IEC 62443: a walkthrough

Six pieces working through the international standard for industrial control system cybersecurity — from foundational terminology to system design, OEM obligations, NIS2 mapping, and a one-page evidence pack.

Version 1.0.0 — 2026-05-18
DOI: 10.5281/zenodo.20276993

Six pieces working through IEC 62443 — the international standard for industrial control system cybersecurity — from foundational terminology to system design, OEM obligations, NIS2 mapping, and a one-page evidence pack.

Rajesh Khanikar
ORCID: 0009-0008-8976-4491
Version 1.0.0 — 2026-05-18

DOI: 10.5281/zenodo.20276993 (this version)
Canonical: https://khanikar.com/series/iec-62443/

To cite this pack:

> Khanikar, R. (2026). *IEC 62443: a walkthrough* (Version 1.0.0). https://doi.org/10.5281/zenodo.20276993. Licensed under CC BY 4.0.

This pack is offered as editorial guidance for technical and procurement audiences. It does not constitute legal, regulatory, or professional advice; the author is not a lawyer, an auditor, or a certification body. The content is provided without warranty of any kind, express or implied — no guarantee of accuracy, completeness, currency, or fitness for any particular product line, project, or jurisdiction. Readers must verify against the primary sources — IEC's published standards — and consult qualified professionals before acting on anything in this pack. The IEC standards are the canonical text; this pack reflects their content as of the publication date above, but standards may have been amended since. The author accepts no responsibility or liability for any decision, action, or omission made in reliance on this content.

Corrections, errata, and substantive disagreements are welcome at linkedin.com/in/rajeshkhanikar.

Contents

IEC 62443-1-x: the words everyone argues about

14 May 2026 · 30 min read · #compliance #security #industrial #iec-62443

Two people stood next to a 33 kV switchgear room at a 220 MW solar plant last autumn, both holding the same audit checklist, both fluent in the same standard, and both completely talking past each other. The certification body's lead auditor said the inverter SCADA "needed SL 3." The integrator's project manager replied, calmly, "we're already SL 3 — the components are certified." The plant's OT engineer, who had to live with whatever they agreed, asked the only question that mattered: "SL 3 of what? Target, achieved or capability? For which zone?"

That is the conversation `IEC TS 62443-1-1:2009` was written to prevent. It usually fails to prevent it — not because the standard is bad, but because almost nobody on a real site has actually read it. They've read a vendor white paper that quoted it, a NIS2 mapping table that paraphrased it, or a slide deck that confused it with `IEC 62443-3-3`. The vocabulary then drifts, the audit grinds, and the asset owner pays for the misunderstanding.

This post is a slow, deliberate walk through the **Part 1** documents of the ISA/IEC 62443 series — the foundation group. These are the documents that define what every other part of the series means by IACS, zone, conduit, security level, foundational requirement, essential function, asset owner, integrator and so on. If you've already read my walkthroughs on IEC 62443-2-x , IEC 62443-3-2 and 3-3 or IEC 62443-4-1 and 4-2 , this is the post that explains why those other posts spend so much time being careful about wording.

TL;DR

`IEC 62443-1-x` is the **foundation** group of the IEC 62443 series. The only document in this group that is presently a published IEC deliverable on the IEC webstore as a standalone text is `IEC TS 62443-1-1:2009` (a Technical Specification, edition 1.0, dating from July 2009) and the newer `IEC TS 62443-1-5:2023` (Technical Specification on security profiles). Parts `1-2` (master glossary), `1-3` (system security conformance metrics) and `1-4` (IACS security lifecycle and use cases) are still under development by ISA99 / IEC TC65 WG10 — they are referenced throughout the series but you cannot, today, buy them as finished documents. That fact alone resolves a surprising number of workshop arguments. Everything below explains the rest.

1. The series map — where 1-x sits and which other parts depend on it

The IEC 62443 series is organised, formally, into four document groups. The ISA99 committee — co-publishing with IEC TC65/WG10 — describes them as:

- **General (1-x):** the terminology, the reference model, the conceptual scaffolding. This is where `IEC 62443-1-1` lives.
- **Policies and procedures (2-x):** what an asset owner organisation has to do to run a programme. `IEC 62443-2-1:2024` is the live anchor here; `2-3`, `2-4` and the upcoming `2-2` (currently `IEC PAS 62443-2-2:2025`) flesh it out.
- **System (3-x):** technical system-level requirements. `IEC 62443-3-2` is the risk-assessment / zoning standard, `IEC 62443-3-3` is the catalogue of system requirements tied to the seven foundational requirements.
- **Component (4-x):** secure development lifecycle for product suppliers (`IEC 62443-4-1:2018`) and component-level technical requirements (`IEC 62443-4-2:2019`).

A more recent fifth group, **Profiles (6-x and the planned 5-x family)**, was added once IEC formally designated the series as a horizontal standard in 2021 — meaning vertical-industry committees should reference 62443 rather than write their own. That horizontal designation is why `IEC TS 62443-1-5:2023` exists: it specifies the scheme by which sector-specific profiles get written and accepted.

Every later document in the series points back to `IEC 62443-1-1` for definitions. When `IEC 62443-3-3` writes "SR 1.1 Human user identification and authentication … shall be capable of … Security Level 2", the word "Security Level" is not defined there. It is defined in `1-1`. When `IEC 62443-2-1:2024` talks about an "asset owner" and a "service provider," those roles are defined in `1-1`. When `IEC 62443-4-2` rates a component at SL-C 2 for FR3, the meaning of foundational requirement, capability, level and component all trace back to `1-1`. The whole series hangs from this hook.

