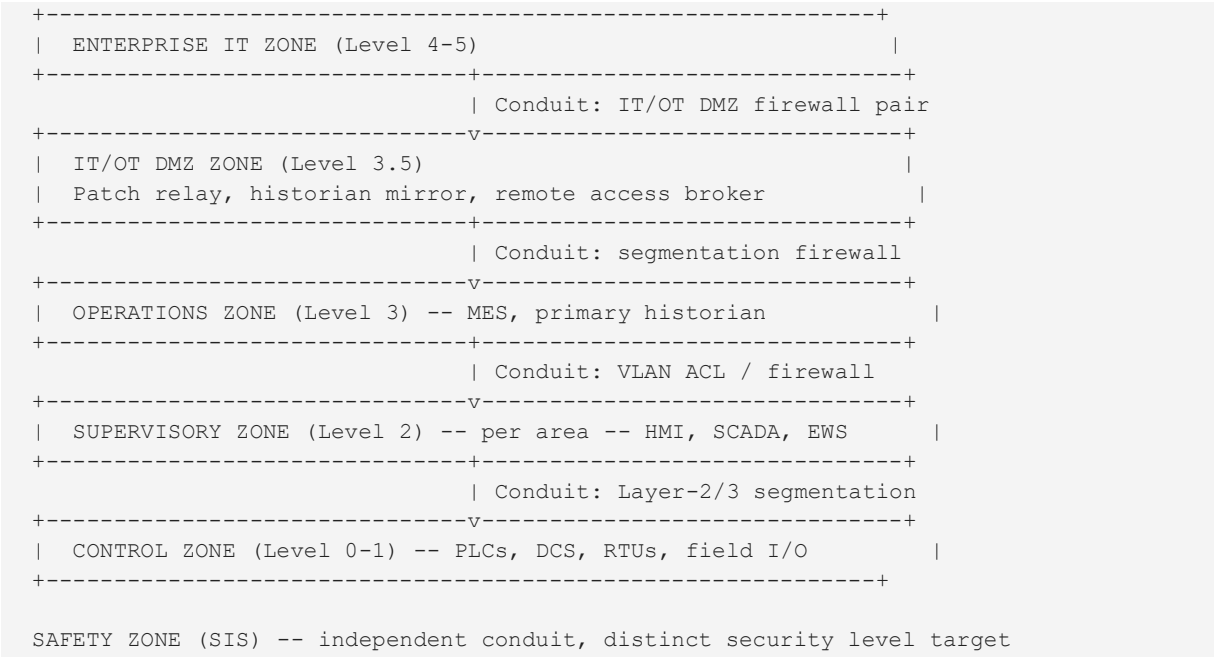
```
Level 5   Enterprise Network (ERP, corporate IT, email, internet)
Level 4   Site Business & Logistics (business planning, IT servers)
----------------- IT/OT DMZ (data diodes, jump hosts, brokers) ---------
Level 3   Operations Management (MES, OT historians, patch mgmt servers)
Level 2   Supervisory Control (HMI, SCADA servers, engineering stations)
Level 1   Basic Control (PLCs, DCS controllers, RTUs, SIS logic solvers)
Level 0   Physical Process (sensors, actuators, motors, valves, drives)
```

1.4 IT vs. OT vs. IIoT

Dimension	IT	OT	IIoT
Primary priority	Confidentiality, then Integrity, then Availability	Safety and Availability, then Integrity, then Confidentiality	Varies; often availability + data integrity for analytics
Asset lifecycle	3–5 years	15–25+ years	3–7 years, often unmanaged post-install
Patch cadence	Regular, often automated	Infrequent, vendor-validated, scheduled outages	Vendor-dependent, frequently neglected
Typical protocols	TCP/IP, HTTP/S	Modbus, DNP3, Profibus, EtherNet/IP, OPC-UA, HART	MQTT, CoAP, cloud APIs
IEC 62443 relevance	Indirect (via IT/OT DMZ conduit requirements)	Direct, primary scope	Emerging scope, addressed via component and zone concepts

1.5 Reference Architecture and Security Zones

The diagram below illustrates a representative segmented architecture. Zone boundaries shown are illustrative; IEC 62443-3-2 requires zone definition to be derived from an organization's own risk assessment rather than applied as a fixed template.



RECOMMENDED PRACTICE

IEC 62443-3-3 concepts support segmenting the Safety Instrumented System into its own zone with an independently defined Security Level target, separate from the Basic Process Control System zone. The specific separation method (physical vs. logical) is an organization-specific engineering decision informed by risk assessment.

Section 2 — Understanding the IEC 62443 Family

2.1 History and Evolution

The IEC 62443 series originated from work by the ISA99 committee of the International Society of Automation, established to address the growing recognition that industrial automation and control systems required security guidance distinct from general IT standards. The work was subsequently adopted and published jointly with the International Electrotechnical Commission as the IEC 62443 series, and has been periodically revised as industrial cybersecurity practice and threat understanding have matured. It remains under active maintenance by ISA99/IEC working groups.

2.2 Objectives and Scope

IEC 62443 aims to provide a flexible framework for securing Industrial Automation and Control Systems (IACS) throughout their lifecycle, applicable across asset owners, system integrators, and product/component suppliers. Its scope covers people, processes, and technology, distinguishing it from purely technical standards and purely management-system standards.

2.3 Risk-Based Philosophy

IEC 62443 is fundamentally risk-based rather than prescriptive: it does not mandate a single fixed set of controls for every organization. Instead, it provides a structured methodology (particularly within 62443-3-2) for assessing risk, defining zones and conduits, and selecting appropriate target Security Levels based on the consequence and likelihood relevant to each organization's specific environment.

2.4 Defense-in-Depth

Consistent with general OT security principles (see Section 3), IEC 62443 embeds defense-in-depth through its zone and conduit model — no single control or boundary is assumed sufficient; layered protection is expected across network, host, application, and procedural controls.

2.5 Security Levels (SL1–SL4)

IEC 62443 defines four Security Levels representing increasing protection against increasingly capable threat actors, roughly summarized as:

Security Level	General Threat Characterization (Conceptual)
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means, low resources, generic skills, low motivation
SL 3	Protection against intentional violation using sophisticated means, moderate resources, IACS-specific skills, moderate motivation

Security Level	General Threat Characterization (Conceptual)
SL 4	Protection against intentional violation using sophisticated means, extended resources, IACS-specific skills, high motivation

IEC 62443 distinguishes between the Target Security Level (SL-T, what an organization determines it needs based on risk assessment), the Achieved Security Level (SL-A, what a system actually delivers as implemented), and the Capability Security Level (SL-C, what a component or system is capable of supporting when properly configured). This distinction is important during assessment: a component may be SL-C 3 capable but achieve only SL-A 1 if misconfigured.

> **NORMATIVE REQUIREMENT**
> The definition of four Security Levels (SL1–SL4) and the SL-T/SL-A/SL-C distinction is a core normative concept of the IEC 62443 series. The specific target SL assigned to any given zone or conduit within an organization, however, is the output of that organization's own risk assessment (per 62443-3-2 concepts), not a value fixed by the standard itself.

2.6 Zones and Conduits

A zone is a grouping of logical or physical assets that share common security requirements, typically based on criticality, function, or risk profile. A conduit is a logical grouping of communication channels connecting two or more zones, through which security requirements for that connection (such as the Security Level target) are defined and enforced. This model provides the structural basis for network segmentation guidance throughout this document.

2.7 Lifecycle Approach

IEC 62443 addresses security across the full IACS lifecycle — from initial risk assessment and system design, through implementation, operation and maintenance, to eventual decommissioning — rather than treating security as a point-in-time implementation project. This lifecycle emphasis is reflected across the -2-x (operational/management) and -3-x/-4-x (technical) parts of the series.

2.8 Secure-by-Design Principles

IEC 62443-4-1 defines requirements for a secure product development lifecycle that automation product suppliers should follow, embedding security considerations from initial product concept through to end-of-life, rather than retrofitting security into already-designed products.

2.9 Structure of the IEC 62443 Series

General (IEC 62443-1-x)

The -1-x parts establish foundational concepts, models, and terminology used throughout the rest of the series, including the zone/conduit model and Security Level concepts introduced above. These parts are primarily reference material rather than a set of directly implementable controls.

Policies and Procedures (IEC 62443-2-x)

The -2-x parts address organizational and management requirements. This includes requirements for an asset owner's IACS security management system (broadly comparable in structure to a management-system standard, addressing governance, risk assessment, and organizational processes) and guidance on patch management practices specific to the IACS environment. These parts are primarily addressed to asset owners.

System (IEC 62443-3-x)

The -3-x parts address system-level requirements, including a structured methodology for security risk assessment and system design (used to determine zone/conduit boundaries and target Security Levels) and system-level technical security requirements organized into foundational requirement categories, each mapped against the four Security Levels.

Component (IEC 62443-4-x)

The -4-x parts address product-level requirements aimed primarily at automation product suppliers: a secure product development lifecycle standard, and a set of technical security requirements for individual components (embedded devices, network devices, host devices, and software applications), similarly organized by foundational requirement category and Security Level.

2.10 How the Standards Relate — Stakeholder Map

```
 ASSET OWNER                SYSTEM INTEGRATOR           PRODUCT SUPPLIER
-------------              -------------------         ----------------
Primary user of:            Primary user of:            Primary user of:
* 62443-2-x (mgmt system,   * 62443-3-x (system design, * 62443-4-1 (secure
  patch mgmt)                 zone/conduit risk assess.)  development lifecycle)
* 62443-3-x (as consumer     * 62443-2-x (as service     * 62443-4-2 (component
  of integrator's design)      provider, where applicable)  technical requirements)
* 62443-1-x (concepts,      * 62443-1-x (concepts,      * 62443-1-x (concepts,
  terminology reference)       terminology reference)      terminology reference)

All three roles share the -1-x foundational concepts and terminology, and
reference the same Security Level (SL1-SL4) vocabulary when specifying,
designing, and delivering IACS components and systems.
```

> **INDUSTRY GUIDANCE**
>
> Shieldworkz observes that organizations new to IEC 62443 frequently attempt to apply -3-x/-4-x technical requirements before establishing the -2-x management system foundation. ISA and IEC guidance generally position the -2-1 management system as the organizational foundation

> upon which technical requirements are applied consistently — Shieldworkz recommends sequencing accordingly.

Section 3 — OT Security Fundamentals

This section outlines core OT security principles and explains, for each, how IEC 62443 supports or structures its implementation.

3.1 Safety

Personnel and process safety takes precedence over other security objectives in OT. IEC 62443 supports this through its emphasis on risk assessment that considers consequence (including safety consequence) when determining target Security Levels, and through specific attention to Safety Instrumented System protection as a distinct zone consideration.

