Cybersecurity for Industrial Systems

A Practical Guide to Protect

OT, ICS, and SCADA Environments

Houari OUCIF

This book addresses industrial systems cybersecurity for education and awareness purposes. The examples, scenarios, and recommendations presented must be adapted to the specific context of each organization.

The author disclaims any liability arising from inappropriate use of the information contained in this work.

Contents

Preface

The digital transformation of industrial environments has profoundly changed the way production systems are designed, supervised, and operated. The growing interconnection between information technology (IT) and operational technology (OT) now makes it possible to improve plant performance, remote supervision, maintenance, and the operation of industrial processes. However, this evolution is accompanied by a significant increase in cyber risks, which must now be taken into account alongside availability, safety, and business continuity constraints.

Unlike traditional information systems, industrial environments rely on equipment and architectures that are often designed to operate for long periods, with high requirements for stability and reliability. A poorly controlled change, an unsuitable patch, or a service interruption can have significant consequences for production, people's safety, or the integrity of facilities. Industrial systems cybersecurity therefore requires a tailored approach that takes into account the technical, operational, and organizational constraints specific to OT.

This book offers a progressive and structured approach to industrial cybersecurity. Its purpose is to provide clear guidance for understanding the differences between IT and OT, identifying the main attack surfaces, understanding the threats, and implementing protection measures suited to the industrial context. The goal is to provide an operational perspective that helps better integrate cybersecurity into projects, operations, and the governance of industrial systems.

This work draws on widely recognized best practices from international frameworks such as IEC 62443, NIST SP 800-82, and recommendations from organizations specialized in securing industrial environments. It is neither a standard nor a formal standard, but rather a guide intended to make the essential concepts easier to understand and to support their practical implementation.

This book is intended for engineers, technical managers, IT/OT specialists, cybersecurity managers, students, and decision-makers who want to better understand the challenges of industrial cybersecurity. It provides an accessible guide without oversimplifying the issues, helping readers identify improvement paths suited to their own context.

Industrial cybersecurity is an ongoing process that unfolds over time. The purpose of this book is to provide a solid foundation for structuring a coherent approach, asking the right questions, and progressively strengthening the security posture of OT environments.

Who Is This Book For?

This book is intended for anyone who needs to understand, manage, or secure industrial environments (OT – Operational Technology), without necessarily being an automation specialist at the outset. Its goal is to provide you with a common

language and a method for making security decisions that are consistent with industrial constraints.

It is particularly useful if you are:

- An IT professional (systems, networks, cloud, cybersecurity) discovering OT and its operating constraints (24/7 availability, safety, operations, long life cycles),
- An OT / operations / maintenance manager looking to structure a realistic cybersecurity approach that is compatible with production requirements,
- A CISO / cybersecurity manager / risk manager working in industrial sectors (industry, energy, transport, water) or on sites with strong operational constraints,
- A project manager / compliance manager (NIS2, IEC 62443, ISO 27001, contractual requirements) needing a clear view of the frameworks and how they apply in an OT context,
- A student or someone transitioning into industrial cybersecurity roles.

Expected Level and Prerequisites

No prior automation background is required to get started.

The book is structured progressively. To get the most out of it, it is recommended that you:

- Know the basics of networks and systems (IP addressing, segmentation, firewall concepts, authentication),
- Have a general understanding of cybersecurity (threats, vulnerabilities, access management), even a basic one.

If some terms are unfamiliar to you, Part I lays the foundations and will allow you to follow along without difficulty. The more technical concepts (industrial protocols, architecture, frameworks) are introduced progressively.

Defensive Use and Legal Framework

This work is designed for defensive purposes: understanding risk, improving the security of industrial systems, and supporting decision-making. The examples and scenarios presented are aimed at risk management and the protection of OT environments. They must be applied in compliance with the laws, regulations, and internal policies of your organization. No part of this book is intended to provide instructions for illegal intrusion or malicious use.

Reading Methodology and Learning Features

This book is designed to help readers understand industrial systems cybersecurity. It provides conceptual, methodological, and practical reference points for

understanding the specific challenges of OT environments, without limiting itself to a purely standards-based or technology-driven approach.

It does not replace a risk analysis, a compliance audit, or the contractual and regulatory documents applicable to your organization. The examples and recommendations presented must be adapted to your context (sector, criticality, operating constraints, functional safety requirements, etc.).

You can read this book in two ways:

- Sequential reading (recommended): start with Part I in order to acquire the vocabulary, the IT/OT differences, and the key concepts. You will then have a common foundation for approaching the risk management, technical measures, and governance presented afterward,
- Goal-oriented reading: if you already have experience in OT or cybersecurity, you can navigate directly to the parts that meet your needs (frameworks, threats, architecture, best practices). Each chapter is designed to remain relatively understandable on its own.

Reading guide

- “Chapter objectives”: what you will be able to do or understand by the end of the chapter,
- “Key takeaways”: a summary of the key points to remember.
- “Self-assessment”: questions to validate your understanding and identify points to review.
- “Micro-cases”: short field-inspired scenarios (context + guided question(s)) to apply the concepts immediately; an answer key or suggested answers are provided in the appendices of each part.
- “Further reading”: resources and references for deeper study.

With this in mind, some chapters conclude with a self-assessment section. These self-assessments encourage active engagement with the concepts: they invite the reader to step back and reflect on the key notions, the underlying risks, and the operational implications. They are neither academic tests nor exhaustive questionnaires, but reflection prompts intended to strengthen the overall understanding of the topics covered.

The suggested answers are grouped at the end of the part in which the relevant chapter appears, within the dedicated appendix (for example: Appendix I-B for Part I). They are provided for guidance only: each industrial system has its own technical, organizational, and regulatory constraints, which must be taken into account in any cybersecurity approach.

Readers are free to use these features as needed: as a verification tool, as a discussion aid, or as a starting point for exploring certain aspects more deeply in their own industrial context.

PART I

Foundations and Essential Threats: Understanding Industrial Systems, Threats, and Blind Spots

General Introduction

Industrial systems (OT) now play a central role in the operation of critical infrastructure and, more broadly, in our modern societies. Whether it involves producing and distributing energy, treating water, operating industrial processes, managing logistics chains, or ensuring the continuity of essential services, these environments rely on specialized technologies—programmable logic controllers, industrial networks, supervisory systems, sensors, actuators—closely tied to continuous and sensitive physical processes.

Historically, these systems were designed for availability, stability, and safety. Cybersecurity was not a design objective, and separation from information systems (IT) was often considered a sufficient barrier. Today, the modernization of plants, the integration of business layers (MES/ERP), remote maintenance, and the adoption of cloud/IIoT solutions have transformed operational reality: exchanges between IT and OT environments have multiplied, and compromise scenarios must be analyzed across the entire industrial system and its ecosystem (service providers, supply chains, remote access).

Five key points to keep in mind before going further

1. The air gap (physical isolation) is rarely real: indirect paths exist (remote access, business flows, maintenance, removable media).
2. IT/OT convergence increases exposure: more interconnections mean more potential attack paths.
3. The OT attack surface is often inherited from legacy design choices: long life cycles, difficult patching, dependencies, and technological heterogeneity.
4. Remote access and third parties are major attack vectors: they can bypass historical boundaries if governance and control are insufficient.
5. Segmentation and the industrial DMZ are not optional: they structure flow control and limit propagation in the event of a compromise.

These messages will be explored from different angles in the following chapters. Whenever a point reappears, it will be addressed from a complementary perspective (architecture, attack scenarios, detection, governance).