That has two practical consequences. First — if you are designing a programme today, you must own and read `IEC TS 62443-1-1:2009`. Not summaries of it. The actual PDF from the IEC webstore, publication 7029 . Second — you must accept that the document is sixteen years old and the second edition is still being written. Some of the language has moved on (the series talks about "service providers" and "automation solutions" with more precision now), but the definitions of zones, conduits, SL-T/SL-A/SL-C and the seven FRs in `1-1` remain the canonical ones until the second edition lands.

2. IACS, ICS, OT, ICS-cybersecurity — what the standard actually says

This is the first thing people get wrong, and the first thing `IEC 62443-1-1` defines.

IACS — Industrial Automation and Control System. This is the 62443 term of art. `IEC TS 62443-1-1:2009` defines IACS broadly: a collec-

tion of personnel, hardware, software and policies involved in the operation of an industrial process and that can affect or influence its safe, secure and reliable operation. Crucially, **personnel and policies are inside the boundary of an IACS.** It is not "the network." It is not "the controllers." It is the operating socio-technical system. `IEC 62443-2-1:2024` reinforces this — its scope explicitly inherits "the broad definition and scope of what constitutes an IACS as described in `IEC TS 62443-1-1`."

ICS — Industrial Control System. A narrower term. Generally used to denote the control technology subset — PLCs, DCSs, SCADA, RTUs, HMIs, the engineering workstations and the industrial network that ties them together. In the older `IEC TR 62443-3-1:2009`, the language used was "ICS" because the term predates the IACS-centric reframing. In modern 62443 documents the preferred umbrella term is IACS, with ICS appearing as a near-synonym in references to the control technology layer.

OT — Operational Technology. Not an IEC 62443 term. OT is the term used by NIST SP 800-82 Rev. 3 (September 2023) , whose title is "Guide to Operational Technology (OT) Security." NIST defines OT as "programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment)." Revision 3 widened the scope from the older "ICS" framing of revisions 1 and 2 because building automation, transportation, physical access control and environment monitoring did not fit comfortably under "industrial." OT is the superset of ICS and the closest external term to IACS, but OT does not include personnel and procedures — IACS does.

ICS-cybersecurity / OT-cybersecurity / IACS security. Used interchangeably in practice. Internally to 62443 they are all "IACS cybersecurity."

The argument this resolves: at the audit I mentioned, the question "is the engineering laptop part of the system?" was disputed. The integrator argued no — it's IT, not an inverter. The asset owner argued yes — it programmes the inverters. The standard agrees with the asset owner. Under `IEC 62443-1-1`, the engineering laptop is part of the IACS because it influences safe, secure and reliable operation. The label on its asset tag does not exempt it.

In renewable-energy work specifically, this matters constantly. A solar plant's IACS includes the inverter SCADA, the meteorological-station data path, the protection relays in the 33 kV switchgear, the BESS battery management system, the network gear at the substation, the engineering laptops the O&M team plug in monthly and the OEM's remote-support VPN. None of those can be argued out of scope on the grounds that they are "just IT" or "just safety."

3. The reference model (Levels 0-5) and how it relates to Purdue

`IEC TS 62443-1-1:2009` lays out a hierarchical reference model used throughout the series. It is informed by the Purdue Enterprise Reference Architecture (PERA) from Purdue University's PLAIC programme, but it is not identical to it. The 62443 reference model defines functional levels — abstract bands — that describe where activities sit in the automation hierarchy.

The levels, as used across the series:

- **Level 0 — Process.** The physical equipment under control: turbines, transformers, inverters, valves, motors, the actual equipment doing work.
- **Level 1 — Basic control.** Sensors, actuators, controllers (PLCs, IEDs, drive controllers, BMS controllers). Real-time, deterministic.

- **Level 2 — Area / supervisory control.** HMIs, local SCADA front-ends, plant historians' acquisition layer. Operator-facing, still real-time-adjacent.
- **Level 3 — Site / operations control.** Plant-level systems: site historian, MES-equivalents, engineering workstations, plant-wide SCADA. Still inside the IACS.
- **Level 3.5 — DMZ.** The industrial demilitarised zone. Brokered data exchange between operations and the corporate enterprise. Not present in the original Purdue model; added in industrial-cybersecurity practice and treated by 62443 as a zone boundary.
- **Level 4 — Site business planning and logistics.** ERP, MES proper, business systems at the site level.
- **Level 5 — Enterprise.** Corporate IT.

`IEC 62443-1-1` is careful about one point that almost everyone gets wrong: **levels are functional, not topological.** Two devices on the same physical VLAN can sit at different reference-model levels. A PLC at Level 1 can be in the same room as a historian at Level 3. The reference model tells you what the device does, not where its Ethernet cable terminates.

The relationship with Purdue is therefore "compatible, not identical." Purdue gave us the hierarchical metaphor. 62443 added security-zone reasoning on top — zones do not have to follow Purdue levels, although in most well-designed plants they end up doing so for very good reasons.