3.2 Availability

OT environments generally prioritize availability alongside safety, ahead of confidentiality. IEC 62443's foundational requirement categories include availability-related considerations (e.g., resource availability, resistance to denial-of-service conditions) alongside confidentiality- and integrity-related categories, reflecting this OT-specific priority ordering.

3.3 Reliability

Deterministic, predictable system behavior is essential in OT. IEC 62443-4-2 component requirements are written with awareness of resource-constrained, real-time embedded devices, distinguishing them from general-purpose IT component security requirements that might assume more headroom.

3.4 Process Integrity

Ensuring sensor readings, setpoints, and control outputs are accurate and untampered is a core OT security objective. IEC 62443's foundational requirements include integrity-focused categories addressing data and communication integrity within zones and across conduits.

3.5 Confidentiality

While typically a lower priority than safety and availability in OT, confidentiality remains relevant — particularly for engineering data, proprietary process recipes, and safety case documentation. IEC 62443 includes confidentiality as one of its foundational requirement categories, applied proportionally to the target Security Level.

3.6 Defense-in-Depth

IEC 62443's zone and conduit model is inherently a defense-in-depth construct: it assumes no single boundary is sufficient and requires security requirements to be defined and enforced at each conduit between zones, not only at the network perimeter.

3.7 Least Privilege

Access control and least-privilege concepts are addressed within IEC 62443's foundational requirement categories covering identification, authentication, and use control, applied at both the system (-3-3) and component (-4-2) level.

3.8 Zero Trust in OT

Zero Trust — verify explicitly, least-privileged access, assume breach — is a general industry security concept (formalized generally in NIST SP 800-207) rather than an IEC 62443-native term. Shieldworkz treats IEC 62443's zone/conduit and strict conduit-level authorization model as broadly compatible with Zero Trust principles adapted for OT, but organizations should not assume IEC 62443 conformance is equivalent to Zero Trust Architecture, or vice versa — they are complementary industry guidance, not interchangeable requirements.

3.9 Secure Remote Access

Remote access into OT zones is treated as a conduit requiring defined security requirements under the IEC 62443 model, including authentication strength appropriate to the target Security Level of the zones being connected.

3.10 Asset Visibility

While asset inventory itself is general OT security guidance rather than a distinctly named IEC 62443 clause, it is a practical prerequisite for conducting the zone/conduit risk assessment that -3-2 requires — an organization cannot meaningfully define zones without knowing what assets exist within them.

3.11 Continuous Monitoring

Ongoing monitoring supports the operational phase of the IACS lifecycle addressed by the -2-x management system parts, and helps verify that the Achieved Security Level (SL-A) of a zone continues to match its Target Security Level (SL-T) over time as systems and threats evolve.

3.12 Cyber Resilience

Resilience — the capacity to continue safe operation or recover quickly from an incident — is supported by IEC 62443's lifecycle approach, which extends beyond initial implementation into ongoing operation, incident handling, and maintenance.

3.13 Safety-Security Convergence

The intersection of functional safety (e.g., IEC 61511 for the process industries) and cybersecurity is an area of growing industry attention. IEC 62443 addresses cybersecurity of systems including SIS, but does not itself define functional safety requirements — organizations should treat functional safety standards and IEC 62443 as complementary, coordinated through joint engineering and security risk assessment rather than a single unified standard.

INDUSTRY GUIDANCE

Safety-security convergence practice — including joint hazard and risk assessments spanning both functional safety (IEC 61511) and cybersecurity (IEC 62443) disciplines — is an area of active industry guidance development rather than a single settled normative requirement. Shieldworkz recommends organizations involve both safety and cybersecurity engineering functions jointly in SIS-related risk assessment.

Section 4 — Standards and Compliance

This section explains how other commonly referenced frameworks relate to IEC 62443. General scope descriptions are provided; organizations should consult current published text for clause-level requirements.

4.1 NIST SP 800-82 Rev. 3

NIST SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security, provides OT-focused threat context and controls guidance (via cross-reference to NIST SP 800-53). It is complementary to IEC 62443: both address OT/ICS security, but SP 800-82 is guidance rather than a certifiable standard, and it references IEC 62443 concepts (zones/conduits, defense-in-depth) as part of its own recommended architecture guidance.

4.2 NIST Cybersecurity Framework (CSF) 2.0

NIST CSF 2.0 organizes cybersecurity outcomes into six functions (Govern, Identify, Protect, Detect, Respond, Recover). It is a voluntary organizing framework that can sit above an IEC 62443 implementation — an organization can use CSF 2.0 for executive communication and program structure while using IEC 62443 as the detailed technical and management-system reference for OT-specific implementation.

4.3 NIST Risk Management Framework (RMF)

The NIST RMF (SP 800-37) defines a structured process for managing information system risk, mandatory for U.S. federal information systems. Its risk-based, lifecycle structure is conceptually aligned with IEC 62443's own risk-based philosophy, though the two use different terminology and are not formally interoperable without a mapping exercise.

4.4 NERC CIP

NERC CIP standards are mandatory, enforceable reliability standards for the North American Bulk Electric System. NERC CIP requirements are independently defined and enforced by NERC, not derived from IEC 62443; however, organizations implementing IEC 62443-aligned zone/conduit segmentation and access control often find this supports (without automatically satisfying) several NERC CIP control objectives, such as Electronic Security Perimeter requirements. Applicability and specific control mapping should be confirmed against current NERC CIP standards documentation.

4.5 ISO/IEC 27001

ISO/IEC 27001 specifies requirements for a certifiable Information Security Management System (ISMS), general-purpose and IT-oriented. Organizations with an existing ISO/IEC 27001 ISMS can often extend its governance structure (policy, risk assessment, internal audit, management review) to cover OT scope using IEC 62443-2-1 as the OT-specific technical content within that broader management system, rather than building two entirely separate management systems.

4.6 ISO/IEC 27019

ISO/IEC 27019 extends ISO/IEC 27001/27002 guidance specifically to process control systems in the energy utility industry. It is sector-specific guidance intended to be applied alongside ISO/IEC 27001, and addresses overlapping ground with IEC 62443 for energy sector organizations — the two are complementary rather than competing.

4.7 EU NIS2 Directive

NIS2 requires designated essential and important entities to implement risk management measures and report significant incidents, transposed into national law by EU member states. NIS2 does not itself mandate IEC 62443 conformance, but IEC 62443-aligned practices (risk assessment, zone/conduit segmentation, supply chain security) can support several of the risk-management measure categories referenced in NIS2's implementing legislation. Organizations should confirm specific requirements under their applicable national transposition.

4.8 EU Cyber Resilience Act (CRA)

The CRA establishes EU-wide cybersecurity requirements for products with digital elements, addressed primarily to manufacturers. IEC 62443-4-1 (secure development lifecycle) and 62443-4-2 (component requirements) are relevant reference standards that OT/IIoT product manufacturers may draw upon to help demonstrate conformance with CRA essential requirements, though the CRA's own harmonized standards process determines formal presumption of conformity — organizations should not assume IEC 62443 conformance alone automatically satisfies CRA obligations without confirming current harmonized standard status.

4.9 Saudi Essential Cybersecurity Controls (ECC) / OTCC

The Saudi NCA's ECC and sector-specific OTCC establish mandatory baseline controls for in-scope government and critical infrastructure entities. The OTCC's control structure addresses similar domains to IEC 62443 (governance, asset management, network security, access control) but is an independently published national regulatory control set, not a direct restatement of IEC 62443 — organizations subject to OTCC should reference NCA's published control text directly, using IEC 62443 as complementary technical depth where the OTCC does not specify implementation detail.

4.10 UAE Information Assurance Regulations

The UAE's Information Assurance regulatory framework establishes information security requirements for in-scope government and critical infrastructure entities. As with the Saudi ECC/OTCC, this is an independent national regulatory framework; organizations should confirm current requirements with the relevant UAE authority and treat IEC 62443 as complementary technical guidance rather than a substitute for the regulation's own text.

4.11 Comparison and Mapping Summary

Framework	Nature	Relationship to IEC 62443
NIST SP 800-82 Rev. 3	Guidance document	Complementary; references IEC 62443 zone/conduit and defense-in-depth concepts
NIST CSF 2.0	Voluntary framework	Can sit above IEC 62443 as executive-level organizing structure
NIST RMF	Mandatory (US federal) risk process	Conceptually aligned risk-based approach; not formally interoperable without mapping
NERC CIP	Mandatory reliability standard (NA BES)	Independently enforced; IEC 62443 practices can support but not automatically satisfy CIP requirements
ISO/IEC 27001	Certifiable ISMS standard	Can host IEC 62443-2-1 as OT-specific content within a broader ISMS
ISO/IEC 27019	Energy sector guidance	Complementary, overlapping scope for energy utility process control
EU NIS2 Directive	Mandatory (per national transposition)	Does not mandate IEC 62443; IEC 62443 practices can support risk-management measure categories
EU Cyber Resilience Act	Mandatory (product manufacturers)	IEC 62443-4-1/4-2 relevant as reference material; formal conformity requires confirming CRA harmonized standard status
Saudi ECC / OTCC	Mandatory (in-scope entities)	Independent national control set; complementary technical depth from IEC 62443
UAE IA Regulations	Mandatory (in-scope entities)	Independent national regulation; complementary technical depth from IEC 62443

> **NOTICE**
> This mapping is a simplified overview for orientation. It is not legal or compliance advice; organizations should confirm current, jurisdiction-specific applicability and any formal conformity mechanisms with qualified counsel and each framework's primary source text.

Section 5 — Compliance Measures and Security Controls

This section addresses governance, administrative, operational, physical, and technical controls relevant to an IEC 62443-aligned OT cybersecurity program. Each control category includes objective, implementation guidance, evidence expected during an assessment, common pitfalls, and relevant IEC 62443 references. References describe the general part and topic area rather than specific clause numbers, which vary by edition and should be confirmed against the current published standard.

5.1 Governance

Objective

Establish clear accountability, decision rights, and management commitment for the IACS security management system.

Implementation Guidance

- Establish an OT security governance structure with executive sponsorship and cross-functional (IT/OT/safety) representation.
- Document the scope of the IACS security management system, including which sites, zones, and systems are covered.
- Define policy review and management review cadence.

Evidence Expected During Assessment

Governance charter; management review minutes; documented scope statement for the security management system.

Common Pitfalls

- Governance structure exists on paper but lacks executive engagement.
- Scope of the management system is undefined or inconsistently applied across sites.

Relevant IEC 62443 References

IEC 62443-2-1 (security management system requirements, general structure).

5.2 Asset Management

Objective

Maintain a complete, accurate, current inventory of IACS assets as the foundation for zone/conduit definition and risk assessment.

Implementation Guidance

- Combine passive network discovery, physical walkthroughs, and engineering documentation review to build and maintain the inventory.
- Capture vendor, model, firmware/software version, network location, and criticality for each asset.
- Reconcile inventory against zone/conduit diagrams periodically.