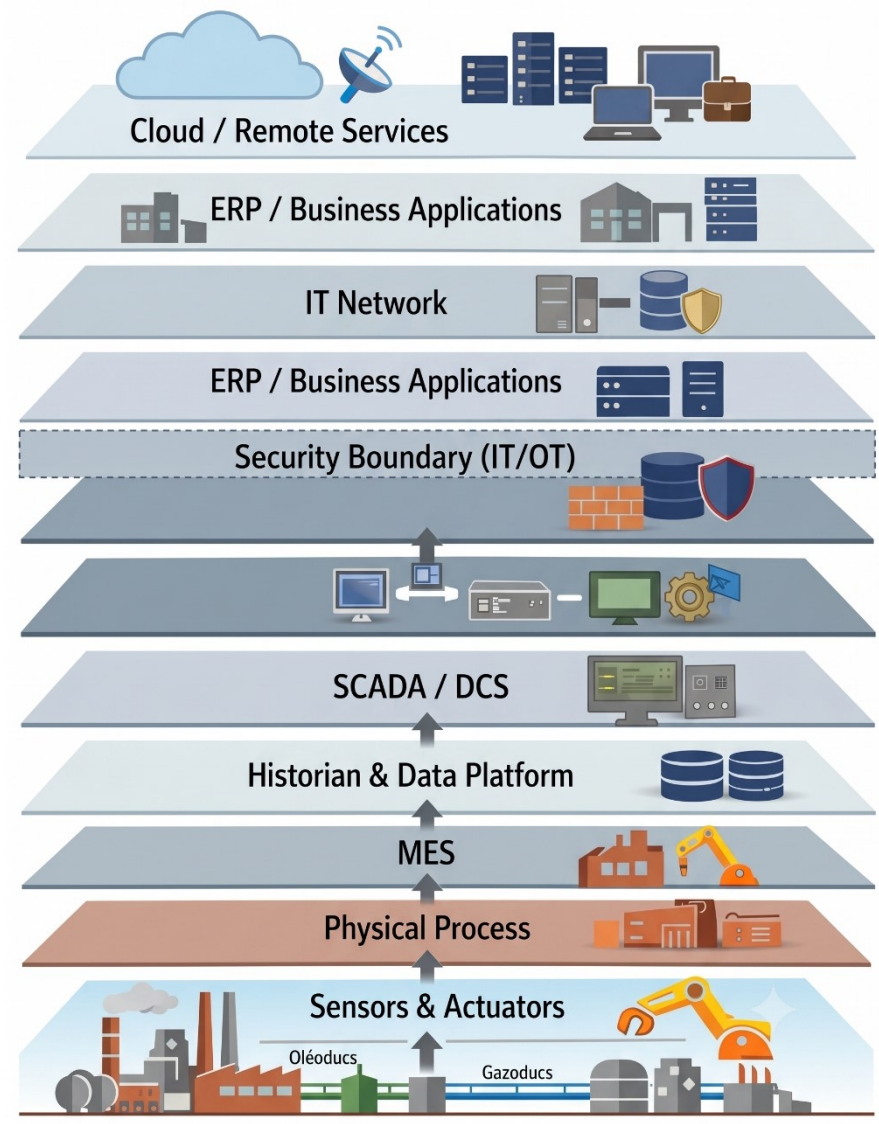

Figure 1: Layered structure of an industrial system (IT, OT, and physical process)

Part I lays the groundwork for understanding the OT ecosystem and the mechanisms that shape the associated risks. It presents:

- The main industrial systems (ICS, SCADA, PLC, DCS) and their role in controlling infrastructure;
- The fundamental differences between IT and OT, as well as the challenges related to their interconnection;
- The characteristics and vulnerabilities specific to critical sectors;
- The major normative frameworks and reference guides for industrial cybersecurity (IEC 62443, NIST, ISO), to provide a baseline;
- The evolution of cyber threats and the typology of actors likely to target industrial environments;

- The logic of infection, propagation, and attack, as well as the factors that explain why incidents persist despite awareness of the risks.

By bringing these elements together, this first part provides a foundation for understanding that makes it possible to approach industrial cybersecurity as a cross-disciplinary field where technical, operational, human, and strategic issues intersect, and where mastering systems, actors, and threats determines the ability to protect vital infrastructure.

Summary table — Part I (foundations)

1) Chapter 1 — Industrial systems: understanding OT, ICS, and SCADA — Scope**: components** (PLC, HMI, SCADA/DCS, networks) + operating logic — Angle: "how it **works"** before "how to protect it" — Lesson: without understanding the process and its dependencies, OT cybersecurity remains theoretical.

2) Chapter 2 — Differences between IT and OT: challenges, constraints, and interconnections — Scope: availability, real time, safety, maintenance, IT/OT convergence **— Angle**: what really changes (risks, priorities, methods) — **Lesson**: applying IT controls directly to OT can break operations; controls must be adapted to industrial constraints.

3) Chapter 3 — Overview of critical sectors (energy, water, oil, transport, healthcare…) — **Scope:** diversity of sectors, impacts, and dependencies **— Angle**: understanding what makes these systems critical (and why some incidents become strategic) — Lesson**: OT** prioritization starts from operational/physical consequences, not just vulnerabilities.

4) Chapter 4 — Concise overview of international standards and frameworks in industrial cybersecurity — Scope: frameworks and best practices (structuring requirements, governance, technical measures) — Angle: providing a common framework (language, objectives, maturity levels) — Lesson: standards provide guidance, but OT security is achieved through pragmatic implementation in the field.

5) Chapter 5 — Evolution of cyber threats: from curiosity to industrial sabotage — **Scope:** progression from exploration -> espionage -> sabotage -> supply chain -> ransomware**/pressure** — Angle: reading history to understand current threats **—** Lesson: OT is no longer "off the radar": preparedness, resilience, and detection are becoming as important as prevention.

6) Chapter 6 — Typology of attackers: states, hacktivists, cybercriminals, and insiders — **Scope:** profiles, motivations, levels of capability and persistence **— Angle**: linking threats to scenarios and controls — Lesson: a good threat model prevents overinvesting in the wrong place (and ignoring internal risk).

7) Chapter 7 — Infection, intrusion, sabotage: kill chain and OT attack vectors — **Scope:** sequence of reconnaissance -> access -> persistence -> IT/OT

pivot -> actions on target -> **impacts** — Angle: understanding “how” an attack unfolds in order to break **it** better — Lesson: effective defense is multi-layered (surface reduction, access control, hardening of critical workstations, protocol visibility, procedures).

8) Chapter 8 — Blind spots in industrial cybersecurity — Scope**: myths,** implicit assumptions, and organizational weaknesses (blind spots in visibility, governance, supplier dependencies, etc.) — **Angle:** what causes OT programs to fail despite having “good” tools **— Lesson**: OT security is as much a governance/operations issue as a technology issue: make things visible, clarify responsibilities, and address real exceptions.

PART II
Study of 20 OT incidents: Attacks, attempts, demonstrations, and anonymized cases — analysis and lessons learned

General introduction

The following chapters examine twenty documented OT incidents (attacks, attempts, demonstrations, and anonymized cases) that have shaped the modern history of cybersecurity in OT environments. These incidents were selected for their diversity, the quality of the available information, and, above all, their ability to illustrate the principles introduced in Part I.

They span a wide range of sectors — energy, nuclear, transportation, heavy industry, oil and gas, water, and public utilities — as well as different geographic regions and categories of adversaries: states, APT groups, opportunistic cybercriminals, hacktivists, and insiders. Each case highlights a distinct modus operandi: targeted sabotage, ransomware with operational impact, strategic espionage, supply-chain compromise, or manipulation of industrial safety systems (SIS).

Part II builds directly on the foundations laid in Part I. After presenting how industrial systems operate, the differences between IT and OT, the applicable frameworks and standards, the evolution of threats, and the typology of attackers, it is essential to confront these concepts with real-world incidents. Analysing actual cases makes it possible to observe how theoretical vulnerabilities materialize in practice, how attackers adapt their tactics to industrial constraints, and how a digital compromise can quickly produce physical, operational, economic, or even geopolitical effects.

The aim of this part is not to compile a catalogue of disasters, but to highlight recurring patterns. Across these twenty incidents, the reader will see that, despite the diversity of contexts, the underlying mechanisms often repeat themselves: IT entry points, poorly controlled remote access, exposed engineering workstations, insufficient segmentation, delayed detection, and excessive reliance on assumptions of isolation. Understanding these patterns is essential for anticipating future attacks and designing effective defense strategies.

The methodology relies exclusively on reputable open sources: reports from specialized agencies (CISA, ANSSI, ENISA, DHS, DOE), researchers' publications, technical analyses from cybersecurity vendors, academic articles, court documents, and industrial lessons learned. The descriptions are deliberately framed from a defensive perspective: they aim to explain the mechanisms, identify the exploited weaknesses, and draw useful lessons from them, without providing actionable offensive detail or reproducible procedures.

To ensure a consistent and structured reading experience, each chapter follows a common outline (with depth varying from case to case): presentation of the context and the target, identification of the attackers, chronological sequence of the incident, technical and operational impacts, response measures, root-cause analysis, and key lessons learned. A detailed technical section is also provided for readers who wish to delve deeper into OT/ICS aspects; it can be read independently without affecting overall understanding.