Why this matters for renewable plants: a modern solar site rarely fits the textbook Purdue diagram. Inverter manufacturers push cloud-connected telemetry directly out of Level 1 devices. BESS systems often arrive with their own walled-garden cloud at "Level 3-ish" without ever transiting a plant historian. Wind turbines connect through OEM remote-support tunnels that bridge Levels 1 and 5 and pretend they

don't. `IEC 62443-1-1` lets you describe these architectures honestly — by zone and conduit, with explicit reference-model levels for each function — without forcing a clean Purdue picture that has never matched reality.

4. Zones and conduits — and what counts as a zone boundary

The single most consequential pair of definitions in `IEC TS 62443-1-1:2009`:

- A **security zone** is a grouping of logical or physical assets that share common security requirements.
- A **conduit** is a logical grouping of communication channels — sharing common security requirements — that connects two or more zones.

Three things follow that catch people out.

First — zones group by security requirement, not by topology or function alone. A zone is whatever set of assets you can defensibly argue needs the same protection, the same trust, the same monitoring, the same access regime. Two physically separated wind-turbine arrays at different voltages can be one zone if they share security requirements. A single substation control building can contain three zones (relay protection, station SCADA, telecom gateway) if those functions warrant different protection levels. The rule of thumb I use on audits: if two assets would, on this site's risk register, ever justify different controls — they are not in the same zone.

Second — conduits are not "the firewall." A conduit is a logical construct: the set of communication channels with shared security needs that crosses a zone boundary. The firewall, switch, data diode or VPN concentrator is a component of the conduit, not the conduit itself. This is why `IEC 62443-3-3` requirements apply to conduits as well

as zones: a conduit has SL targets, capabilities and an achieved level of its own.

Third — "trust zone" is not the same as "security zone." A trust zone (in the IT zero-trust sense) is a boundary at which identity and policy are re-evaluated. A 62443 security zone is a boundary at which security requirements change. They overlap but are not synonymous. Saying "we've zero-trusted the OT network so we don't need zones" is a category error. The 62443 zone definition still applies; zero trust is one possible means of enforcing the conduit between two zones.

A practical zone-boundary checklist for a hybrid renewable site:

1. Where does the cyber-physical risk profile change? (e.g. moving from inverter control to battery thermal management to grid protection)
2. Where does the population of users / vendors / service providers change?
3. Where do regulatory or contractual obligations differ (e.g. grid-code-mandated systems vs. owner-operated systems)?
4. Where does the consequence of compromise change in kind (revenue loss vs. safety vs. grid stability)?

Each affirmative answer is a candidate zone boundary. Each is, by `IEC 62443-1-1`, the basis for a conduit.

This is the input that IEC 62443-3-2 consumes when it asks for a partitioned system under consideration (SuC) with documented zones and conduits. The reasoning lives in `1-1`; the methodology lives in `3-2`; the control catalogue applied to each zone and conduit lives in `3-3`.

5. Security Levels — SL-T, SL-A, SL-C, and the often-confused SL 1-4 numeric scale

This is the section that, if I were writing this post for one person only, would be the entire post.

`IEC TS 62443-1-1:2009` defines a Security Level as a measure of confidence that an IACS is free from vulnerabilities and functions in the intended manner. It then defines four numeric bands:

- **SL 1** — protection against casual or coincidental violation.
- **SL 2** — protection against intentional violation using simple means with low resources, generic skills and low motivation.
- **SL 3** — protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills and moderate motivation.
- **SL 4** — protection against intentional violation using sophisticated means with extended resources, IACS-specific skills and high motivation.

These four levels describe threat actor capability. They do not, on their own, describe a plant, a product, a zone or a control.

The next step is where everyone goes wrong. The series defines three types of Security Level, and the numeric scale (1-4) applies to each:

- **SL-T (Target)** — the security level a particular zone or conduit needs to achieve based on its risk assessment. SL-T is selected, on a per-zone, per-FR basis, by the asset owner in the context of IEC 62443-3-2 . The output of risk assessment is an SL-T vector — seven numbers, one per foundational requirement — for each zone and each conduit.
- **SL-C (Capability)** — the security level a component or system is capable of meeting when properly configured and integrated. SL-C is what a product supplier declares about a device, tested against

IEC 62443-4-2 for components or `IEC 62443-3-3` for systems. A certified PLC might be SL-C 2 across all seven FRs, or SL-C 3 for FR1 and SL-C 2 for everything else. The certificate carries the vector.

- **SL-A (Achieved)** — the security level the as-built, as-operated zone or conduit actually delivers in service. SL-A is measured (or estimated) after design, integration, commissioning and operational handover. It is, in practice, what your audit evidence is supposed to prove.

The chain that the standard wants you to walk is therefore: **SL-T (from risk) → choose components / system with sufficient SL-C → design and operate to deliver SL-A ≥ SL-T**. If SL-A falls short of SL-T, you must either accept residual risk, apply compensating countermeasures, or change the design.

This is why the auditor and the integrator were arguing past each other in the opening scene. The integrator said "we're SL 3" meaning SL-C 3 for the components they shipped. The auditor said "we need SL 3" meaning SL-T 3 for the zone. Neither had measured SL-A. A component with SL-C 3 dropped into a zone with SL-T 3 does **not** automatically produce SL-A 3 — that depends on configuration, integration, the surrounding compensating countermeasures, and whether the operational practices (covered in IEC 62443-2-1:2024) actually sustain the capability.