Evidence Expected During Assessment

Asset inventory export; validation records showing reconciliation against physical/discovery findings.

Common Pitfalls

- Inventory built once during initial assessment and never maintained.
- Passive discovery alone used, missing serial or air-gapped devices.

Relevant IEC 62443 References

Asset inventory itself is general OT security guidance rather than a distinctly numbered IEC 62443 clause; it is a practical prerequisite for the 62443-3-2 risk assessment and zone/conduit definition process.

5.3 Risk Assessment

Objective

Identify, analyze, and evaluate cybersecurity risk to determine zone/conduit boundaries and target Security Levels.

Implementation Guidance

- Conduct a structured risk assessment considering consequence (safety, environmental, production, financial) and likelihood, per zone rather than as a single organization-wide exercise.
- Reassess risk when significant architecture, threat landscape, or asset changes occur, and on a defined periodic cycle.
- Document the rationale for each zone's target Security Level (SL-T).

Evidence Expected During Assessment

Risk assessment methodology documentation; risk register with per-zone consequence/likelihood ratings and assigned SL-T values.

Common Pitfalls

- Risk assessment performed once at program inception and never revisited.
- SL-T values assigned without documented rationale traceable to the risk assessment.

Relevant IEC 62443 References

IEC 62443-3-2 (security risk assessment for system design).

5.4 Security Policies

Objective

Establish documented policies and procedures governing OT security practices across the organization.

Implementation Guidance

- Develop policies covering, at minimum, access control, remote access, change management, patch/vulnerability management, and incident response.
- Ensure policies are approved by appropriate governance authority and communicated to affected personnel.
- Review and update policies on a defined cycle or following significant incidents/changes.

Evidence Expected During Assessment

Current, approved policy documents; version history showing periodic review; training/acknowledgment records.

Common Pitfalls

- Policies copied from IT without OT-specific adaptation.
- Policies approved but not operationally followed, with no verification mechanism.

Relevant IEC 62443 References

IEC 62443-2-1 (policies and procedures requirements).

5.5 Identity and Access Management

Objective

Ensure only authorized individuals and services can access IACS assets, with access proportional to role and the target Security Level of the zone.

Implementation Guidance

- Implement individual (non-shared) accounts wherever technically and operationally feasible.
- Apply role-based access control and least privilege for engineering, operator, and administrative functions.
- Deploy multi-factor authentication for remote and administrative access commensurate with target Security Level.

Evidence Expected During Assessment

Access review/recertification records; authentication configuration evidence for remote/admin paths.

Common Pitfalls

- Shared operator accounts persisting without compensating controls.
- Authentication strength not scaled to the target Security Level of the zone being accessed.

Relevant IEC 62443 References

IEC 62443-3-3 and 62443-4-2 foundational requirements addressing identification and authentication control (FR 1) and use control (FR 2).

5.6 Network Segmentation

Objective

Divide the IACS environment into zones with controlled conduits, limiting lateral movement between areas of differing risk.

Implementation Guidance

- Define zone boundaries based on the risk assessment (Section 5.3) rather than existing physical topology alone.
- Establish a dedicated IT/OT DMZ; disallow direct conduits between enterprise IT and OT supervisory/control zones.
- Segment the SIS network from the BPCS network as a distinct zone.

Evidence Expected During Assessment

Network diagrams reflecting actual configuration; firewall/VLAN rule review confirming enforcement matches documented zone boundaries.

Common Pitfalls

- Documented segmentation that does not match actual configured rules.
- SIS network sharing a zone with the BPCS without a documented risk-based justification.

Relevant IEC 62443 References

IEC 62443-3-2 (zone/conduit definition); IEC 62443-3-3 (system security requirements applied per zone).

5.7 Zones and Conduits (Formal Definition)

Objective

Formally define, document, and maintain the zone and conduit model as the structural basis for the security program.

Implementation Guidance

- Document each zone's assets, boundary, and target Security Level.
- Document each conduit's connected zones, allowed traffic/protocols, and target Security Level.
- Review and update the zone/conduit model when architecture changes.

Evidence Expected During Assessment

Zone/conduit diagram and register with assigned SL-T per zone/conduit; change history showing periodic review.

Common Pitfalls

- Zone/conduit model created for an assessment but not maintained as a living document.
- Conduits identified in diagrams but not enforced through actual technical controls.

Relevant IEC 62443 References

IEC 62443-1-1 (zone/conduit model concepts); IEC 62443-3-2 (application of the model to risk assessment).

5.8 Secure Remote Access

Objective

Ensure any remote connection into IACS zones is authenticated, authorized, time-bound, and monitored, consistent with the conduit's target Security Level.

Implementation Guidance

- Route all remote access through a dedicated, monitored jump host or broker in the IT/OT DMZ.
- Require MFA and time-bound, request-based access rather than persistent always-on connections.
- Log and, where appropriate, record remote sessions, particularly for vendor/third-party access.

Evidence Expected During Assessment

Session logs demonstrating time-bound access; absence of persistent always-on vendor tunnels; MFA enforcement records.

Common Pitfalls

- Always-on VPN tunnels left open for vendor convenience.
- Remote access permitted directly into control zones without traversing the DMZ.

Relevant IEC 62443 References

IEC 62443-3-3 foundational requirements on access control and restricted data flow (FR 2, FR 5).

5.9 Engineering Workstation Security

Objective

Protect the systems capable of pushing configuration and logic changes to controllers.

Implementation Guidance

- Restrict engineering workstations to dedicated, hardened use — no general web browsing or email.
- Apply strict access control and disconnect from the network when not actively programming, where operationally feasible.
- Maintain vendor-validated patching and endpoint protection.

Evidence Expected During Assessment

Inventory of engineering workstations with confirmed dedicated-use status; access logs.

Common Pitfalls

- Engineering workstations also used for general office productivity.
- No baseline logic comparison capability after workstation use.

Relevant IEC 62443 References

IEC 62443-3-3 and 62443-4-2 requirements addressing endpoint and use control relevant to engineering tools.

5.10 PLC Protection

Objective

Protect programmable controllers from unauthorized logic changes and firmware manipulation.

Implementation Guidance

- Enable controller-native authentication features where the platform supports them.
- Restrict physical and network access to controller programming ports.
- Maintain and compare logic against a known-good baseline to detect unauthorized changes.

Evidence Expected During Assessment

Baseline logic comparison records; documented physical access restrictions to control cabinets.

Common Pitfalls

- Controller programming mode left permanently enabled.
- No baseline established, so unauthorized logic changes go undetected.

Relevant IEC 62443 References

IEC 62443-4-2 (component technical security requirements applicable to embedded/controller devices).

5.11 HMI Security

Objective

Protect operator interfaces from unauthorized use or manipulation while preserving necessary operational usability.

Implementation Guidance

- Avoid shared/generic operator accounts where individually attributable accounts are operationally feasible; apply compensating controls where they remain necessary.
- Lock screens after inactivity consistent with operational safety requirements.
- Restrict HMI software installation/configuration privileges to authorized engineering personnel.

Evidence Expected During Assessment

Account configuration review; screen-lock policy verification; change log for HMI configuration.

Common Pitfalls

- All operators sharing a single generic account with no compensating control.
- HMI configuration changes made without change management.

Relevant IEC 62443 References

IEC 62443-3-3/4-2 foundational requirements on identification, authentication, and use control.

5.12 Logging and Monitoring

Objective

Capture sufficient logs and maintain monitoring capability to support detection, investigation, and evidence of the Achieved Security Level.

Implementation Guidance

- Centralize logs from firewalls, remote access systems, and supported engineering/HMI/server assets.
- Deploy passive, protocol-aware network monitoring at zone boundaries.
- Define log retention aligned to operational and regulatory needs.

Evidence Expected During Assessment

Log source coverage inventory; monitoring sensor placement map against zone/conduit diagram; retention policy.

Common Pitfalls

- Monitoring deployed only at the IT/OT boundary with no zone-level visibility.
- Logs generated locally but never centralized, lost on device reboot or replacement.

Relevant IEC 62443 References

IEC 62443-3-3 foundational requirement on timely response to events (FR 6), including audit logging.

5.13 Backup and Recovery

Objective

Ensure configurations, logic, and engineering data can be restored quickly following a failure or incident.

Implementation Guidance

- Maintain current, tested, offline backups of PLC/DCS logic, HMI configuration, and engineering project files.
- Test restoration procedures periodically, not only backup capture.
- Maintain physical/printed fallback documentation for critical configurations where feasible.

Evidence Expected During Assessment

Successful test-restore records; backup age against defined recovery point objective.

Common Pitfalls

- Backups stored on the same network segment they protect against.
- Backup jobs configured but never validated through an actual restore test.

Relevant IEC 62443 References

IEC 62443-3-3 foundational requirement on resource availability (FR 7), which includes backup/recovery considerations.

5.14 Vulnerability Management

Objective

Identify known vulnerabilities in deployed IACS assets and prioritize remediation or compensating controls.

Implementation Guidance

- Monitor vendor advisories and recognized ICS vulnerability sources (e.g., CISA ICS advisories) for deployed asset types.
- Prioritize remediation by exploitability and consequence rather than treating all findings uniformly.
- Document compensating controls where immediate remediation is infeasible.

Evidence Expected During Assessment

Vulnerability register with prioritization rationale and remediation/compensating control status.

Common Pitfalls

- Vulnerabilities identified but never tracked to closure or documented compensating control.
- Vulnerability scanning performed without safety/engineering sign-off, risking system disruption.

Relevant IEC 62443 References

IEC 62443-2-3 (patch management guidance, closely related to vulnerability management practice); IEC 62443-2-1.

5.15 Patch Management

Objective

Apply security patches to IACS assets in a controlled manner that respects vendor validation and operational constraints.

Implementation Guidance

- Require vendor validation of patches for the specific control system version before deployment.
- Test patches in a non-production environment before applying to production systems.
- Align patch deployment to scheduled maintenance windows.

Evidence Expected During Assessment

Patch management procedure documentation; records of vendor validation and test-before-deploy practice.

Common Pitfalls

- IT-standard automatic patching applied to OT systems without vendor validation.
- No compensating controls documented for systems that cannot be patched.

Relevant IEC 62443 References

IEC 62443-2-3 (patch management in the IACS environment).

5.16 Change Management

Objective

Ensure modifications to IACS systems are reviewed, tested, approved, and documented before implementation.

Implementation Guidance

- Require formal change requests with safety impact assessment for any change touching control or safety logic.
- Maintain an approval trail distinguishing routine, emergency, and standard changes.
- Reconcile implemented changes against the configuration baseline (Section 5.17).

Evidence Expected During Assessment

Change request records with approval trail; reconciliation reports showing baseline alignment.