Part II can be read either linearly or selectively. The reader is encouraged to focus on understanding the cross-cutting lessons rather than memorizing every technical detail of each attack. The following chapters draw on these cases to illustrate the defense strategies, security architectures, and operational practices required to protect modern industrial systems.

Note on attribution: The case studies presented in this section are based on open sources (public reports, technical analyses, communications from organizations, and lessons learned). In the field of industrial systems, attribution of an attack to a specific actor is often uncertain, contested, or incomplete.

Accordingly, these chapters are not intended to "name" an attacker, but to highlight the observable technical mechanisms, the organizational failures, and the security controls that could have prevented, detected, or contained each incident.

Summary table — 20 OT incidents (Part II)

- 1) Chapter 1 — Stuxnet (2010, Iran) — Nuclear / enrichment — Entry: Supply chain + removable media / engineering workstation — Effect: Stealthy alteration of logic / parameters + equipment degradation — Lesson: Protecting engineering workstations (EWS) is just as critical as protecting the network.
- 2) Chapter 2 — BlackEnergy (2015) — Ukraine — Energy / power distribution — Entry: Spear-phishing + legitimate access / IT→OT pivot — Effect: Power outage + disruption of recovery (KillDisk, support-system sabotage) — Lesson: Remote access and legitimate accounts are critical IT→OT "bridges."
- 3) Chapter 3 — Triton / Trisis / HatMan (2017) — Oil & gas / process safety — Entry: Engineering workstation compromise + OT access — Effect: Emergency shutdown + major safety risk (SIS targeted) — Lesson: SIS ≠ BPCS: separation and engineering governance are vital.
- 4) Chapter 4 — Unitronics PLC compromises (water / multiple sectors, 2023–2024) — Water / industry (exposed PLCs) — Entry: Internet exposure + weak/default passwords — Effect: Parameter alteration / potential loss of control — Lesson: Reducing the exposed surface (no Internet-exposed PLCs) is a major OT control.
- 5) Chapter 5 — Havex (2013–2014) — Energy (OT espionage) — Entry: Supply chain + watering hole — Effect: Information gathering / potential OT access — Lesson: Supply chain: hardening software/update intake in OT is essential.
- 6) Chapter 6 — Industroyer / CrashOverride (2016) — Energy (electric grid) — Entry: IT→OT intrusion + supervisory control compromise — Effect: Coordinated outage (actions through protocols) — Lesson: OT security must include protocol-level visibility (OT IDS/NDR).
- 7) Chapter 7 — Dragonfly (2011–2014, United States / Europe) — Energy (campaign) — Entry: Phishing / watering hole / trojanized supplier software — Effect: Access to and reconnaissance of industrial environments — Lesson: Treat OT suppliers as an extension of the attack surface.

- 8) Chapter 8 — EKANS (2020) — and the confusion around “snake” — Industry (IT→OT ransomware) — Entry: IT intrusion (phishing/credentials) followed by propagation — Effect: Production stoppage / unavailability of control systems — Lesson: IT→OT ransomware: OT continuity depends heavily on IT dependencies.
- 9) Chapter 9 — Industroyer2 / INCONTROLLER (Ukraine, 2022) — Energy — Entry: IT→OT intrusion + preparation — Effect: Attempted outage / automated sabotage — Lesson: The actors return: capitalize on lessons learned and harden defenses for the long term.
- 10) Chapter 10 — Israel: water systems (2020) — Water / treatment — Entry: Remote access / exposure / passwords — Effect: Public health and safety risk (dosage alteration) — Lesson: Remote access: MFA + bastion + intervention windows are must-haves.
- 11) Chapter 11 — “Predatory Sparrow / Gonjeshke Darande” campaign (Iran, 2021–2023) — Industry (multiple events) — Entry: Multiple vectors (variable) — Effect: Claimed operational disruptions — Lesson: Separate claims, observations, and attribution.
- 12) Chapter 12 — Oldsmar Water Plant (2021) — Water (treatment) — Entry: Remote access (e.g., TeamViewer) + poor hygiene — Effect: Risk to water quality (corrected in time) — Lesson: OT remote access: MFA + bastion + restrictions on tools and accounts.
- 13) Chapter 13 — Norsk Hydro (2019) — Industry (aluminum) — Entry: IT intrusion + propagation — Effect: Production stoppages / switch to manual operations + major costs — Lesson: OT continuity depends on IT dependencies (AD, MES, network).
- 14) Chapter 14 — Maroochy Shire (2000) — Wastewater — Entry: Radio access / weak authentication — Effect: Sewage spills (environmental impact) — Lesson: The field layer (radio/RTU) is part of the OT security perimeter.
- 15) Chapter 15 — Viasat KA-SAT (2022) — Connectivity / energy (turbine supervision) — Entry: Attack on the ground segment (modems/management) — Effect: Loss of connectivity / remote supervision — Lesson: Telecommunications dependencies are part of OT risk.
- 16) Chapter 16 — Aurora Generator Test (2007) — cyber-physical demonstration — Energy (demonstration) — Entry: Command manipulation (test) — Effect: Physical damage demonstrated — Lesson: Cyber→physical: integrate electrical protections and procedures.
- 17) Chapter 17 — German Steel Mill (2014, Germany) — Steel industry — Entry: IT intrusion + likely pivot — Effect: Reported damage (limited details) — Lesson: When information is limited: proceed cautiously and make hypotheses explicit.
- 18) Chapter 18 — FrostyGoop (Ukraine, 2024) — District heating — Entry: OT access + commands — Effect: Service outage (public impact) — Lesson: Protocol-level visibility is a prerequisite for OT detection.

- 19) Chapter 19 — Bowman Avenue Dam (United States, 2013) — Infrastructure (dam) — Entry: Remote access/exposure (reported) — Effect: Reported limited impact (often nuanced) — Lesson: Distinguish between access, ability to act, and actual impact.
- 20) Chapter 20 — “Kemuri Water Company” — anonymized case (Verizon) — Water (teaching case) — Entry: Vectors described by Verizon (anonymized) — Effect: Defensive lessons on access, detection, and governance — Lesson: Be transparent: anonymized/training case vs. specifically attributed incident.

PART III
Industrial Cybersecurity Strategies and Tools: Protecting Critical Systems

Methods, tools, and practices for securing ICS, SCADA, and DCS environments, with a focus on the differences between IT and OT.

General Introduction

Industrial Cybersecurity Strategies and Tools: Protecting OT and Critical Systems

Part II examined major cyberattacks against OT environments and showed just how vulnerable industrial systems can be, whether the threat is opportunistic, highly sophisticated, or somewhere in between. Part III shifts the perspective.

The focus is no longer on the damage attacks can cause, but on how to prevent them in a durable, operationally sound way.

The earlier parts of this book established a central reality:

industrial incidents rarely stem from a single technical weakness. More often, they emerge from a combination of architectural, organizational, and operational decisions that, taken together, create systemic risk.

In environments where IT, OT, IoT, and cloud services are now interconnected, even a well-intentioned control can become a new source of fragility if it is poorly adapted to industrial constraints.

The objective of Part III is straightforward:

to provide a structured, pragmatic, and operational approach to defending industrial environments while respecting their specific constraints and mission-critical priorities.

Unlike traditional IT cybersecurity, which has historically emphasized data confidentiality, OT cybersecurity is driven first by:

Human safety,Operational continuity,The integrity of industrial processes and the availability of critical facilities.

Recent attacks - from targeted sabotage such as Stuxnet to opportunistic incidents such as Oldsmar and complex campaigns attributed to nation-state actors - have put an end to a long-standing myth:

ICS/SCADA systems can no longer be treated as isolated, nor can they be protected by obscurity alone.

Part III therefore examines the strategies and tools needed to build a modern, coherent, and resilient OT security posture, including:

- Defense in depth, segmentation, and isolation,
- Identity and access management (IAM, PAM),
- Strong authentication and remote access control,
- Continuous monitoring and anomaly detection,
- Normative and architectural frameworks such as the Purdue Model and ISA/IEC 62443.

Each chapter follows three complementary threads:

- Understanding the principle or tool
  Definition, purpose, and OT-specific characteristics.
- Identifying the risks created by its absence or poor implementation
  Using practical examples drawn from the incidents analyzed earlier.
- Putting the security measure into practice
  Operational recommendations, industrial constraints, and common pitfalls to avoid.

The aim is not simply to inform, but to equip the reader - whether an OT engineer, CISO, operator, consultant, or student - to implement realistic measures that fit industrial reality.