Three further traps the vocabulary still doesn't fully resolve:

- **SL is per foundational requirement, not a single scalar.** Saying "we're SL 2" without a vector across FR1-FR7 is, strictly, not a 62443 statement. The standard expects a tuple. In practice many programmes report a single dominant value plus exceptions; that's defensible if the exceptions are listed.

- **IACS-wide SL vs zone SL.** There is no such thing as an "IACS-wide SL" in `IEC 62443-1-1`. SLs apply to zones and conduits. An IACS is a collection of zones, each with its own SL-T vector. A single-number SL for an entire plant is a marketing artefact.
- **Maturity level (ML 1-4) is not Security Level.** Maturity Levels appear in `IEC 62443-2-4` (service-provider requirements) and `IEC TS 62443-6-1:2024` (the evaluation methodology for 2-4). ML measures the maturity of a process. SL measures the security level of a zone, conduit, system or component. They are different scales for different things and are not interchangeable.

6. The seven Foundational Requirements (FR1-FR7)

`IEC TS 62443-1-1:2009` defines seven foundational requirements. They are the columns of the matrix that the rest of the series fills in.

1. **FR1 — Identification and Authentication Control (IAC).** Who or what is requesting action, and have they proven it?
2. **FR2 — Use Control (UC).** Are they permitted to do the requested action?
3. **FR3 — System Integrity (SI).** Is the integrity of code, data and configuration maintained against intentional and unintentional change?
4. **FR4 — Data Confidentiality (DC).** Is information at rest and in transit protected from disclosure where required?
5. **FR5 — Restricted Data Flow (RDF).** Are data flows partitioned along zone and conduit boundaries?
6. **FR6 — Timely Response to Events (TRE).** Are security-relevant events detected, logged, alerted and responded to in time?
7. **FR7 — Resource Availability (RA).** Are essential functions kept available under stress, attack or degradation?

Two important things about the FRs that the vocabulary still trips people on.

FRs are not controls. They are objectives. `IEC 62443-3-3` decomposes them into System Requirements (SRs) and Requirement Enhancements (REs), and IEC 62443-4-2 decomposes them again into Component Requirements (CRs). The phrase "we are compliant with FR3" is meaningless on its own — what is meaningful is "we meet SRs 3.1 through 3.9 at SL-C 2 in zone X, with REs for 3.4 and 3.8 applied." If a vendor's data sheet just says "compliant with FR3" with no SR / CR detail and no SL vector, treat that as marketing copy.

The ordering of FRs is not a priority order. FR1 is not "more important" than FR7. In OT, the opposite is often true: FR7 (resource availability) and FR3 (system integrity) frequently outrank FR4 (data confidentiality) in the risk register. The FRs are an enumeration, not a ranking.

The seven FRs are also the dimensions of every SL vector. When an integrator hands you a `IEC 62443-3-3` compliance matrix for a system, it should be a 7-column grid keyed to FR1 through FR7 with an SL-C value in each cell. When the asset owner derives SL-T from `IEC 62443-3-2`, the output is the same shape. The reason for matching shapes is so SL-C and SL-T can be compared component-by-component.

7. Roles — asset owner, system integrator, product supplier, service provider

`IEC 62443-1-1` introduces the role taxonomy that the rest of the series operationalises. Subsequent ISA99 work and the ISAGCA Quick Start Guide sharpen these into four principal roles:

- **Asset owner.** The organisation accountable for the IACS in operation. In renewables this is the IPP, the utility, the asset-management company — whoever bears operational and

regulatory accountability for the plant. Asset-owner-facing requirements live primarily in IEC 62443-2-1:2024 .

- **Product supplier.** The organisation that designs, develops and supports a product — a component or a system — used in the IACS. Product suppliers are addressed by IEC 62443-4-1:2018 (development-process requirements) and IEC 62443-4-2:2019 (component-level technical requirements) .
- **System integrator.** The organisation that takes products from suppliers and assembles them into an automation solution for an asset owner. Integrators are addressed by `IEC 62443-2-4:2023` (security programme requirements for IACS service providers) in their integration role, and by IEC 62443-3-2 and 3-3 where they execute the design and verification on behalf of the asset owner.
- **Service provider.** The organisation that operates, maintains, monitors or otherwise services the IACS after handover. `IEC 62443-2-4` covers them too — explicitly distinguishing between integration service providers and maintenance service providers.

The maintenance-service-provider role is the one that's most often invisible in renewable contracts and the one that causes the most pain at year-three audits. The OEM that ships you the turbines is a product supplier. The EPC who built the wind farm is a system integrator. The O&M contractor who comes on site every quarter — and the OEM remote-support team behind a VPN tunnel — is a maintenance service provider, and `IEC 62443-2-4` requirements apply to them. If your O&M contract is silent on cybersecurity capability requirements, you've shifted the maturity rating of your programme down. That is an `IEC 62443-2-1` problem caused by a vocabulary problem from `1-1`.

The argument this vocabulary resolves: when "the vendor" is doing remote support on a Sunday night to recover an inverter, is that a product supplier action or a service provider action? The answer matters because the requirement sets are different. Under `IEC 62443-1-1` it

is a service-provider action (they are performing operational work on the as-built solution), and your contract should reflect `2-4` capability requirements.

8. Essential functions and compensating countermeasures

Two more `IEC 62443-1-1` terms that everyone uses sloppily.