Common Pitfalls

- Emergency changes made verbally and never retroactively documented.
- Change approval process bypassed under production pressure.

Relevant IEC 62443 References

IEC 62443-2-1 (management of change requirements).

5.17 Configuration Management

Objective

Maintain an authoritative, version-controlled record of approved system configurations.

Implementation Guidance

- Maintain version-controlled baselines for PLC/DCS logic, HMI screens, and network device configurations.
- Reconcile deployed configurations against baseline on a defined schedule.
- Investigate and document any detected configuration drift.

Evidence Expected During Assessment

Configuration baseline records; drift detection reports with resolution status.

Common Pitfalls

- Baseline established once and never reconciled against live systems.
- No process to distinguish authorized changes from drift.

Relevant IEC 62443 References

IEC 62443-2-1 and 62443-3-3 configuration management-related requirements.

5.18 Third-Party and Vendor Security

Objective

Manage security risk introduced through vendors, system integrators, and contractors with access to IACS environments.

Implementation Guidance

- Require vendor remote/physical access to follow the organization's secure remote access and change management policies.
- Maintain a current register of active vendor access arrangements, reviewed periodically.
- Assess vendor security practices as part of contract renewal, not only initial onboarding.

Evidence Expected During Assessment

Vendor access register; vendor risk assessment records.

Common Pitfalls

- Vendors granted informal, undocumented access during site visits.
- Vendor risk assessed once at contract inception and never revisited.

Relevant IEC 62443 References

IEC 62443-2-1 (supply chain and third-party considerations within the management system).

5.19 Physical Security

Objective

Prevent unauthorized physical access to control cabinets, network equipment, and IACS spaces.

Implementation Guidance

- Lock and monitor control cabinets and network closets; log access.
- Apply badge/access control to control rooms and server rooms consistent with facility security policy.
- Extend physical security assessment to remote/unmanned sites.

Evidence Expected During Assessment

Access logs for control cabinets and OT spaces; physical security walkthrough findings tracked to closure.

Common Pitfalls

- Control cabinets left unlocked for operational convenience.
- Remote/unmanned sites overlooked in physical security programs.

Relevant IEC 62443 References

IEC 62443-2-1 (physical security considerations within the management system).

5.20 Supply Chain Security

Objective

Manage security risk introduced through the OT product and software supply chain, from component sourcing through delivery.

Implementation Guidance

- Include IEC 62443-4-1/4-2 conformance expectations in procurement specifications where applicable to the product category.
- Maintain a software/firmware bill of materials for critical assets where feasible.
- Assess subcontractor/component-level supply chain visibility for critical systems.

Evidence Expected During Assessment

Procurement documentation showing security requirements included; supply chain risk assessment records.

Common Pitfalls

- Security requirements added to contracts but never verified prior to acceptance.
- No visibility into component-level supply chain for critical systems.

Relevant IEC 62443 References

IEC 62443-4-1 (secure product development lifecycle, supplier-facing); IEC 62443-2-1 (supply chain considerations for asset owners).

5.21 Continuous Monitoring

Objective

Maintain ongoing visibility into the operational state of the security program, not only at the point of initial implementation.

Implementation Guidance

- Track KPIs (see Section 11) on a defined reporting cadence.
- Periodically reassess whether the Achieved Security Level of each zone continues to match its Target Security Level.
- Incorporate lessons learned from incidents, exercises, and audits into program updates.

Evidence Expected During Assessment

KPI reporting records; periodic SL-A vs. SL-T reassessment documentation.

Common Pitfalls

- Program treated as complete after initial implementation, with no ongoing verification.
- Metrics collected but never reviewed by leadership or acted upon.

Relevant IEC 62443 References

IEC 62443-2-1 (ongoing management system operation, monitoring, and improvement).

IMPLEMENTATION ADVICE

Shieldworkz recommends scoring each of the twenty-one control categories above against the maturity model in Appendix H to identify the highest-priority gaps for the next planning cycle, rather than attempting uniform improvement across all categories simultaneously.

Section 6 — Starting Point for OT Security

This section provides a five-phase implementation roadmap for organizations beginning or restructuring their OT security program around IEC 62443 principles. It is Shieldworkz implementation guidance built on the concepts in Sections 2, 3, and 5; sequencing should be adapted to organizational context.

Phase 1 — Discover (typically months 0–6)

- Secure executive sponsorship and establish OT security governance (Section 5.1).
- Conduct initial asset inventory combining passive discovery and physical walkthroughs (Section 5.2).
- Perform network discovery and architecture review to document actual, not assumed, topology.
- Conduct an initial risk identification exercise to inform zone/conduit definition in Phase 2.

> **IMPLEMENTATION ADVICE**
>
> Expected outcome: a documented governance structure, an initial asset inventory, and a clear picture of current segmentation gaps — the prerequisites for a meaningful 62443-3-2 risk assessment.

Phase 2 — Protect (typically months 4–14, overlapping Phase 1)

- Formally define zones and conduits with assigned target Security Levels, based on risk assessment (Section 5.3, 5.7).
- Implement network segmentation aligned to the zone/conduit model, prioritizing the IT/OT DMZ and SIS boundary.
- Strengthen identity and access management, including MFA on remote and administrative access.
- Migrate remote access to a monitored jump-host architecture; formalize vendor access governance.
- Harden engineering workstations and HMIs; establish configuration baselines.
- Establish tested backup and recovery for critical configurations.
- Review and strengthen physical security for control rooms, cabinets, and remote sites.

> **IMPLEMENTATION ADVICE**
>
> Expected outcome: measurable reduction in the highest-likelihood attack paths and a defensible zone/conduit architecture that can be independently verified against its documented target Security Levels.

Phase 3 — Detect (typically months 10–18)

- Deploy passive, protocol-aware OT network monitoring at zone boundaries.

- Integrate Network Detection and Response (NDR) capability with SOC processes, including OT-aware escalation.
- Incorporate relevant OT/ICS threat intelligence into detection use cases.
- Establish anomaly detection baselines for critical zones.
- Centralize logging per Section 5.12 with defined retention.

> **IMPLEMENTATION ADVICE**
> Expected outcome: reduced dwell time and the ability to detect anomalies before they result in safety or production consequence, tracked through the MTTD KPI in Section 11.

Phase 4 — Respond (typically months 14–20)

- Develop and formalize OT-specific incident response playbooks (see Section 9).
- Conduct tabletop exercises involving OT engineering and operations, not security personnel alone.
- Establish business continuity procedures, including manual operating fallback for critical processes.
- Build lessons-learned processes to feed findings back into governance and technical controls.

> **IMPLEMENTATION ADVICE**
> Expected outcome: a tested, OT-aware incident response capability with documented playbooks and defined regulatory reporting ownership, tracked through the MTTR KPI in Section 11.

Phase 5 — Improve (typically months 18–24+, ongoing)

- Conduct periodic IEC 62443 assessments (see Section 7) to track maturity and reassess SL-A vs. SL-T.
- Track and report the KPI suite in Section 11 to executive leadership.
- Formalize compliance management against applicable frameworks (Section 4).
- Embed continuous improvement based on incident lessons, assessment findings, and evolving threat intelligence.

6.1 Maturity Milestones by Phase

Phase	Typical Entry Maturity	Exit Milestone
1: Discover	No formal asset inventory or governance	Governance chartered; asset inventory covers majority of critical assets
2: Protect	Ad hoc or partial segmentation	Zone/conduit model documented with assigned SL-T; segmentation enforced and verified
3: Detect	Limited or no OT-specific monitoring	Passive monitoring live across priority zones; MTTD tracked and trending down
4: Respond	IT-only or undocumented incident response	OT-specific IR plan tested via tabletop exercise; MTTR tracked and trending down
5: Improve	One-time or absent assessment cycle	Recurring assessment cadence; KPI reporting to leadership; SL-A periodically reverified against SL-T

Section 7 — Conducting an IEC 62443 Assessment

This section outlines a practical assessment methodology reflecting Shieldworkz field experience conducting IEC 62443-aligned assessments across manufacturing, energy, water, and pharmaceutical environments. This methodology is Shieldworkz implementation guidance; organizations pursuing formal third-party certification should confirm the specific methodology required by their chosen certification body, which may differ in detail.

7.1 Assessment Methodology Overview

- Scope Definition: agree the sites, zones, and systems in scope, and confirm safety/operational constraints on any technical validation activity in advance.
- Stakeholder Identification: identify governance, engineering, operations, IT security, and vendor stakeholders to engage.
- Asset Inventory Validation: verify existing inventory against passive discovery and physical walkthrough findings.
- Documentation Review: review policies, procedures, zone/conduit diagrams, change records, and prior assessment findings.
- Architecture Assessment: review network diagrams, firewall rules, and segmentation design against actual configuration.
- Site Walkthrough: physically inspect control rooms, cabinets, and network infrastructure.
- Interviews: engage stakeholders identified above using structured interview guides.
- Evidence Collection: gather logs, configuration exports, and supporting documentation for each control category assessed.
- Technical Validation: where in scope and safety-approved, validate segmentation and access controls through controlled, non-disruptive testing.
- Maturity Scoring: score each control category against the maturity model in Appendix H.
- Gap Analysis: compare current state against the organization's target Security Levels and applicable control requirements.
- Risk Prioritization: rank findings by consequence and likelihood, not solely by control maturity score.
- Reporting: document findings, evidence, and recommendations for both executive and technical audiences.

7.2 Sample Interview Questions

For OT Engineering / Control System Engineers

- How were the current zone and conduit boundaries determined, and is the rationale documented?
- What is the process for approving and testing a change to controller logic?
- Are there any known undocumented network connections or 'temporary' bridges currently in place?

For Operations / Plant Management

- What manual fallback procedures exist if the HMI/SCADA system becomes unavailable, and when were they last exercised?
- How is vendor remote access to this site currently requested, approved, and monitored?

For IT Security / SOC

- What visibility does the SOC have into OT network traffic, and how are OT alerts triaged differently from IT alerts?
- How is the Achieved Security Level of each zone verified against its Target Security Level over time?