Part III is therefore the bridge between understanding how attackers operate and building a defense strategy that is effective, pragmatic, and sustainable.

In short:

Now that we understand how industrial attacks happen, it is time to look at how to resist them without compromising the process itself.

Chapter 1 - Defense in Depth for ICS/OT: An Architecture for Survival

Chapter objectives

By the end of this chapter, you will be able to:

- Explain why defense in depth is essential in ICS/OT (availability, integrity, safety)
- Map a typical architecture using the Purdue Model and the ISA/IEC 62443 “zones and conduits” logic
- Define coherent layers of control (segmentation, hardening, monitoring, physical access, organization)
- Identify common design mistakes (poorly designed DMZs, unmanaged flows, ungoverned contractor access)
- Define a realistic OT security MVP for an industrial site (high-impact first measures).

1.1 Introduction

From Stuxnet to Colonial Pipeline, industrial cyberattacks have made one fact impossible to ignore: relying on a single barrier - a firewall, an antivirus product, or a VPN - means betting the plant on a single point of failure. In ICS/OT environments, a breach is not just a data-security problem. It can disrupt production, degrade quality, trigger a safety event, or put people at risk.

Defense in Depth turns that constraint into an architectural principle: layer independent controls so that an attacker is slowed, lateral movement is constrained, malicious activity is detected early, and the process remains under control even when one layer fails. This chapter lays out the core principles, the main reference frameworks (Purdue and ISA/IEC 62443), and a practical method for designing a robust OT architecture.

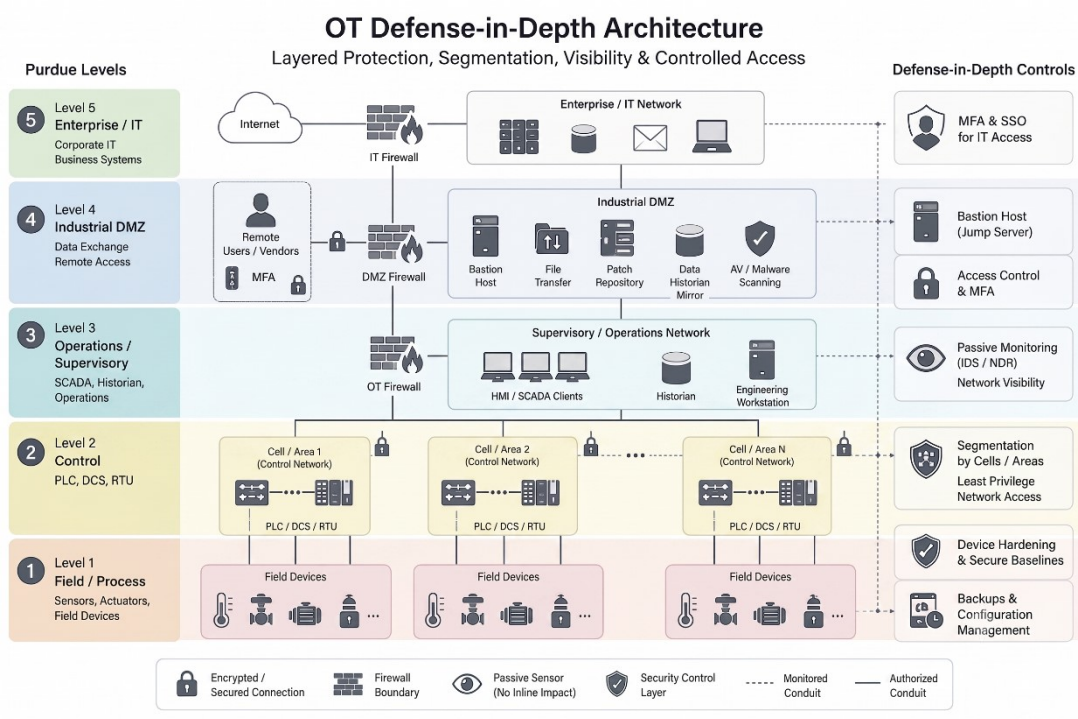

Figure 1: OT Defense-in-Depth Architecture

APPENDIX III-A — Answer Elements for the Self-Assessments (Part III)

Reader's note

The answer elements in this appendix are intended to support the reader's reflection after the self-assessment questions proposed at the end of several chapters.

They are neither exhaustive answers nor universal prescriptions. Every industrial environment has its own technical, organizational, and regulatory constraints, and these must be taken into account in any cybersecurity initiative.

Chapter 1 — Defense in Depth for ICS/OT: a survivable architecture

1. Because it isolates zones and limits lateral movement: a compromise is contained by multiple boundaries (conduits), not a single perimeter.
2. The most critical entry points are remote access and telemaintenance, IT/OT interconnections through the DMZ, sensitive workstations such as EWS/HMI, and removable media.
3. Useful compensating controls include segmentation and allowlist-based filtering (firewalls, ACLs, DPI), hardening and application control, and passive monitoring (NDR/IDS).
4. Prevention reduces the probability of compromise; detection reveals abnormal activity early enough to react before process impact occurs.
5. MOC keeps the architecture coherent over time: changes are tracked, exceptions expire, baselines and flows are reviewed, and incidents can be correlated with approved changes.

Chapter 2 — OT inventory and asset classification: the foundational prerequisite

1. An IDS/NDR must know which assets exist, what role they play, which zone they belong to, and what "normal" traffic looks like in order to detect deviations.
2. At a minimum, an OT asset record should contain a logical name/type, IP address (and ideally MAC), Purdue/zone mapping, OT owner, criticality, exposure, and basic version information where available.
3. Frequent IT dependencies include AD, DNS, NTP, and backup services.
4. Passive discovery comes first because it does not inject traffic and therefore reduces the risk of disturbing fragile devices; "safe active" checks come later, in a targeted and validated manner.
5. Use process criticality and exposure together to prioritize hardening on the riskiest combinations.

Chapter 3 — Identity and access management: locking the doors of the industrial kingdom

1. RBAC assigns rights according to roles and scope; PAM governs privileged access through vaulting, temporary elevation, session traceability, and review.
2. Service accounts are a frequent blind spot because they are long-lived, often highly privileged, weakly monitored, and rarely rotated.
3. A breakglass path must be time-limited, strongly traceable, and reviewed after use.
4. High-priority OT IAM events include MFA failures followed by success, off-hours logins, access to EWS/SCADA, PAM checkouts, and creation or modification of privileged accounts.
5. Useful KPIs include MFA coverage on OT entry points and the percentage of privileged sessions that pass through bastion/PAM with recording.

Chapter 4 — OT change management and secure configuration

1. MOC is a cybersecurity control because it governs who changes what, when, and how—and prevents "temporary" exceptions from becoming lasting weaknesses.
2. A baseline is a validated reference configuration for services, settings, rules, and versions; it should be tested, versioned, and protected.
3. PLC/DCS programs and network-device configurations should always have a rollback plan; SCADA/HMI servers should as well.
4. MOC structures patching by forcing impact analysis, testing, windows, rollback, and compensating controls when delay is necessary.
5. Unauthorized change can be detected through configuration drift monitoring, version control, centralized logs, and SIEM/IDS correlation with the MOC journal.

Chapter 5 — Intrusion detection and prevention: the plant's digital sentries

1. An IDS observes and alerts, usually passively; an IPS can block inline. In OT, active blocking must be used far more cautiously because availability is critical.
2. The best sensor locations are the choke points: DMZ boundaries, key conduits, and critical paths between supervision and control.
3. Without a baseline, tuning becomes noisy and unsustainable because normal production, maintenance, and batch cycles are mistaken for anomalies.
4. Useful MVP alerts include new assets, new inter-zone flows, unexpected protocols, unusual scans or connections, and write activity outside normal windows.
5. Allowlists stay useful only if they are governed through MOC, review cycles, and expiry of temporary exceptions.

Chapter 6 — Security tools for industrial protocols

1. Many industrial protocols were designed for trusted, closed environments with real-time constraints, not for modern hostile networks.
2. OT DPI understands protocol functions and can authorize or deny actions based on meaning—not just IPs and ports.
3. When equipment cannot support modern cryptography, a secure tunnel between zones or sites protects transport without changing the legacy endpoint.
4. Key deployment risks include added latency, jitter, fragile device behavior, and false blocking that may disrupt the process.
5. The right approach is progressive: observe first, test in representative conditions, prepare rollback, and supervise closely.