Essential function. A function whose loss of operation, or operation in a degraded state, could cause unacceptable consequence to safety, integrity or availability. In a solar plant, essential functions include: protection tripping at the 33 kV / HV interface, BESS thermal runaway shutdown, primary frequency response (if the site provides ancillary services), and the safety-related controls of any high-voltage switchgear. Essential function is not the same as important function. The bar is "loss is unacceptable," not "loss is inconvenient." `IEC 62443-3-3` explicitly says certain SRs apply more strictly where essential functions are at stake — for example, requirements around denial-of-service tolerance lean heavily on the essential-function concept.

The practical consequence: when you draw the zone diagram for IEC 62443-3-2 , every essential function must end up identified and traceable to a zone. SL-T for that zone is then influenced by the consequence of compromise of that essential function. A zone that hosts only "important" functions can have a lower SL-T than one hosting essential functions.

Compensating countermeasure. A control applied because the inherent control cannot be implemented or is impractical. The standard's logic is: if you cannot meet an SR directly inside a zone, you can apply a compensating countermeasure elsewhere (often in the surrounding conduit, or by procedural means) provided you can argue the residual risk is equivalent. Compensating countermeasures are not "we skipped it because it was hard." They are documented,

justified and traceable. A reasonable example: a legacy inverter controller that cannot enforce strong human-user authentication directly (FR1 / SR 1.1) can be compensated by a jump host inside the conduit, plus an admin-procedure that proves which named human used which session — provided that compensation is documented, tested and reviewed at the frequency the security programme requires.

The argument this resolves: when a procurement team writes "the system shall comply with `IEC 62443-3-3` SL 2 across all FRs without exceptions," they have written a procurement requirement that may be impossible to satisfy with the field equipment that physically exists. The standard expects exceptions, expects compensating countermeasures, and expects them to be argued on paper. Buying as if compensating countermeasures were a sign of weakness rather than a normal output of design is itself a misreading of `IEC 62443-1-1`.

9. The security lifecycle (from 1-4) — assess, design, implement, maintain

`IEC TR 62443-1-4` — IACS security lifecycle and use cases — is a Technical Report, currently still in development at the ISA99 / IEC TC65 WG10 level. Drafts have circulated within the committee since around 2013. It is intended to provide a detailed description of the underlying lifecycle that the rest of the series assumes, with worked use cases. It is not, as of writing, a finished IEC deliverable on the IEC webstore . What is published — and widely cited — is the ISAGCA Security Lifecycles whitepaper by ISA's Global Cybersecurity Alliance, which captures the same conceptual content pending the formal TR.

The lifecycle the series uses has four broad phases:

1. **Assess.** Risk assessment, definition of the SuC, zoning and conduit partitioning, derivation of SL-T per zone and conduit per FR. This is the home of IEC 62443-3-2 and the entry point for any new

project or major modification. IEC 62443-2-1:2024 makes assess-phase activities a programme requirement for asset owners.

2. **Design and implement.** Selection of products and integrators with adequate SL-C against SL-T, design of compensating countermeasures, factory acceptance test (FAT) and site acceptance test (SAT) including cybersecurity test cases, commissioning. `IEC 62443-3-3` is the design-verification reference; IEC 62443-4-2 is the component-selection reference; `IEC 62443-2-4` is the integrator capability reference.
3. **Operate and maintain.** Patch management, account hygiene, monitoring, incident response, periodic re-assessment, supply-chain controls for maintenance service providers. IEC 62443-2-1:2024 is the operating-phase reference. `IEC TR 62443-2-3:2015` covers patch management.
4. **Decommission.** Secure handling of credentials, configurations, decommissioned assets, residual data. Often the most neglected phase. The maintenance documentation says "decommission per OEM instructions" and the OEM instructions are silent on cybersecurity.

The lifecycle in `1-4` and ISAGCA's whitepaper is not linear. It is the intersection of three lifecycles: the product lifecycle (owned by product suppliers), the automation-solution lifecycle (owned by integrators) and the operations lifecycle (owned by asset owners and service providers). Where they intersect is where contracts, evidence and handovers live. That's why renewable-energy plant cybersecurity is so contract-driven: the lifecycle model in `1-4` is the only way to map who has to prove what to whom at which milestone.

The argument this resolves: "we did `IEC 62443-3-2` at the design phase, so we're compliant." No — `3-2` is one activity in the assess phase. The lifecycle continues for the next twenty years. A zoning document from

2024 is stale by 2028 unless re-validated. The lifecycle framing in `1-4` is what forces that continual re-validation into the contract.

10. Metrics (1-3) — what "compliance metric" attempts and why it is hard

`IEC 62443-1-3` — System security conformance metrics (sometimes written as "compliance metrics" in older committee correspondence; the published title uses conformance) — is under development as a Technical Report. Its objective: define a methodology to derive quantitative metrics from the process and technical requirements that the rest of the series specifies. In plain terms — turn "comply with `3-3` SR 1.1 at SL-C 2" into a number you can measure, report and trend.