7.3 Evidence Checklist

Control Area	Evidence to Request
Governance	Governance charter; management review records
Asset Management	Current asset inventory export; last validation date
Risk Assessment	Risk register with per-zone SL-T rationale
Zones and Conduits	Zone/conduit diagram and register
Network Segmentation	Firewall rule sets; VLAN configuration
Remote Access	Remote access architecture diagram; session logs; MFA configuration
Identity & Access	Access review records; account/role mapping
Change Management	Sample change requests with approval trail (last 6–12 months)
Vulnerability Management	Current vulnerability register; remediation/compensating control tracking
Patch Management	Patch procedure documentation; vendor validation records
Backup & Recovery	Backup schedule; most recent test-restore record
Incident Response	IR plan; most recent tabletop exercise report
Physical Security	Cabinet access logs; physical walkthrough findings

7.4 Maturity Scoring Methodology

Shieldworkz uses a five-level maturity scale to score each control category, consistent with Appendix H:

Score	Level	Description
1	Initial / Ad Hoc	No formal process; reactive, undocumented, inconsistent
2	Developing	Basic process exists but inconsistently applied or documented
3	Defined	Documented, repeatable process consistently applied
4	Managed	Process is measured, reported, and reviewed at leadership level
5	Optimizing	Process is continuously improved based on metrics and lessons learned

7.5 Risk Rating Methodology

Findings are rated using a consequence-likelihood matrix, so that findings affecting safety-critical or high-consequence zones are prioritized appropriately regardless of their raw maturity score:

Consequence \ Likelihood	Low Likelihood	Medium Likelihood	High Likelihood
High Consequence (safety/environmental)	Medium Priority	High Priority	Critical Priority
Medium Consequence (production/financial)	Low Priority	Medium Priority	High Priority
Low Consequence	Low Priority	Low Priority	Medium Priority

7.6 Executive Reporting Template

Assessment reports should include the following sections, structured to serve both executive and technical audiences:

- Executive Summary: overall maturity posture, top risks, and business impact framing, in non-technical language.
- Scope and Methodology: sites, zones, and systems assessed, and the methodology summarized in Section 7.1.
- Maturity Scorecard: control category scores against the five-level model, presented visually (e.g., radar chart).

- Detailed Findings: each finding with supporting evidence, risk rating, and affected zone/conduit.
- Gap Analysis: current state vs. target Security Level per zone, and vs. applicable normative requirements.
- Prioritized Remediation Roadmap: findings sequenced by risk rating, with owners and target dates.
- Appendices: full evidence log and interview notes.

> **NOTICE**
> Recommendations in any assessment report should distinguish clearly between normative requirements the organization must meet under a specific target Security Level or applicable regulation, and Shieldworkz implementation guidance offered to accelerate improvement.

Section 8 — IEC 62443 Implementation Checklist

The checklist below consolidates the control categories from Section 5 into a practical, priority-ranked implementation reference. Priorities (Critical, High, Medium, Low) are Shieldworkz implementation guidance reflecting typical risk-reduction value observed across assessments, not a ranking defined by the standard itself; organizations should adjust priority based on their own risk assessment.

8.1 Governance and Policy

Item	Priority
Executive sponsorship and governance structure established	Critical
Security management system scope documented	High
Core policies (access, remote access, change mgmt) approved	High
Policy review cadence defined and followed	Medium

8.2 Asset Inventory and Risk Assessment

Item	Priority
Asset inventory covers majority of critical OT assets	Critical
Risk assessment methodology documented and applied per zone	Critical
Target Security Levels (SL-T) assigned with documented rationale	High
Inventory and risk assessment refreshed on a defined cycle	Medium

8.3 Network Segmentation and Architecture

Item	Priority
Zone/conduit model documented	Critical
IT/OT DMZ implemented with deny-by-default conduits	Critical
SIS network segmented from BPCS network	Critical

Item	Priority
Segmentation verified against actual firewall/VLAN configuration	High

8.4 Identity, Access, and Remote Access

Item	Priority
MFA enforced on all remote and administrative access	Critical
Individual accounts used wherever feasible; shared accounts compensated	High
Remote access routed through monitored jump host	Critical
Vendor access time-bound and logged	High

8.5 Endpoint and Controller Security

Item	Priority
Engineering workstations dedicated-use and hardened	High
PLC/controller logic baseline established and compared periodically	High
HMI accounts and screen-lock configuration reviewed	Medium
Endpoint protection validated with control system vendor before deployment	Medium

8.6 Patch, Vulnerability, and Configuration Management

Item	Priority
Vulnerability register maintained with remediation/compensating control tracking	High
Patch management process aligned to vendor validation and maintenance windows	High
Configuration baselines maintained and reconciled periodically	Medium
Change management process covers all control/safety logic changes	Critical

8.7 Backup, Recovery, and Monitoring

Item	Priority
Backups tested via restoration within the last 12 months	High
Passive OT network monitoring deployed at priority zone boundaries	High
Logs centralized with defined retention	Medium
Manual operating fallback procedures documented	Medium

8.8 Incident Response, Physical Security, and Compliance

Item	Priority
OT-specific incident response plan documented	Critical

Item	Priority
IR plan tested via tabletop exercise within last 12 months	High
Control cabinets and OT spaces physically secured	High
Applicable compliance frameworks identified and gap-assessed	High

8.9 Documentation, Training, and Continuous Improvement

Item	Priority
Zone/conduit and architecture documentation kept current	Medium
OT-relevant security awareness training delivered to engineers/operators	Medium
KPI reporting to leadership established (see Section 11)	Medium
Recurring assessment cadence established (see Section 7)	Medium

Section 9 — Managing Security During Incidents

This section presents an OT incident response framework aligned with IEC 62443 lifecycle principles, structured around the standard preparation-through-lessons-learned cycle.

9.1 The OT Incident Response Lifecycle

Preparation

Establish OT-aware incident response plans, playbooks, and trained response teams before an incident occurs, including pre-arranged contact with IACS vendors and applicable regulatory bodies.

Detection

Identify indicators of a potential incident through monitoring (Section 5.12), alerting, operator reports, or anomalous process behavior.

Analysis

Determine scope, root cause, and severity, with OT engineering involved from the outset alongside the security team, including assessment of impact on the zone's Achieved Security Level.

Containment

Limit the spread of the incident while preserving safety and, where possible, continuity of critical operations, evaluating any containment action's own operational and safety impact before execution.

Eradication

Remove the root cause and validate systems are clean before restoration, including verification of controller logic against a known-good baseline.

Recovery

Restore systems to normal operation using validated backups and configurations, with heightened monitoring during the recovery period.

Lessons Learned

Conduct a formal post-incident review, updating playbooks, policies, and the risk assessment/zone model based on findings.

9.2 Maintaining Safety and Operational Continuity

- No containment or eradication action should be taken without assessing its safety impact; safety systems should never be disabled as a response action without documented engineering and safety sign-off.
- Operations and engineering personnel must be part of the response team, not merely informed after the fact.

- Manual operating procedures should be activated where digital control is unavailable or untrusted during the incident.
- Regulatory reporting obligations and timelines (per applicable frameworks in Section 4) should be identified in advance, with designated owners.

9.3 Incident Response Playbooks

Playbook: Ransomware Affecting IT Systems with OT Dependency

- Assess which OT-dependent IT systems (engineering workstations, historians, domain controllers, patch servers) are affected.
- Consider controlled isolation of OT zones from affected IT segments per documented isolation procedures reviewed with operations.
- Activate manual operating procedures if supervisory/historian systems are unavailable or untrusted.
- Do not restore from backup until the initial access vector and persistence mechanisms are understood, to avoid reinfection.

Playbook: Suspected PLC / Controller Compromise

- Do not power-cycle or reprogram the controller until logic has been compared against the known-good baseline and, where feasible, forensically captured.
- Engage the controller vendor for platform-specific investigation support.
- Assess safety system interaction before any containment action; involve safety engineering explicitly.
- Restore from validated baseline following change management procedures if manipulation is confirmed.

Playbook: Unauthorized Remote Access Detected

- Immediately disable the affected remote access account/session and preserve session logs.
- Assess what systems and data the session accessed or could have accessed, in coordination with OT engineering.
- Reset credentials for any potentially exposed account and review for privilege escalation or lateral movement.
- Remediate the architectural gap that allowed unauthorized access (e.g., missing MFA) before restoring access.

Playbook: Malware Outbreak on the OT Network

- Identify affected systems via passive network monitoring and endpoint telemetry where available.
- Isolate affected zones while preserving safety-critical functions, coordinating with operations on isolation impact.
- Use offline/isolated media scanning stations to check removable media before reintroducing it to any cleaned system.
- Rebuild affected systems from known-good, validated images/backups rather than attempting in-place remediation on critical control systems.

Playbook: Insider Threat

- Engage HR and legal counsel early, in parallel with technical investigation, given the personnel dimension of insider incidents.

- Review access logs and change records for the individual's account across all zones they had access to, not only the suspected point of concern.
- Suspend or restrict access following documented procedures while investigation proceeds, balancing evidence preservation against ongoing operational risk.
- Review whether least-privilege and segregation-of-duties controls (Section 5.5) require strengthening as a result of the finding.

Playbook: Engineering Workstation Compromise

- Immediately disconnect the affected workstation from the network while preserving forensic evidence.
- Treat any logic pushed from the workstation since the estimated compromise window as untrusted; compare all downstream controller logic against baseline.
- Reset credentials associated with the workstation and review engineering software license server logs for unauthorized use.
- Rebuild the workstation from a known-good image before returning it to service, with updated hardening per Section 5.9.

Playbook: Vendor Credential Abuse

- Immediately disable the affected vendor account and preserve session/access logs.
- Assess scope of access the credential permitted across zones, and review all activity conducted during the suspected abuse window.
- Engage the vendor formally to determine whether the compromise originated on their side, and review the vendor risk assessment (Section 5.18) accordingly.
- Reissue credentials under strengthened controls (time-bound access, MFA) before restoring vendor access.

> **NOTICE**
> These playbooks are structural templates, not exhaustive procedures. Organizations should develop fully detailed, site-specific playbooks incorporating their actual zone/conduit architecture, vendor contacts, and regulatory obligations, and validate them through tabletop exercises.

Section 10 — Strengthening Shop Floor Security

This section translates the control categories in Section 5 into practical, floor-level guidance. All items are Shieldworkz implementation guidance intended to complement applicable IEC 62443 requirements, not restate them.

10.1 Physical Access Control

- Restrict access to control rooms, server rooms, and network closets to authorized personnel with logged entry.
- Extend physical security review to remote/unmanned sites (substations, pump stations, remote wellheads).

10.2 Control Cabinets

- Lock control cabinets containing PLCs, RTUs, and network equipment; log any access outside routine maintenance.
- Disable or physically secure unused programming ports on controllers within cabinets.

10.3 USB and Removable Media Policies

- Route all removable media through a dedicated, isolated scanning station before use on any OT system.
- Disable USB ports on HMIs and engineering workstations where not operationally required, or use port-control software.

10.4 Engineering Workstation Hardening

- Restrict engineering workstations to programming/configuration use only — no email, web browsing, or general office use.
- Apply vendor-validated OS patching and endpoint protection; maintain a current hardening baseline.

10.5 PLC and Controller Protection

- Enable controller-native authentication features where supported by the platform.
- Maintain a current, version-controlled logic baseline for comparison after any suspected incident.

10.6 HMI Security

- Use individually attributable accounts where operationally feasible; apply compensating controls where shared accounts remain necessary.
- Lock HMI screens automatically after inactivity consistent with operational safety requirements.