Chapter 7 — OT log monitoring and analysis

1. Priority log sources include VPN, bastion, PAM, network-security devices, selected OT Windows servers, SCADA/EWS/HMI systems, and IDS/NDR alerts.
2. Consistent time is indispensable because a timeline is the foundation of both attribution and reliable investigation.
3. Logging collects and stores events; detection analyzes and correlates them to generate actionable alerts.
4. Logs should be centralized on a protected collector, with restricted access, retention, integrity protection where feasible, and monitoring of the logging chain itself.
5. A simple but useful signal is a privileged login outside normal hours or the appearance of a new undocumented inter-zone flow.

Chapter 8 — ICS penetration tests and audits

1. Safety and availability come first: use non-intrusive techniques, controlled windows, and a solid understanding of the process.
2. Rules of engagement should define scope, windows, allowed and forbidden techniques, stop conditions, OT contacts, and evidence/reporting expectations.
3. Start with passive mapping, configuration review, and analysis of logs and flows before any simulation or more active step.
4. Findings should be ranked by process impact and real exposure, not just by technical score.
5. A retest proves that corrective action worked and did not introduce regression.

Chapter 9 — Business continuity and disaster recovery plans

1. An OT DRP aims to restore the process to a safe operating state, not merely to rebuild servers.

2. Offline or immutable backups matter because ransomware often targets recovery data.
3. PLC/DCS programs and configurations, SCADA/HMI/EWS images or VMs, and OT network configurations are among the highest priorities.
4. Restoration should occur in a controlled sequence, with version checks, communication validation, and process/safety approval before return to production.
5. A degraded mode is a reduced but validated way of operating; preparing it limits full shutdown and safety risk.

Chapter 10 — Zero Trust applied to OT

1. The principle is simple: trust nothing implicitly, verify continuously, enforce least privilege, and assume compromise is possible.
2. It reduces lateral movement between cells and zones and limits domino effects.
3. Context matters: identity, role, zone, workstation posture, entry point, time window, and approved change or ticket.
4. A realistic rollout begins with MFA and bastion control, then stronger segmentation and allowlisting, and finally contextual access and micro-segmentation where justified.
5. Exceptions must be justified, time-bound, and reviewed to avoid silent drift.

Chapter 11 — Remote access and third-party management

1. Third-party access combines high privileges, operational dependency, and limited visibility; permanent external paths often become major entry points.
2. A robust model uses a single entry point (bastion), MFA, session recording, temporary rights, and linkage to a maintenance ticket.
3. MFA is the second factor at connection time; step-up authentication is an additional challenge triggered when a sensitive action is attempted.
4. The full access process should include request, validation, activation, supervision, rapid cut-off capability, closure, and review.
5. A safe path that is fast and well-governed is far better than pushing teams toward shadow access methods.

Chapter 12 — ICS anomaly detection and analysis

1. An anomaly is a deviation from the baseline; an incident is an anomaly confirmed as malicious or operationally harmful enough to require response.
2. OT baselines must account for shifts, batch cycles, maintenance windows, and periodic behavior; otherwise they create false positives.
3. Typical OT priority alerts include undocumented inter-zone flows, unexpected protocols, out-of-window writes or setpoint changes, and unexpected controller state changes.
4. MOC and IAM reduce false positives by providing context: if an action matches an approved change and a legitimate identity chain, the alert can often be downgraded.

5. Useful KPIs include false-positive rate, time to triage and qualify, percentage of alerts correlated to MOC, and the number of newly detected undocumented flows.

Chapter 13 — OT vulnerability management

1. CVSS alone is not enough because it does not reflect process impact, true exposure, or the effect of compensating controls.
2. Typical compensating measures include strict segmentation, virtual patching, application control, legacy isolation, and stronger monitoring.
3. MOC governs safe patching and mitigation through testing, windows, rollback, exception traceability, and updates to inventory and flows.
4. High-priority assets often include entry points, SCADA/HMI/EWS servers, exposed Windows assets, gateways, DMZ services, and high-criticality or high-exposure systems.
5. Verification means proving the corrected or mitigated state, updating the inventory, and confirming lower exposure through retest or OT-validated control checks.

Chapter 14 — Incident response in ICS environments

1. In OT, the first objective is safety and continuity. Incident response must preserve a safe process state and be performed with operations, not in parallel to it.
2. Containment must be targeted, because a blunt action can stop production or degrade safety.
3. Core evidence sources include VPN/bastion/PAM logs, IDS/NDR traces, SCADA/EWS records, validated PLC references or checksums, and Historian trends.
4. Integrity is validated by comparing against known-good logic and configurations, reviewing change history, and testing before return to service.
5. Lessons learned should improve segmentation, IAM, MOC, backups, EWS/SCADA hardening, and team readiness.

Chapter 15 — The OT SOC

1. The minimum building blocks are an OT inventory/CMDB, NDR/IDS sensors, logging/SIEM collection, OT runbooks, and an escalation capability that includes operations.
2. Process context matters because many alerts may be related to maintenance or expected process variation; response should reduce noise and avoid unnecessary disruption.
3. Useful KPIs include MTTD or triage time, false-positive rate, coverage of critical assets and flows, traceable privileged sessions, and the number of undocumented flows detected.
4. An OT SOC depends on earlier foundations: segmentation, inventory, IAM/PAM, MOC, logging, and anomaly detection.

5. A simple runbook for a “new inter-zone flow” should verify MOC, identify the owner, determine read versus write capability, choose block or allowlist action, and document the outcome.

Chapter 16 — OT technical resilience

1. Redundancy is duplication of components or paths. Resilience is the broader ability to withstand, degrade safely, and recover quickly to a trusted state.
2. The most critical recovery elements are PLC/DCS programs and configurations, SCADA/HMI/EWS images, OT network configurations, and essential access services such as bastion/PAM.
3. A backup is not trustworthy until restore exercises prove that timing, procedure, and safe return-to-service conditions actually work.
4. High-yield hardening measures include removing default accounts, using unique credentials, enforcing allowlisting where feasible, hardening services, and controlling USB usage.
5. Before returning to production, verify integrity against the baseline or golden reference, validate communication and alarming, confirm process and safety behavior, keep monitoring active, and maintain rollback capability.

APPENDIX III-B — Solutions to the Micro-Cases (Part III)

This appendix provides the full context for each micro-case presented in **Part III**, followed by a model response (indicative), common pitfalls, and expected evidence.

Micro-case Chapter 1 — "Pilot plant: an OT architecture that must survive IT"

Context: A pilot water treatment plant is modernizing its OT (supervision + automation) while maintaining a very high availability requirement. IT→OT exchanges are necessary (reporting, KPIs, central supervision), and contractors intervene remotely. Part of the OT estate is "legacy" and unpatchable in the short term.

What is happening: The architecture project is progressing... but the teams do not agree on the boundaries, the DMZ, or the truly indispensable flows. You are asked for a target architecture that "holds" even if IT is compromised.

Constraints / clues: Contractor remote access is indispensable; coexistence of modern and legacy equipment; requirements for segmentation by zones (cells); need for visibility without disturbing the process.

Your mission (CISO/OT sec): Define a robust OT architecture (zones/conduits + industrial DMZ) and a "MVP" set of controls that can be deployed quickly, without creating additional downtime.

Questions (to structure your approach):

- Which zones (Purdue / cells) do you distinguish and why (supervision, engineering, process cells, field, DMZ)?
- Which IT<->OT flows are legitimate and which must be removed or mediated via the DMZ?
- Which "MVP" controls do you prioritize (allowlist filtering, bastion, passive monitoring, EWS/HMI hardening, backups/restoration)?
- How do you govern contractor remote access (single entry point, traceability, temporary rights, scope)?
- In the event of an IT ransomware attack, which layers must prevent propagation and what emergency actions do you apply without stopping the process?

Key point not to miss: A "survivable" OT architecture requires strict boundaries and minimal flows, regardless of the state of IT.