This is harder than it sounds, and the reasons it's hard are worth being honest about:

- **Most 62443 requirements are capability statements, not measurements.** "The system shall be capable of human-user identification and authentication" is a binary at first glance, but capability under different operational conditions is not. Does a capability that requires manual configuration count? Only when configured? Only when audited?
- **SL is not a metric, it is a level.** Turning a level into a metric requires deciding what proportion of requirements at that level must be met, with what evidence, at what frequency. Different organisations have different answers, and the standard is rightly reluctant to mandate one universal answer.
- **Asset owners want time-series metrics.** "How is our 62443 posture trending quarter on quarter?" is a perfectly reasonable executive question. The 62443 framework, born from engineering rather than from information-security management, has historically been better at point-in-time conformance than at time-series telemetry.

- `IEC 62443-2-2` **overlaps.** The Protection Scheme (SPS) work in the current `IEC PAS 62443-2-2:2025` introduces security programme ratings (SPR) which provide a related but separate measurement framework. The relationship between `1-3` metrics and `2-2` SPRs has been an active area of committee work.

Until `1-3` lands as a published TR, asset owners build their own metrics. Reasonable choices include: percentage of zones with current `3-2` documentation; percentage of components with SL-C ≥ SL-T per FR; percentage of maintenance service providers with documented `2-4` capability; mean time from CVE publication to patch verification; percentage of essential functions with tested fallback procedures. None of those are 62443-mandated, but each is defensible and traceable to a `1-1` concept.

The argument this vocabulary resolves: when management asks "are we 62443 compliant — yes or no?" you can correctly answer "the series doesn't work that way." `IEC 62443-1-1` does not define a single binary state of compliance for an IACS. It defines roles, capabilities, levels and zones, each of which can be assessed. A 62443 programme in IEC 62443-2-1 can be conformant. A component can be SL-C certified. A zone can have an SL-A that meets its SL-T. The plant as a whole is the sum of those statements, not a single yes/no. Pretending otherwise is what produces the unfortunate sales pitch "we're 62443 compliant" — which is usually short for "we sell a product that someone certified once."

11. The arguments this vocabulary still doesn't resolve

For all that `IEC TS 62443-1-1:2009` settles, plenty of arguments remain genuinely open. Some are about the world having moved on since 2009; some are about gaps the second edition is meant to close; some are about places where the standard is intentionally silent.

Cloud and IIoT. `IEC 62443-1-1` was written before "the cloud" was a routine deployment target for industrial telemetry. Where does AWS IoT Core sit on the reference model? Is it Level 3? Level 4? Level 5? Is the OEM's cloud a zone of the IACS at all, given that the asset owner does not run it? The forthcoming `IEC TR 62443-1-6` (Application of the ISA/IEC 62443 series to the Industrial Internet of Things) is intended to address exactly this. Until it lands, asset owners deal with it case by case — most commonly by treating the cloud endpoint as a zone owned by a service provider with a defined conduit to the on-site IACS.

Wireless and 5G. Same problem. Wireless links are conduits with peculiar physical-layer threat models. The series broadly accommodates them, but the practical question of whether a 5G slice is a conduit or a zone is unresolved in published text.

Safety-security interaction. `IEC 61511` (functional safety) and `IEC 62443` (cybersecurity) overlap explicitly at the safety-instrumented system. Where the safety lifecycle and the security lifecycle disagree — for example, on patching of safety PLCs — the standards do not perfectly reconcile. Recent ISAGCA work and `IEC TR 63069:2019` provide partial guidance. The argument continues in real audits.

Horizontal designation and sector profiles. The 2021 designation of 62443 as a horizontal standard means vertical-sector committees should reference it rather than redefining its terms. `IEC TS 62443-1-5:2023` formalises the scheme for sector profiles. But the content of sector profiles for renewable energy, water, building automation, medical devices and so on is still being written, and the meaning of "SL-T 2" in a hospital differs materially from "SL-T 2" on a wind farm. The vocabulary holds; the calibration differs.

Second edition of 1-1. A second edition has been circulating for committee review since 2021. It will refine some definitions, add ontology-driven precision (the WG5TG3 consistency task group has

done substantial work on this) and reflect lessons from the rest of the series. Until it is published, `IEC TS 62443-1-1:2009` is the authoritative reference, and there is some risk that conscientious readers find local divergence between the 2009 text and newer parts.

Mandatory or not? `IEC 62443` is not, by itself, a law anywhere. The European NIS2 Directive names "European standards and specifications relevant to security of network and information systems" — and `IEC 62443` is widely cited as the most-relevant reference for the OT scope, but the directive does not mandate 62443 by document number. Norway, where I work, is transposing NIS2 with similar latitude. The EU Cyber Resilience Act imposes binding cybersecurity essential requirements on products with digital elements; harmonised standards under the CRA will lean heavily on 62443-4-1 and 4-2, but again, document numbers are not in the legal text. For renewable-energy operators in Europe, the practical answer is: 62443 is voluntary by name but functionally required by procurement, insurance, regulator expectation and supply-chain pressure. See my walkthroughs on NIS2 applicability and CRA applicability for the detail.

Red flags in conversation

A short field guide. These are the phrases that, when I hear them in a workshop or an audit, tell me the speaker has not read `IEC TS 62443-1-1:2009` recently and probably has not read it at all.

- **"We're SL 3 compliant."** Compliant against what? Target, capability or achieved? For which zone? For which FRs? On what evidence? Without those qualifiers it's a marketing phrase.
- **"The whole plant is SL 2."** There is no plant-wide SL in `IEC 62443-1-1`. SL applies to zones and conduits.
- **"OT and IACS are the same thing."** They overlap, but OT (per NIST SP 800-82r3) is a broader term and excludes the personnel

and process scope that `IEC 62443-1-1` includes in IACS. They are not synonyms.