10.7 Industrial Switch Configuration

- Change default credentials on all managed switches; disable unused ports.
- Maintain current firmware on network devices per vendor guidance and organizational patch management process.

10.8 Wireless Security

- Use strong authentication (WPA2-Enterprise or better) for any Wi-Fi in or near OT zones; segment from wired OT networks.
- Inventory and assess proprietary industrial wireless (e.g., wireless HART) deployments for security configuration.

10.9 Vendor Access Management

- Require time-bound, request-based access grants for vendor personnel, both physical and remote.
- Maintain a current register of all active vendor access arrangements, reviewed periodically.

10.10 Secure Maintenance

- Require maintenance activity to follow the same change management and remote access controls as any other change.
- Log and review all maintenance-related access, whether physical or remote.

10.11 Backup and Recovery

- Maintain offline, tested backups of controller logic, HMI configuration, and engineering project files.

10.12 Operator Awareness

- Provide OT-relevant security awareness training to operators and maintenance staff, covering removable media, phishing, and incident reporting.

10.13 Secure Commissioning

- Apply the organization's change management and configuration baseline process to newly commissioned systems before they are connected to production networks.
- Change all default vendor credentials and disable unused services/ports as part of the commissioning checklist, before go-live.
- Validate that newly commissioned assets are captured in the asset inventory and assigned to the correct zone before production use.

10.14 Configuration Baselines

- Maintain and periodically reconcile configuration baselines for controllers, HMIs, and network devices against live systems.

10.15 Network Segmentation

- Verify segmentation is enforced in practice (firewall/VLAN rule review), not only documented on paper.

10.16 Industrial DMZ Implementation

- Route all data flows between IT and OT (patch distribution, historian replication, remote access) through the DMZ; disallow direct conduits between enterprise IT and OT supervisory zones.
- Deploy dedicated DMZ services (patch repository, AV update relay, jump host, historian mirror) rather than a simple pass-through firewall pair.
- Apply the same change management and monitoring rigor to DMZ systems as to OT systems, given their bridging role.

10.17 Shop Floor Quick-Reference Checklist

Area	Action Item	Priority
Physical	Control cabinets locked and access logged	High
Removable Media	Dedicated scanning station in use before any USB use on OT systems	High
Remote Access	All vendor remote sessions routed through monitored jump host with MFA	High
Engineering Workstations	Dedicated-use only, hardened, patched per vendor guidance	High
Network Devices	Default credentials changed; unused ports disabled	High
Commissioning	New assets follow commissioning checklist before production connection	High
Segmentation	Firewall/VLAN rules verified against documented zone/conduit model	Medium
Backups	Offline backup of logic/config validated via test restore in last 12 months	Medium
Wireless	Strong authentication and segmentation verified for all site wireless	Medium
Awareness	Operators trained on removable media and phishing risks in last 12 months	Medium

Section 11 — KPIs and Metrics

The KPIs below provide a starting framework for measuring IEC 62443 program effectiveness at both executive and operational levels. Target values are illustrative and should be set by each organization based on its own risk tolerance and maturity trajectory; they are not normative requirements of the standard.

11.1 Governance Maturity

Attribute	Detail
Definition	Aggregate maturity score of governance-related control categories against the five-level model.
Formula	Weighted average of governance-related maturity scores (Appendix H)
Data Source	Internal assessment / Section 7 methodology
Reporting Frequency	Annual
Target Threshold (illustrative)	Organization-defined target maturity level
Executive Interpretation	Indicates whether accountability and management commitment are keeping pace with technical implementation
Dashboard Visualization	Radar/spider chart alongside other domain scores

11.2 Asset Inventory Completeness

Attribute	Detail
Definition	Proportion of known OT assets captured in the current inventory.
Formula	(# assets in inventory / # assets identified via independent validation) x 100
Data Source	Asset inventory system, passive discovery tool, physical walkthrough records
Reporting Frequency	Quarterly
Target Threshold (illustrative)	Organization-defined; commonly cited industry aspiration is above 95%, though this is Shieldworkz guidance, not a standards mandate
Executive Interpretation	Low completeness signals blind spots undermining the zone/conduit risk assessment

Attribute	Detail
Dashboard Visualization	Gauge or trend line by site

11.3 Risk Assessment Currency

Attribute	Detail
Definition	Proportion of zones with a risk assessment and SL-T assignment reviewed within the defined cycle.
Formula	(# zones with current risk assessment / total zones) x 100
Data Source	Risk register
Reporting Frequency	Annual
Target Threshold (illustrative)	Organization-defined, ideally full coverage
Executive Interpretation	Stale risk assessments may not reflect current threat landscape or architecture
Dashboard Visualization	Scorecard by zone

11.4 Vulnerability Remediation / Compensating Control Rate

Attribute	Detail
Definition	Proportion of identified vulnerabilities remediated or covered by an approved compensating control within target timeframe.
Formula	(# vulnerabilities remediated or compensated within SLA / total identified) x 100
Data Source	Vulnerability management register
Reporting Frequency	Monthly
Target Threshold (illustrative)	Organization-defined SLA, typically tiered by severity
Executive Interpretation	Persistent backlog signals under-resourced vulnerability management
Dashboard Visualization	Stacked bar by severity tier

11.5 Patch Currency

Attribute	Detail
Definition	Proportion of in-scope OT systems on a vendor-validated current patch level.
Formula	(# systems at current validated patch level / total in-scope systems) x 100
Data Source	Patch management system, asset inventory
Reporting Frequency	Quarterly
Target Threshold (illustrative)	Organization-defined, reflecting vendor validation cycles
Executive Interpretation	Low currency may be unavoidable for legacy systems; should correlate with compensating controls
Dashboard Visualization	Trend line with vendor-support-status overlay

11.6 Compliance / Framework Alignment Score

Attribute	Detail
Definition	Aggregate maturity score against the organization's applicable compliance frameworks (see Section 4).
Formula	Weighted average of control maturity scores across applicable framework requirements
Data Source	Internal assessment or external audit results
Reporting Frequency	Annual, or per audit cycle
Target Threshold (illustrative)	Organization-defined target maturity level
Executive Interpretation	Provides an executive-level proxy for audit/regulatory readiness
Dashboard Visualization	Radar/spider chart by framework domain

11.7 Network Segmentation Coverage

Attribute	Detail
Definition	Proportion of defined zone boundaries with verified, enforced conduits matching the documented model.
Formula	(# boundaries with verified enforcement / total defined boundaries) x 100
Data Source	Firewall/VLAN configuration audit
Reporting Frequency	Semi-annual
Target Threshold (illustrative)	Organization-defined based on risk assessment
Executive Interpretation	Gaps indicate potential lateral movement paths between zones
Dashboard Visualization	Heat map by zone boundary

11.8 Security Level Achievement Rate

Attribute	Detail
Definition	Proportion of zones where the Achieved Security Level (SL-A) meets or exceeds the Target Security Level (SL-T).
Formula	(# zones with SL-A >= SL-T / total zones with an assigned SL-T) x 100
Data Source	Periodic SL-A reassessment records
Reporting Frequency	Annual
Target Threshold (illustrative)	Organization-defined, ideally full coverage
Executive Interpretation	A core IEC 62443-specific indicator of whether the program is delivering its intended protection level
Dashboard Visualization	Scorecard by zone, colored by gap size

11.9 Incident Response Readiness

Attribute	Detail
Definition	Proportion of planned tabletop/functional exercises completed within the reporting period.
Formula	(# exercises completed / # exercises planned) x 100
Data Source	Incident response program records
Reporting Frequency	Annual
Target Threshold (illustrative)	Organization-defined, ideally full completion of planned exercise calendar
Executive Interpretation	Low completion indicates untested response capability
Dashboard Visualization	Simple scorecard

11.10 Mean Time to Detect (MTTD)

Attribute	Detail
Definition	Average elapsed time between an incident's occurrence and its detection.
Formula	Sum of (detection time − occurrence time) across incidents / number of incidents
Data Source	SOC/SIEM incident records
Reporting Frequency	Quarterly (rolling)
Target Threshold (illustrative)	Organization-defined; trend should show improvement over time
Executive Interpretation	Declining MTTD indicates improving monitoring and detection maturity
Dashboard Visualization	Trend line, rolling average

11.11 Mean Time to Respond (MTTR)

Attribute	Detail
Definition	Average elapsed time between detection and containment of an incident.

Attribute	Detail
Formula	Sum of (containment time − detection time) across incidents / number of incidents
Data Source	Incident response records
Reporting Frequency	Quarterly (rolling)
Target Threshold (illustrative)	Organization-defined; trend should show improvement over time
Executive Interpretation	Declining MTTR indicates improving response readiness
Dashboard Visualization	Trend line, rolling average

11.12 Backup Success Rate

Attribute	Detail
Definition	Proportion of scheduled backup restoration tests completed successfully.
Formula	(# successful test restores / total scheduled test restores) x 100
Data Source	Backup/DR test records
Reporting Frequency	Semi-annual
Target Threshold (illustrative)	Organization-defined, ideally full coverage of critical systems
Executive Interpretation	Low success rate indicates recovery time risk during an actual incident
Dashboard Visualization	Simple scorecard by critical system

11.13 Third-Party Risk Coverage

Attribute	Detail
Definition	Proportion of active vendors with OT access that have completed a current risk assessment.
Formula	(# vendors assessed within policy cycle / total active vendors with OT access) x 100

Attribute	Detail
Data Source	Vendor risk register
Reporting Frequency	Annual
Target Threshold (illustrative)	Organization-defined
Executive Interpretation	Gaps indicate unmanaged third-party risk exposure
Dashboard Visualization	Scorecard by vendor tier

11.14 Security Awareness Training Completion

Attribute	Detail
Definition	Proportion of in-scope OT personnel who completed OT-relevant security awareness training within the defined cycle.
Formula	(# personnel trained / total in-scope personnel) x 100
Data Source	Training/LMS records
Reporting Frequency	Annual
Target Threshold (illustrative)	Organization-defined, ideally full coverage
Executive Interpretation	Low completion correlates with elevated risk from removable media and phishing vectors
Dashboard Visualization	Gauge by site/role

11.15 Operational Resilience Index

Attribute	Detail
Definition	Composite indicator combining backup success rate, manual fallback procedure currency, and IR exercise completion.
Formula	Organization-defined weighted composite of the three underlying metrics
Data Source	Backup/DR, business continuity, and IR program records

Attribute	Detail
Reporting Frequency	Annual
Target Threshold (illustrative)	Organization-defined
Executive Interpretation	Provides a single executive-level proxy for the organization's ability to withstand and recover from a significant OT incident
Dashboard Visualization	Single composite gauge with drill-down to underlying metrics

IMPLEMENTATION ADVICE

Shieldworkz recommends limiting executive dashboards to 6–8 KPIs that map directly to business risk and Security Level achievement, reserving the full KPI set for operational/program-management reporting.