Model Response (indicative)

- **Objective: build a "survivable" architecture (IT compromised).**
- **Divide into zones and conduits (Purdue):**

    - Clarify L4/IT, industrial DMZ, L3 supervision, L2 cells/control, L1/0 field.
    - Enforce unique and filtered conduits (allowlist) between zones, no "shortcuts".
- **Minimal IT<->OT flows:**
    - Identify only indispensable flows (KPI/Historian, third-party access, controlled updates).
    - Mediation via DMZ (reverse proxy / relay / jump); forbid direct IT→L3/L2 access.
- **MVP Controls (30–60 days):**
    - Bastion + MFA + named accounts + session recording (third parties and internals).
    - Allowlist filtering at the conduits, pre-validated "crisis mode" rules.
    - Passive monitoring (NDR/IDS) + baseline; EWS/HMI hardening; tested OT backups.
- **IT ransomware crisis mode:**
    - Immediate reduction of IT→DMZ→OT flows to the "minimum vital set".
    - Freeze changes, suspend non-essential remote access, reinforced monitoring of write-paths.

Common pitfalls

- Confusing "air-gap" with the reality of IT dependencies (AD/DNS/NTP, recipes, licenses).
- Allowing a "temporary" direct IT→OT access that becomes permanent.
- Deploying controls without an operational runbook (who does what during an incident).

Good evidence

- Zones/conduits mapping and flow matrix (read/write) validated by the field.
- Exported and versioned firewall/ACL rules + justification for retained flows.
- Bastion/PAM/VPN logs (sessions, accounts, actions) + proof of MFA.
- OT restoration test reports (sign-offs) and "golden" images of critical workstations.

Micro-case Chapter 2 — "The OT inventory that reveals the ghost asset"

Context: In a water treatment plant, an OT inventory is launched to prepare for detection (IDS/NDR) and asset governance.

What is happening: The team discovers an undocumented workstation communicating with several PLCs, with more "active" exchanges than expected.

Constraints / clues: The workstation is used occasionally by a contractor; no official "owner"; observed flows include writes to sensitive registers outside maintenance windows; remote access to this workstation does not appear in any procedure.

Your mission (CISO/OT sec): Qualify the asset (role, flows, owners, risks), stop uncontrolled writes without disrupting production, and integrate everything into a change management process (MOC) and an up-to-date inventory.

Questions (to structure your approach):

- What minimum information must this asset's record contain (role, zone, owner, accounts, dependencies, read/write flows)?
- How do you distinguish a "normal" (functional) write from a risky write (outside process, outside window, unauthorized source)?
- What immediate "anti-surprise" measure do you apply (allowlist filtering, cutting a write-path, restricting remote access)?
- What evidence do you collect to attribute the activity (workstation + account + time + target)?
- How do you prevent this type of "ghost" asset from reappearing (MOC + periodic review + owner accountability)?

Key point not to miss: In OT, a useful inventory is not a list of equipment: it is assets + flows + write rights + ownership.

Model Response (indicative)

- Stabilize: understand the "ghost" asset.
    - Locate the asset (switchport, ARP/MAC, VLAN), identify the owner (OT/IT/integrator).
    - Qualify its role: passive (listening), active (OPC/engineering), bridge (dual-homing).
- Decide: treat the risk without breaking prod.
    - If asset unjustified: logically isolate (quarantine VLAN / ACL) then plan removal.
    - If asset useful: document, harden, integrate into inventory (owner, MOC, backups, logs).
- Implement a defensible OT inventory.
    - Process: passive discovery + reconciliation with MOC + operations validation.

    - Classification: process criticality, role (write-path), inter-zone exposure, dependencies.

Common pitfalls

- Treating the asset like a simple "unknown PC" without analyzing its process role (write-path).
- Abruptly cutting off equipment that serves as a relay/recipe/collector and causing a shutdown.
- Accepting a "temporary" setup without an owner or evidence (it becomes permanent debt).

Good evidence

- Network evidence (MAC/ARP, ports, VLAN, routes) + capture (PCAP) of observed protocols.
- Configuration report of the asset (services, accounts, access) + applied hardening.
- Asset record: owner, criticality, MOC, windows, backups, removal plan if applicable.

PART IV
Governance, Standards, and Regulation:
The Strategic Framework for Industrial Cybersecurity

General introduction

Part IV moves from technical mechanisms to strategic governance: the goal is no longer just to understand how attacks work or how segmentation is implemented, but to understand how an organization governs industrial cybersecurity over time—with clear direction, responsibilities, rules, and deliberate trade-offs.

In an OT environment, security cannot rely on improvisation or on simply piling up tools. It must be embedded in a strategic framework built on standards, governance, regulatory compliance, an ecosystem of external stakeholders, and risk management capable of connecting the plant floor, IT, leadership, and economic reality.

Concretely, this part helps you move:

- From a "technical" language to a common, measurable language (frameworks, requirements, security levels).
- From a theoretical framework to policies and procedures that are applicable, repeatable, and auditable on a day-to-day basis.
- From a voluntary approach to sector-specific obligations (incidents, notification deadlines, minimum requirements, penalties).
- And from ad hoc security to a risk-driven posture that can be defended before both management and auditors.

Throughout the chapters, you will see how to align the major frameworks (ISA/IEC 62443, NIST, etc.), translate those requirements into documentary governance (OT security policy, policies, procedures), understand the role of authorities and information-sharing communities, build a decision-oriented risk approach, and then make compliance "audit-ready" by producing verifiable evidence and deliverables.

Note on the case studies included in this part:

How can you tell which chapter a case study belongs to (and avoid confusion)?

In Part IV, several chapters address governance, rules, evidence, and operations. It is natural to ask: "Why is this case here? Could it not be placed elsewhere?"

The answer often turns on a single question.

A simple test: "Who is forcing me to do this?"

- If the answer is "standards / frameworks," then the case study belongs in Chapter 1 (the standards landscape: ISA/IEC 62443, NIST, ISO, etc.).
- If the answer is "our organization / our internal rules," then it belongs in Chapter 2 (policies and procedures: access, MOC, backups, removable media, patching, etc.).
- If the answer is "a regulator / a law / a sector-specific obligation / an external audit," then it belongs in Chapter 3 (sectoral compliance: requirements, deadlines, notification, supply chain, demonstration).

- If the answer is “the number of stakeholders involved and the need to coordinate who does what,” then it belongs in Chapter 4 (the cybersecurity ecosystem: OT/IT/CISO roles, integrators, OEMs, SOC, GRC, decision flows).
- If the answer is “the need to arbitrate, prioritize, and justify choices under constraints,” then it belongs in Chapter 5 (risk management: assessment, treatment, acceptance, priorities, risk-reduction plan).
- If the answer is “the need to prove, in black and white, what is being done and to manage deviations,” then it belongs in Chapter 6 (OT compliance and audits: evidence, test reports, logs, non-conformities, action plans).

This logic helps classify most case studies unambiguously, even when the context (drinking water, energy, transport, healthcare, etc.) might appear reusable across several chapters. The key point is therefore not the chosen sector, but the teaching angle: standardize, organize, comply, orchestrate, arbitrate, or demonstrate.

Summary table — Part IV (governance & compliance)

1) Chapter 1 — Standards and frameworks (ISA/IEC 62443, NIST SP 800-82, ISO 27001, etc.)

Scope: “common language” reference points for structuring an OT approach (OT-specific frameworks plus bridges to the ISMS, continuity, and safety).

Angle: understanding what each framework is for (requirements, architecture, organization) and how to combine them without doing “IT copy-paste.”

Lesson: standards do not “secure” anything by themselves; most importantly, they align vocabulary, objectives, and expected evidence so that a coherent program can be managed.

2) Chapter 2 — OT governance: roles, responsibilities, and decision cycles

Scope: OT/IT organization, committees, responsibilities, policies/procedures, multisite consistency, and KPI-based steering.

Angle: turning OT cybersecurity into an organizational capability (clarifying who decides, who executes, who controls, and how things are reviewed).

Lesson: without documentation and enforced policies, even a solid architecture becomes “uneven,” hard to audit, and fragile (turnover, changes, exceptions).

3) Chapter 3 — Regulation and critical sectors: NIS2, NERC CIP, DORA, etc.

Scope: sector-based obligations (notification, risk management, resilience requirements, supply chain) and the integration of cyber into existing safety frameworks.

Angle: translating texts (directives/laws/regulators) into actionable requirements: gap analysis, priorities, evidence, and governance.

Lesson: compliance is only useful if it lands in measurable controls and real governance; in several sectors, it often brings security and safety into much closer alignment.

4) Chapter 4 — The industrial cybersecurity ecosystem and stakeholders

Scope: CERT/CSIRT and authorities, EU/international coordination (e.g., ENISA), standardization, and information-sharing communities (ISAC/ISAO).

Angle: mapping who to call and who to cooperate with (before a crisis), and leveraging collective intelligence (guides, exercises, incident feedback).