- **"FR3 is a control we implemented."** FR3 is a foundational requirement — an objective. Controls are SRs, REs and CRs underneath it. If someone calls an FR a control they have skipped a level of the standard.
- **"Our PLC is 62443-certified."** Against which part? `4-1`? `4-2`? At which SL-C? Across which FRs? "62443-certified" is not a specification.
- **"Zones are just VLANs."** Zones are groupings by shared security requirement. VLANs are one possible enforcement mechanism for the conduit between zones. The two concepts are at different levels of abstraction.
- **"We don't need compensating countermeasures, we're fully compliant."** A 62443 design with no documented compensating countermeasures on a real industrial site is almost always wishful thinking, not rigour.
- **"`IEC 62443-1-1` is just definitions, we can skip it."** It defines every term the rest of the series rests on. Skipping it is how the audit conversation in this post's opening scene happens.
- **"The integrator handed over an SL-T document, so we're done."** SL-T is the input to design, derived from risk. SL-A is what you must measure post-commissioning and re-measure through the lifecycle. SL-T on its own proves intent, not delivery.
- **"Maturity level 3 equals security level 3."** They are different scales for different objects. ML measures process maturity; SL measures zone, conduit, system or component security.

Each of these red flags points back to a section of `IEC 62443-1-1`. The remedy is rarely to argue louder; it is to open the document and read the relevant definition together. The vocabulary, once shared, re-

moves about two-thirds of the disagreements that consume audit time.

FAQ

What is IEC 62443-1-1?

`IEC TS 62443-1-1:2009` is the foundation Technical Specification of the IEC 62443 series. Published by IEC in July 2009 (edition 1.0), it defines the terminology, concepts and reference models that the rest of the series uses — including IACS, zones, conduits, security levels (SL-T, SL-A, SL-C), the seven foundational requirements (FR1-FR7) and the principal roles (asset owner, product supplier, integrator, service provider). It is available from the IEC webstore as publication 7029 . A second edition has been in committee review at ISA99 / IEC TC65 WG10 since 2021.

What is the difference between SL-T and SL-C?

SL-T (Target) is the security level a particular zone or conduit needs to achieve, derived from risk assessment under IEC 62443-3-2 . SL-T is an asset-owner output: it says "this zone needs SL 3 across these FRs because of the risk profile here." **SL-C (Capability)** is the security level a component or system is capable of meeting when properly configured. SL-C is a product-supplier output, certified against IEC 62443-4-2 (components) or `IEC 62443-3-3` (systems). A component with SL-C 3 dropped into a zone with SL-T 3 does not automatically deliver SL-A (Achieved) 3 — that depends on configuration, integration, compensating countermeasures and operational practices.

Is IEC 62443 mandatory?

By itself, no. `IEC 62443` is a voluntary international standards series, not legislation. However, it is referenced or relied upon by a growing list of frameworks that are binding — the EU NIS2 Directive, the EU Cyber Resilience Act, sector regulators and national transpositions in countries including Norway. Procurement contracts, insurance re-

quirements and supply-chain expectations increasingly cite specific parts (commonly `IEC 62443-2-1`, `3-3`, `4-1` and `4-2`). The practical answer for an asset owner in critical infrastructure is: not mandatory by name, but very often mandatory by the things that are mandatory. See my posts on NIS2 applicability and CRA applicability for the full chain of reasoning.

Why isn't IEC 62443-1-2 (the master glossary) available?

Because, as of 2025-2026, it is still under development at ISA99 / IEC TC65 WG10. The ISAGCA Structuring the ISA/IEC 62443 Standards writeup notes that `1-2` "is a master glossary of terms and abbreviations used throughout the series" and that the committee intends to deliver it in an online format. Until it is published as a finished IEC deliverable, the authoritative definitions remain those given inside `IEC TS 62443-1-1:2009` and inside each numbered part's own definitions clause. Cross-reference with NIST SP 800-82 Rev. 3 is useful for OT/ICS terminology that touches but is not identical to 62443's IACS vocabulary.

How do zones and conduits relate to the Purdue model?

The Purdue Enterprise Reference Architecture (PERA) is a hierarchical functional model — Levels 0 through 5 — that describes where activities sit in an automation hierarchy. `IEC 62443-1-1`'s reference model is informed by Purdue but adds the security concepts of zones and conduits on top. A zone groups assets that share common security requirements; a conduit is the set of communication channels between zones. Zones do not have to align one-to-one with Purdue levels, although in well-designed plants they often do for sensible engineering reasons. The two models are complementary, not competing.

Further reading on this site: the management-system view is in IEC 62443-2-x: what asset owners must prove ; the system-design view is in IEC 62443-3-2 and 3-3: what asset owners and integrators must prove ; the product-supplier view is in IEC 62443-4-1 and 4-2: what OEMs must prove . Read them in any order — but read this one first, because it's the document the others assume you already understand.

IEC 62443-2-x: the management system behind a secure industrial plant

13 May 2026 · 26 min read · #compliance #security #industrial #iec-62443

Two of the other pieces in this series cover the technical dimension of IEC 62443. The 4-1 and 4-2 article looks at how an OEM proves their product is built securely and what their product can actually do. The 3-2 and 3-3 article looks at how the asset owner sizes the security requirement of their system and how the system integrator delivers against it. Together those four standards cover the design, the components and the delivered system. What they do not cover — and what the entire standards family is incomplete without — is the day-to-day running of things. The people who operate the plant, the procedures they follow, the policies that govern them, the patches that keep the system current, and the service providers who come on site to maintain it. That is the dimension addressed by IEC 62443 Part 2.