Section 12 — Common Audit Findings and Best Practices

12.1 Common Implementation Gaps

Finding	Typical Root Cause	Recommended Remediation
Zone/conduit diagrams do not match actual network configuration	Diagrams created for a single assessment and never maintained as architecture changes	Establish a change process that updates zone/conduit documentation as part of any network change
Target Security Levels assigned without documented rationale	SL-T values estimated informally rather than derived from a structured risk assessment	Apply the 62443-3-2 risk assessment methodology consistently and document consequence/likelihood rationale per zone
Remote access lacks MFA on legacy or vendor-managed paths	Vendor tooling predates organizational MFA policy; exception never revisited	Extend MFA requirement contractually to all vendor remote access; treat as a critical-priority gap
Asset inventory incomplete for serial/air-gapped devices	Reliance on passive network discovery alone	Combine passive discovery with physical walkthroughs and engineering documentation review
No baseline for controller logic comparison	Baseline capture never established as a standard practice	Capture and version-control a known-good baseline for all critical controllers
Incident response plan is IT-focused and untested for OT scenarios	IR planning conducted by IT security without OT engineering involvement	Develop OT-specific playbooks (Section 9) and test via tabletop exercises with engineering/operations
Patch management applies IT timelines to OT without vendor validation	IT-standard patch policy extended to OT without adaptation	Establish a distinct OT patch management process aligned to vendor validation and maintenance windows

12.2 Frequent Audit Findings by Control Category

- Governance: steering committee exists on paper but does not meet on a defined cadence.
- Asset Management: inventory age exceeds the organization's own defined refresh cycle.
- Network Segmentation: documented segmentation does not match live firewall/VLAN rule configuration.
- Access Management: shared operator or administrative accounts persist without compensating controls.
- Change Management: emergency changes made verbally and never retroactively documented.
- Vulnerability Management: findings tracked but never closed or formally accepted as residual risk with compensating controls.
- Physical Security: control cabinets found unlocked during site walkthroughs.

12.3 Root Causes Observed Across Industrial Environments

Across manufacturing, energy, water, and pharmaceutical assessments, Shieldworkz consistently traces recurring findings to a small number of underlying root causes: documentation created once for a specific audit or assessment and never subsequently maintained as a living artifact; controls implemented without genuine engineering/operations buy-in, leading to informal workarounds; and security programs sequenced to implement advanced capabilities (e.g., monitoring or active testing) before completing foundational asset visibility and governance.

12.4 Best Practices for Maintaining Compliance

- Treat zone/conduit diagrams, asset inventory, and risk assessments as living documents updated through the same change management process used for the underlying systems, not as static assessment deliverables.
- Build cross-functional governance (Section 5.1) so that IT security and OT engineering jointly own compliance evidence, rather than IT security collecting evidence in isolation.
- Schedule recurring internal assessments (Section 7) between formal external audits or certification cycles to catch drift early.
- Map overlapping requirements across applicable frameworks (Section 4) to a single internal control set so one implemented control can evidence multiple obligations.
- Close the loop on every audit finding with a documented remediation owner and target date, tracked to closure rather than left open indefinitely.

> **IMPLEMENTATION ADVICE**
>
> Shieldworkz's field experience indicates that organizations which schedule a lightweight internal self-assessment roughly midway between formal audit cycles catch and remediate significantly more findings proactively than those that only assess at audit time.

Section 13 — Illustrative Case Study

> **NOTICE**
> This case study is a composite, illustrative scenario constructed by Shieldworkz from patterns commonly observed across multiple client engagements. It does not describe any specific, identifiable organization, and all figures are illustrative rather than drawn from a single real assessment.

13.1 Background

A mid-sized municipal water treatment operator ('the Utility') operates three treatment facilities and a network of pump stations serving approximately 250,000 residents. Following a sector-wide advisory regarding intrusion attempts against water utility HMIs, the Utility's leadership commissioned an IEC 62443-aligned assessment to establish its current OT security posture and a remediation roadmap.

13.2 Initial OT Security Posture

- No formal OT security governance structure; OT security decisions made ad hoc by the SCADA engineering lead.
- Asset inventory existed but covered only PLCs and HMIs at the main treatment facility — pump station RTUs and network devices were undocumented.
- Flat network architecture: the corporate network, SCADA supervisory systems, and PLCs shared a single VLAN at two of the three facilities.
- Vendor remote access maintained via an always-on VPN connection with a shared account and no MFA.
- No documented incident response plan specific to OT; general IT incident response plan did not address SCADA scenarios.

13.3 Assessment Process

Shieldworkz applied the methodology described in Section 7: scope definition covering all three facilities and the pump station network, stakeholder interviews with SCADA engineers, operations managers, and IT security staff, a documentation review, site walkthroughs at each facility, and technical validation of segmentation (network configuration review, not active penetration testing, given the utility's risk tolerance for the initial assessment).

13.4 Key Findings

Finding	Risk Rating
Flat network with no segmentation between corporate IT and SCADA at two facilities	Critical

Finding	Risk Rating
Vendor remote access via always-on VPN, shared account, no MFA	Critical
Incomplete asset inventory (pump station RTUs undocumented)	High
No documented OT-specific incident response plan	High
No controller logic baseline for comparison after incidents	Medium
Control cabinets at two pump stations found unlocked during walkthrough	Medium
No formal risk assessment or Target Security Level assignment for any zone	High

13.5 Gap Analysis and Risk Prioritization

Applying the consequence-likelihood matrix from Section 7.5, the flat network architecture and ungoverned vendor remote access were jointly rated Critical Priority given high consequence (potential to affect water treatment chemical dosing, a safety and public health concern) combined with medium-to-high likelihood (both vectors are commonly implicated in publicly documented water sector incidents). The incomplete asset inventory and absent incident response plan were rated High Priority as foundational gaps undermining every subsequent control.

13.6 Remediation Roadmap

Phase	Key Actions	Timeframe
Immediate (0–30 days)	Disable always-on vendor VPN; implement time-bound access with MFA; lock all control cabinets	30 days
Phase 1: Discover (0–6 months)	Complete asset inventory across all facilities and pump stations; establish OT security governance	6 months
Phase 2: Protect (4–14 months)	Implement network segmentation (IT/OT DMZ) at all three facilities; formalize risk assessment and SL-T assignment per zone	14 months
Phase 3: Detect (10–18 months)	Deploy passive monitoring at SCADA supervisory zone boundaries	18 months
Phase 4: Respond (14–20 months)	Develop and exercise OT-specific incident response playbooks	20 months
Phase 5: Improve (18–24 months)	Establish recurring internal assessment cadence; begin KPI reporting to the utility board	24 months

13.7 Illustrative KPI Improvements (24-Month Horizon)

KPI	Baseline	24-Month Target
Asset Inventory Completeness	~40% (main facility only)	>90% across all sites
Network Segmentation Coverage	0% (flat network at 2 of 3 facilities)	100% of defined zone boundaries verified
Remote Access Governance	0% (always-on, no MFA)	100% time-bound sessions with MFA
Incident Response Readiness	0 exercises conducted	Annual tabletop exercise cycle established
Security Level Achievement Rate	Not assessed (no SL-T assigned)	SL-T assigned for all zones; SL-A verified for supervisory and control zones

13.8 Lessons Learned

- Flat network architecture and ungoverned vendor access were both long-standing, informally accepted risks — neither had been previously assessed against a structured risk methodology.
- Engaging SCADA engineering staff directly in the assessment (rather than relying on IT security documentation alone) surfaced the undocumented pump station assets that passive network discovery alone would have missed.
- Immediate, low-cost actions (disabling the always-on VPN, locking cabinets) delivered meaningful risk reduction within 30 days, ahead of the longer segmentation and monitoring roadmap — illustrating the value of sequencing quick wins alongside the multi-year program.
- Board-level KPI reporting, introduced in Phase 5, gave the utility's leadership a sustained mechanism for tracking progress beyond the initial assessment engagement.

Section 14 — Appendices

Appendix A — IEC 62443 Assessment Checklist

#	Item	Status (Y/N/Partial)
A1	OT security governance structure established with executive sponsorship	
A2	Current, validated OT asset inventory exists	
A3	Risk assessment methodology documented and applied per zone	
A4	Zone/conduit model documented with assigned target Security Levels	
A5	IT/OT DMZ implemented with deny-by-default conduit rules	
A6	SIS network segmented from BPCS network	
A7	All remote access routed through monitored jump host with MFA	
A8	Engineering workstations dedicated-use, hardened, and access-controlled	
A9	Formal change management process covers all control/safety logic changes	
A10	Vulnerability register maintained with remediation/compensating control tracking	
A11	Patch management aligned to vendor validation and maintenance windows	
A12	Backups tested via restoration within the last 12 months	
A13	OT-specific incident response plan exists and has been exercised	
A14	Vendor/third-party access governed by formal, time-bound agreements	
A15	Achieved Security Level periodically reverified against Target Security Level	

Appendix B — Shop Floor Security Checklist

#	Item	Status (Y/N/Partial)
B1	Control cabinets locked with logged access	
B2	Removable media scanned at a dedicated station before OT use	
B3	Default credentials changed on all network devices	
B4	Unused network ports and controller programming ports disabled	
B5	Wireless networks in/near OT zones use strong authentication and are segmented	
B6	HMI screens lock after inactivity consistent with safety requirements	
B7	Controller logic baseline maintained and compared periodically	
B8	Vendor remote maintenance sessions logged and time-bound	
B9	Newly commissioned assets follow the commissioning checklist before production use	
B10	Operators trained on removable media and phishing risks in last 12 months	

Appendix C — Incident Response Checklist

Phase	Key Actions
Preparation	IR plan documented; playbooks current; contact list for vendors/regulators maintained; roles assigned
Detection	Monitoring alerts and operator reports triaged promptly; initial severity assessment made
Analysis	Scope and root cause assessed with OT engineering involvement; safety implications reviewed
Containment	Containment actions safety-reviewed before execution; operations informed and involved
Eradication	Root cause removed; controller logic verified against baseline before returning to service
Recovery	Systems restored from validated backups; heightened monitoring during recovery period
Lessons Learned	Post-incident review conducted; playbooks, controls, and risk assessment updated

Appendix D — Asset Inventory Template

Field	Description
Asset ID	Unique internal identifier
Asset Name / Tag	Site-standard equipment tag or name
Asset Type	PLC, RTU, HMI, engineering workstation, historian, network device, SIS, etc.
Vendor / Manufacturer	Original equipment manufacturer
Model	Model number/designation
Firmware / Software Version	Current installed version
Zone	Assigned zone per the zone/conduit model
Physical Location	Site, building, cabinet/panel reference
IP Address / Network ID	If applicable
Criticality Rating	Safety-critical / production-critical / supporting, per risk assessment
Support Status	Vendor-supported / end-of-life / unsupported
Last Validated Date	Date the record was last physically or technically confirmed

Appendix E — Vendor Risk Assessment Template

#	Item
E1	Does the vendor require remote access, and if so, does it comply with the organization's secure remote access policy?
E2	Does the vendor's product/service conform to IEC 62443-4-1/4-2 or an equivalent secure-development standard, where applicable?
E3	Does the vendor have a documented vulnerability disclosure and patch notification process?
E4	Is there a documented software/firmware bill of materials available for critical components?
E5	Has the vendor's access to the organization's OT environment been logged and reviewed within the last 12 months?
E6	Does the vendor contract include security requirements and audit rights?
E7	Is there a named security point of contact at the vendor for incident coordination?