Lesson: in OT, being prepared also means having your network in place (contacts, procedures, communities); organizational isolation is extremely costly during a crisis.

5) Chapter 5 — Industrial cyber risk management

Scope: the full cycle (identify -> analyze -> assess -> treat -> monitor), risk appetite, risk register, and prioritization.

Angle: turning “diffuse fear” into comparable scenarios and arbitrable decisions (including with finance and executive management).

Lesson: risk becomes the common language (OT/IT/operations/management) and the maturity tool: deciding what is accepted and why, consciously.

6) Chapter 6 — OT compliance & audits (evidence, reporting, supply chain)

Scope: audit preparation, evidence production, reporting, and supply-chain requirements (NIS2/62443/ISO 27019).

Angle: moving from “doing security” to “demonstrating and sustaining it” (traceability, documentation, continuous control).

Lesson: audit-readiness is a component of resilience: it enforces discipline, reduces blind spots, and secures relationships with customers, regulators, and suppliers.

Chapter 1 — The Standards Landscape: ISA/IEC 62443, NIST SP 800-82, and the Key Frameworks

1.1 Introduction — The need for a common standards language

Industrial systems operate under constraints that make cybersecurity fundamentally different: continuous availability, human safety, process quality, physical constraints, and direct interaction with the real world. In that environment, cybersecurity cannot rely on improvisation or a patchwork of tools. It needs a structured framework that guides organizations, harmonizes practices, and delivers measurable, sustainable security.

Standards provide that framework.

They help organizations harmonize practices across sites, teams, and service providers; define common requirements for a sector or an organization; integrate cybersecurity across the industrial lifecycle; facilitate audits, monitoring, and regulatory compliance; and provide a solid basis for managing security over time.

Among the many existing frameworks, ISA/IEC 62443 and NIST SP 800-82 hold a central place. They offer a unique complementarity: one provides technical and organizational requirements, while the other provides practical, immediately actionable methods.

This chapter clarifies these frameworks, presents their respective contributions, and shows how they structure modern industrial cybersecurity.

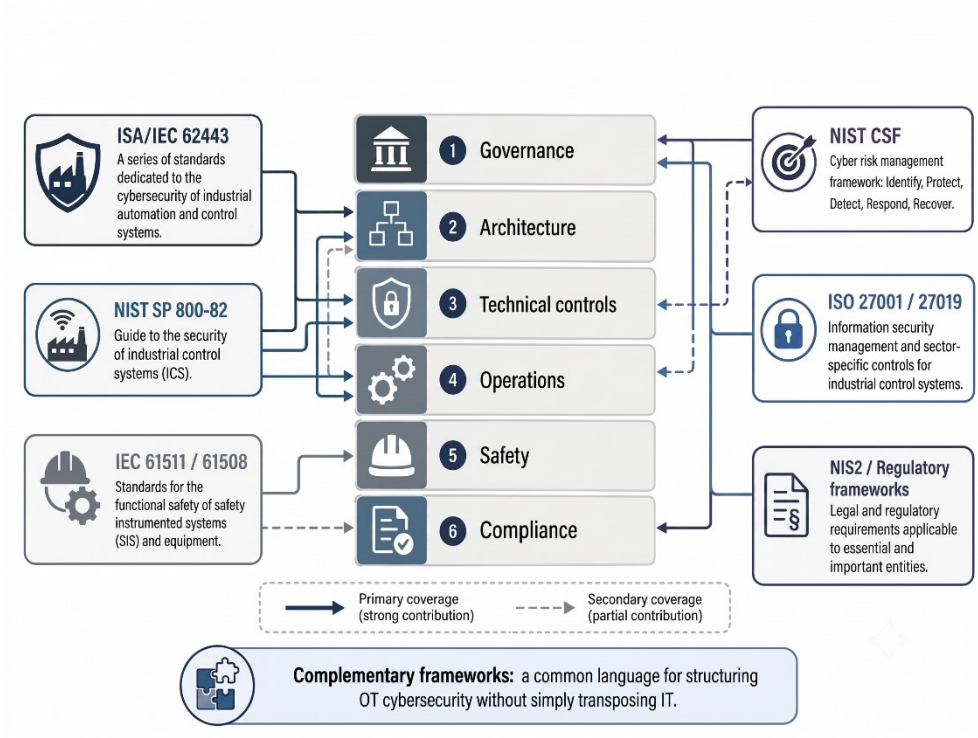

Figure 1: Overview of industrial cybersecurity frameworks: who covers what?

1.2 ISA/IEC 62443 — The global reference standard for industrial cybersecurity

//

Hiden in free Sample

//

Chapter 3 — Sector-Specific Compliance and Regulations: The Rules of the Game by Industry

3.1 Introduction – From Voluntary Action to Legal Obligation

Standards (ISA/IEC 62443, NIST SP 800-82, ISO 27001, etc.) and internal policies are part of a voluntary approach: an organization chooses to align with good practices to improve its security posture.

But for infrastructures whose failure can affect society as a whole - electricity grids, drinking water, transport, healthcare, chemicals, oil & gas - this approach is no longer

sufficient. States and regulators have gradually put in place a binding regulatory framework:

- Minimum security obligations.
- Governance requirements.
- Incident-notification deadlines.
- Audits and inspections.
- Financial penalties, and in some cases even criminal sanctions.

The goal of this chapter is not to turn the reader into a lawyer, but to provide:

- A clear view of the regulatory landscape governing industrial cybersecurity.
- An understanding of the concrete impacts on an OT program: governance, procedures, investments, reporting, and documentation.

We will start with the NIS 2 Directive, the cornerstone of European cybersecurity regulation, then look at how certain sectors - energy, water, transport, and chemicals - are governed by specific rules, often complementing the technical standards discussed in the previous chapters.

3.2 The Paradigm Shift: the NIS 2 Directive and Its Impact

The NIS 2 Directive (Network and Information Security 2) now forms the backbone of cybersecurity regulation in Europe.

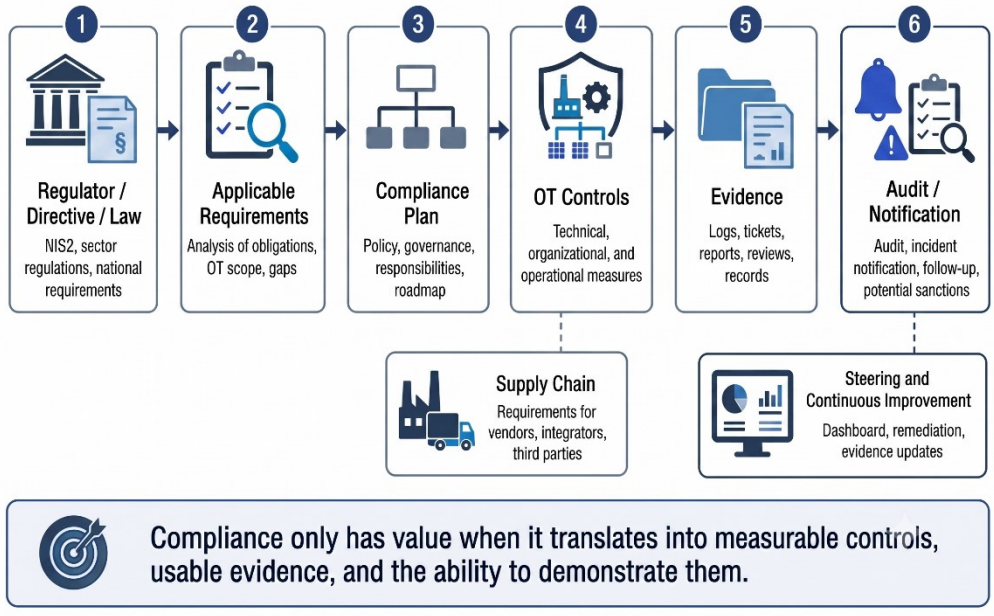

Figure 6: Sector Compliance Chain – From Regulatory to Demonstrable Control

It succeeds NIS 1 by expanding:

- The number of sectors concerned.
- The depth of the requirements.
- And, most importantly, the level of accountability placed on executives.

The core idea is simple: organizations operating services that are critical to society no longer have the right to manage cybersecurity poorly. They must demonstrate a minimum level of maturity under the supervision of national authorities.