Appendix F — Compliance Matrix (Illustrative Cross-Framework Mapping)

This matrix illustrates, at a high level, which frameworks address similar control domains as IEC 62443. It is a starting orientation tool, not a certified equivalence mapping — organizations should validate specific clause-level alignment with qualified compliance resources before relying on it for formal conformity claims.

Control Domain	IEC 62443	NIST SP 800-82 Rev.3 / CSF 2.0	ISO/IEC 27001	NERC CIP
Governance / Management System	62443-2-1	CSF 2.0 Govern function	Clause 5–7 (leadership, planning, support)	CIP-003
Risk Assessment	62443-3-2	SP 800-82 risk guidance / CSF Identify	Clause 6.1 / Annex A risk controls	CIP-002 (BES Cyber System categorization)
Network Segmentation	62443-3-2 / 3-3 (zones/conduits)	SP 800-82 architecture guidance	Annex A network security controls	CIP-005 (Electronic Security Perimeter)
Access Control	62443-3-3 / 4-2 (FR 1, FR 2)	SP 800-53 AC family (via SP 800-82)	Annex A access control	CIP-004 / CIP-007
Incident Response	62443-2-1	SP 800-61 / CSF Respond	Annex A incident management	CIP-008
Patch/Vulnerability Management	62443-2-3	SP 800-82 guidance / CSF Protect	Annex A technical vulnerability mgmt	CIP-007 (patch management)

Appendix G — Sample RACI Matrix

Activity	CISO	OT Security Mgr	Plant/Ops Mgr	Control Sys Engineer	SOC
OT security governance	A	R	C	C	I
Zone/conduit definition and SL-T assignment	C	A	I	R	I
Asset inventory maintenance	I	A	C	R	I
Network segmentation design	C	A	I	R	I
Remote access approval	I	A	R	C	I
Change management (control logic)	I	C	A	R	I
Vulnerability management	I	A	C	R	C
Incident detection & triage	I	C	I	C	A/R
Incident response execution	A	R	R	R	R
Compliance reporting	A	R	C	I	I
KPI reporting to leadership	A	R	I	I	C

R = Responsible, A = Accountable, C = Consulted, I = Informed. This matrix is a starting template; roles and titles should be adapted to the organization's actual structure.

Appendix H — OT Security Maturity Model

Level	Name	Description
1	Initial / Ad Hoc	No formal OT security process; reactive; undocumented; dependent on individual knowledge
2	Developing	Basic processes exist but are applied inconsistently across sites or teams
3	Defined	Documented, repeatable processes consistently applied across the organization
4	Managed	Processes are measured, reported to leadership, and resourced accordingly
5	Optimizing	Processes are continuously refined using metrics, incident lessons, and threat intelligence

Appendix I — Glossary of IEC 62443 and OT Cybersecurity Terms

Term	Definition
Achieved Security Level (SL-A)	The Security Level that a zone, conduit, or system actually delivers as implemented and configured.
Basic Process Control System (BPCS)	The control system responsible for routine, non-safety process control functions.
Capability Security Level (SL-C)	The Security Level a component or system is capable of supporting when properly configured.
Conduit	A logical grouping of communication channels connecting two or more zones, through which security requirements for that connection are defined.
Cyber-Physical System (CPS)	A broader engineering term for systems where computational elements are tightly integrated with physical processes; OT/ICS is a subset of CPS.
Defense-in-Depth	A layered security approach using multiple, independent controls so that failure of any single control does not result in compromise.
Distributed Control System (DCS)	A control architecture distributing control functions across controllers close to the process, typically within a single site.
Engineering Workstation	A computer running vendor software used to configure and program controllers and safety systems.
Foundational Requirement (FR)	One of the seven high-level requirement categories defined in the IEC 62443-3-3/4-2 system and component technical requirements (e.g., identification and authentication control, use control).
Historian	A database system that logs process data over time for trending, reporting, and analysis.
Human-Machine Interface (HMI)	The graphical interface through which operators monitor and control industrial processes.
Industrial Automation and Control System (IACS)	IEC 62443's term for personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.
Industrial Control System (ICS)	An umbrella term for control system types including SCADA, DCS, and PLC-based systems, plus associated instrumentation.
Programmable Logic Controller (PLC)	An industrial computer that executes control logic to operate field devices based on sensor input.

Term	Definition
Purdue Enterprise Reference Architecture (PERA)	A conceptual model segmenting industrial environments into hierarchical levels for architecture and security planning.
Remote Terminal Unit (RTU)	A field device that interfaces with sensors/actuators and communicates data to a SCADA master.
Safety Instrumented System (SIS)	An independent system designed to bring a process to a safe state upon detection of unsafe conditions.
Security Level (SL)	An IEC 62443 concept describing the degree of protection required or achieved against a defined threat capability, rated 1 (lowest) to 4 (highest).
Security Management System (per 62443-2-1)	The organizational policies, processes, and procedures an asset owner establishes to manage IACS cybersecurity risk.
Supervisory Control and Data Acquisition (SCADA)	A system providing centralized monitoring and control over geographically dispersed industrial assets.
Target Security Level (SL-T)	The Security Level an organization determines it needs for a given zone or conduit, based on risk assessment.
Zone	A grouping of logical or physical assets sharing common security requirements, per the IEC 62443 zone/conduit model.

Appendix J — Acronyms

Acronym	Meaning
BES	Bulk Electric System
BPCS	Basic Process Control System
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency (U.S.)
CPS	Cyber-Physical System
CRA	Cyber Resilience Act (EU)
CSF	Cybersecurity Framework
DCS	Distributed Control System

Acronym	Meaning
DMZ	Demilitarized Zone
ECC	Essential Cybersecurity Controls (Saudi NCA)
ENISA	European Union Agency for Cybersecurity
FR	Foundational Requirement (IEC 62443)
HMI	Human-Machine Interface
IACS	Industrial Automation and Control Systems
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
ISA	International Society of Automation
ISMS	Information Security Management System
MFA	Multi-Factor Authentication
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond
NCA	National Cybersecurity Authority (Saudi Arabia)
NERC	North American Electric Reliability Corporation
NIS2	Network and Information Security Directive 2 (EU)
NIST	National Institute of Standards and Technology (U.S.)
OT	Operational Technology
OTCC	Operational Technology Cybersecurity Controls (Saudi NCA)
PERA	Purdue Enterprise Reference Architecture
PLC	Programmable Logic Controller

Acronym	Meaning
RACI	Responsible, Accountable, Consulted, Informed
RMF	Risk Management Framework
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIS	Safety Instrumented System
SL	Security Level (IEC 62443)
SL-A	Achieved Security Level
SL-C	Capability Security Level
SL-T	Target Security Level
SOC	Security Operations Center

Appendix K — References to Authoritative Publications

IEC 62443 series (all parts), International Electrotechnical Commission / International Society of Automation.

ISA/ISA99 committee guidance and technical reports, International Society of Automation.

NIST Special Publication 800-82 Revision 3, Guide to Operational Technology (OT) Security, National Institute of Standards and Technology.

NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology.

NIST Special Publication 800-37, Risk Management Framework for Information Systems and Organizations.

NIST Special Publication 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations.

NIST Special Publication 800-61, Computer Security Incident Handling Guide.

NERC Critical Infrastructure Protection (CIP) Standards, North American Electric Reliability Corporation.

ISO/IEC 27001, Information Security Management Systems — Requirements.

ISO/IEC 27019, Information Security Controls for the Energy Utility Industry.

Directive (EU) 2022/2555 (NIS2 Directive), European Union.

Regulation (EU) 2024/2847 (Cyber Resilience Act), European Union.

Essential Cybersecurity Controls (ECC) and Operational Technology Cybersecurity Controls (OTCC), Saudi National Cybersecurity Authority.

UAE Information Assurance Regulations, UAE Cyber Security Council / Telecommunications and Digital Government Regulatory Authority.

CISA Industrial Control Systems advisories and guidance, Cybersecurity and Infrastructure Security Agency.

ENISA Industrial Control Systems and OT security guidance publications, European Union Agency for Cybersecurity.

About Shieldworkz

Shieldworkz is a specialist OT/ICS cybersecurity firm with an NDR solution and AI-based tools for securing SCADA, PLCs and Cyber Physical Systems. We serve critical infrastructure operators, industrial organisations, and government entities across the energy, oil and gas, manufacturing, utilities, transport, and defence sectors.

Our service areas include OT security assessments (powered by OThello Assess with sub-24-hour assessment cycles), NIS2 and IEC 62443 compliance programmes, OT threat intelligence advisories, OT SOC design and implementation, and regulatory readiness engagements for NCA (Saudi OTCC/ECC), NERC CIP, SOCI, and Singapore Cybersecurity Act obligations.

NDR Solution: shieldworkz.com/products/ot-security-platform **| Media Scan:** shieldworkz.com/products/ot-security- **| Othello Assess:** shieldworkz.com/othello/assess **| Patch Management:** shieldworkz.com/products/patch-management-solution **| Regulatory Playbooks:** shieldworkz.com/regulatory-playbooks **| Remediation Guides:** shieldworkz.com/remediation-guides **| Reports:** shieldworkz.com/reports

About Shieldworkz

ISOC and Honeypot Locations

Honeypot Locations

Security Operations Center

Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

Secure Your Industrial Future

Talk to us today!

From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.

Contact Us

Fritz-Schäffer-Street 1,
4th floor

Bonn, 53113, Germany

+49 (0) 228 / 929 39210

europe@shieldworkz.com

396 Old Colony Road
Richmond Hill,
ON L4E 5A5 Canada

+1 (437) 223-7770

americas@shieldworkz.com

Tenth floor,

Abu Dhabi,
United Arab Emirates,
FAB Business Center

+971 56 660 5200

middleeast@shieldworkz.com

Gopalan Signature Tower,
No 6, 2nd Floor, Old Madras
Road, Benniganahalli

Bengaluru,
Karnataka 560093

+91 9059620557

apac@shieldworkz.com