Terminology note: IEC 62443 defines technical Security Levels (SLs) (by zone/system) to characterize a target security level. NIS 2, for its part, primarily imposes obligations relating to risk management, governance, organizational measures, and incident notification, without requiring a specific SL to be reached.

3.2.1 Who Is Covered?

NIS 2 replaces the former OES (Operators of Essential Services) and DSP (Digital Service Providers) categories with two broad groups:

- Essential entities.
- Important entities.

The logic is no longer purely sector-based, but also based on:

- The size of the organization.
- Its potential impact on society.

The essential sectors notably include:

- Energy: electricity, gas, oil, hydrogen, district heating and cooling, etc.
- Transport: air, rail, maritime, inland waterway, and road transport.
- Water: drinking water and wastewater.
- Health: hospitals, critical laboratories, manufacturers of medical devices.
- Digital infrastructure: Internet exchange points, DNS, critical data centers.
- Public administration, etc.

Among the important sectors, NIS 2 also includes areas directly linked to industry:

- Waste management.
- Production and distribution of chemicals.
- Food.
- Manufacture of medicines, medical devices, computers, electronic components, etc.

In practice, a great many medium-sized and large industrial players are now subject to NIS 2, sometimes without yet fully realizing it.

3.2.2 Key Obligations for Industrial Operators

NIS 2 imposes a number of obligations transposed into national legislation. For industrial sites, this notably means:

- **Risk management and "appropriate and proportionate" security measures.**
    - Implementation of technical and organizational measures covering:
        - Governance.
        - Access management.
        - Vulnerability management.
        - Business continuity and recovery.
        - Security of OT/IT networks and systems.
        - Supply-chain security.
    - The choice of technical framework (ISA/IEC 62443, NIST, ISO 27001, etc.) becomes a lever for demonstrating compliance.

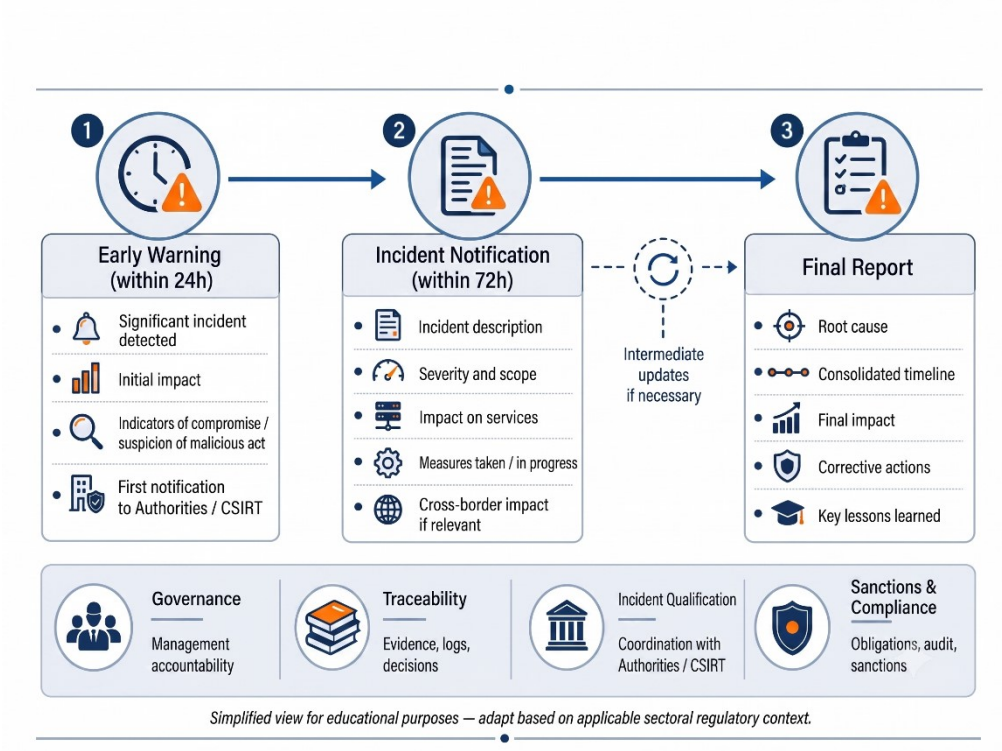

Figure 7: Notification Timeline: 24 h -> 72 h -> Final report.

- **Incident notification.**
  - Reporting to the competent authorities (national CSIRT and/or competent cybersecurity authority, depending on the country) incidents that have a significant impact on the availability, confidentiality, or integrity of services.
  - Tight deadlines:
    - **Initial alert within 24 hours.**
    - **More detailed report within 72 hours.**
    - **Final report (closure) within 30 days; it often takes the form of a formalized post-mortem/lessons-learned report (depending on national transposition).**
- **Supply-chain security.**
  - Assessing cyber risks related to suppliers, service providers, and integrators.
  - Embedding security requirements into contracts.
  - Monitoring exposure through third-party software, OEMs, cloud services, etc.

- **Security policy, cryptography, and business continuity.**
    - Existence of a formal security policy (see Chapter 2).
    - Use of appropriate cryptographic mechanisms.
    - Business continuity and recovery plans in the event of a major cyber incident.
- **Controls, audits, and sanctions.**
    - National authorities may:
        - Request detailed reports.
        - Carry out audits.
        - Require remediation plans.
        - Impose significant fines (up to several percent of annual global turnover).

The objective is not "technical perfection," but a structured, traceable, managed, and verifiable approach.

3.2.3 Governance Implications

One major new feature of NIS 2 is the explicit accountability of senior management.

- **Members of management must:**
    - Approve the cybersecurity policy.
    - Oversee risk management.
    - Receive regular reports.
    - Undertake cybersecurity training.
- **In the event of serious failure:**
    - Individual sanctions may be considered (for example, a temporary ban on holding certain functions, depending on national transposition).

As a result, industrial cybersecurity is no longer merely a technical topic for the CISO and the OT Manager, but a governance issue at executive-committee level. Bringing an organization into compliance with NIS 2 is therefore as much an organizational project as it is a technical one.

3.2.4 What NIS Does Not Require:

The NIS2 Directive significantly strengthens cybersecurity requirements, but it must not be interpreted as imposing systematic certification. Here is what NIS2 does not explicitly require:

Pitfall: No requirement for ISO 27001 or 62443 certification

Organizations must demonstrate that they manage their risks, but the text does not require any specific certification.

Compliance may be demonstrated through internal or external non-certification audits.

Pitfall: No requirement to reach a specific SL (Security Level)

NIS2 requires a method, not a numerical target.

It does not say: "Achieve SL-2 or SL-3," unlike certain requirements in heavily regulated sectors.

Pitfall: No requirement to use a particular standard

NIS2 cites references (ISO 27001, 62443, NIST, etc.) but imposes none of them. Member States may provide guidance, but they may not impose a single framework.

Pitfall: No requirement to physically separate IT and OT

NIS2 requires OT risk management and logical segmentation, but not a prescribed architecture.

Pitfall: No requirement for specific technological means

The Directive does not require:

- A SIEM.
- A SOC.
- An OT IDS.
- An XDR solution.
- Microsegmentation,
  etc.

It imposes objectives, not tools.

NIS2 imposes accountability, methodology, documentation, and the ability to demonstrate control of risk - but not certification, a single standard, or a fixed architecture.

//

Hiden in free Sample

//

Chapter 5 — Industrial Cyber Risk Management: The Compass of Strategic Decision-Making

5.1 Introduction – From Intuition to Informed Decision-Making

In an industrial environment, no organization can protect everything to the same level:

- 24/7 availability constraints.
- Safety requirements.
- Limited budgets.
- Architectures that are sometimes old and complex.

So the real question is not:

“Are we completely secure?”

(Because the honest answer will always be no), but rather:

“Have we invested our resources in the most effective way to reduce the risks that are most critical to our business?”

Cyber risk management provides the framework needed to answer that question:

identify what truly matters, understand threats and vulnerabilities, estimate possible impacts, prioritize actions, and justify decisions to management.

This chapter proposes a structured approach, inspired by frameworks such as ISO 31000, ISO 27005, ISA/IEC 62443-3-2, and industry practice, to make risk management the compass of strategic decision-making in OT cybersecurity.

5.2 The Fundamental Principles of Risk Management

Risk management is not a one-off theoretical exercise, performed once for an audit and then forgotten.
It is a continuous process that is repeated and refined over time.

5.2.1 The Risk Lifecycle

Risk management can be represented as a cycle (a PDCA-type cycle):