A useful way to see why this matters is by extending the building analogy from the previous article. If 3-2 is the architect's brief, 3-3 is the building code, 4-2 is the kitemark on each component, and 4-1 is the brick-factory's quality system, then **Part 2 is the hospital management system**. You can have the best architects, the strictest building code, the highest-rated components and the most rigorously controlled manufacturers, but if the hospital is then operated with sloppy hygiene, untrained staff, no audit trail of who did what, and no system for recalling faulty medical equipment, none of it will save you. Part 2 is what makes the construction matter in operation. It is the discipline that turns a secure design into a sustainably secure plant.

There are five active members of the Part 2 family — 2-1 through 2-5 — and they distribute neatly between two audiences. **The asset owner** is the audience for 2-1, 2-2 and 2-5, with 2-3 affecting them as

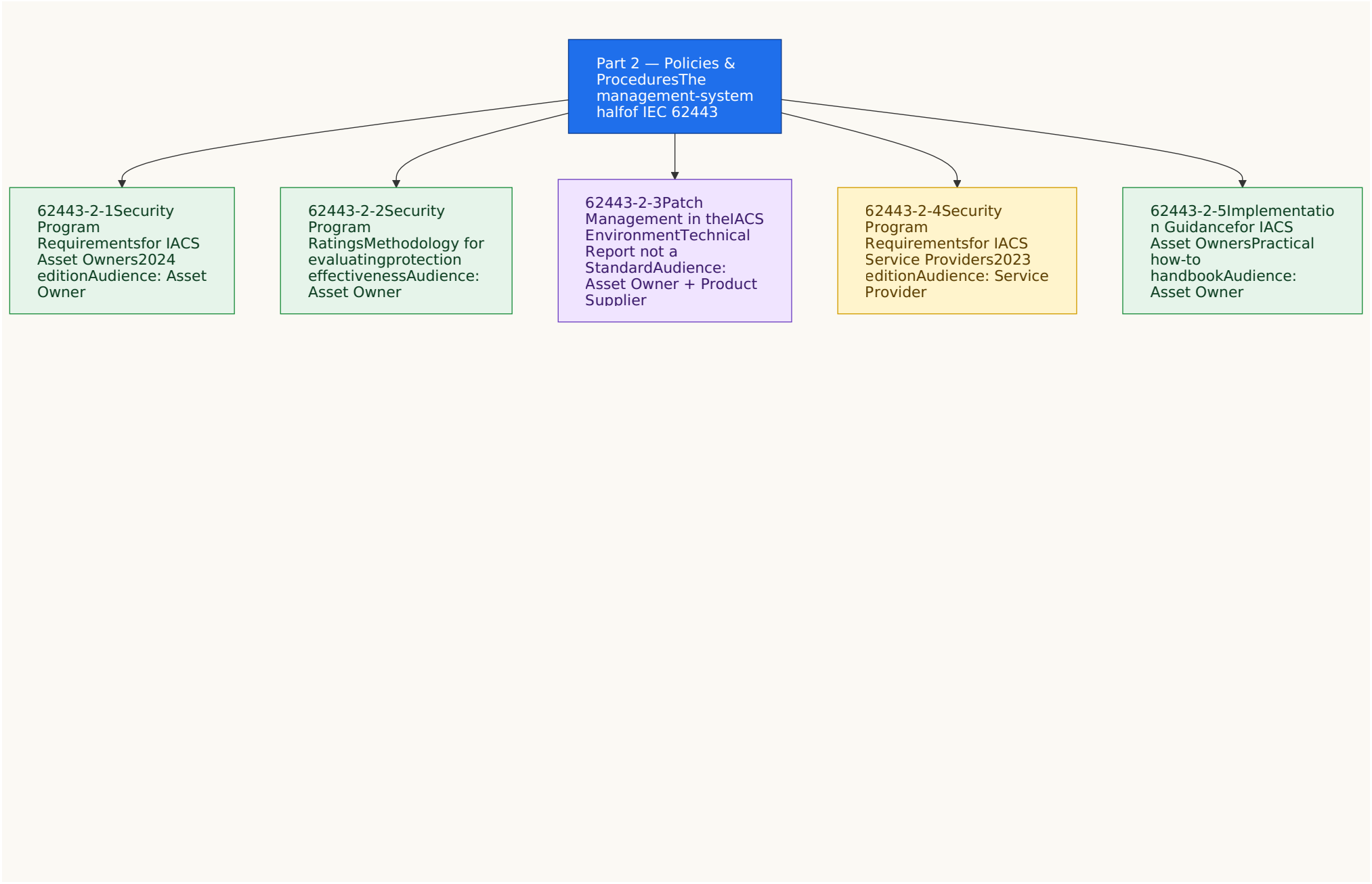
well. **The service provider** — by which the standard means system integrators, maintenance contractors, managed-service providers and similar third parties who work on or in your IACS — is the audience for 2-4. The product supplier appears in Part 2 only in a supporting role (mainly in 2-3, where they have to provide patch information for their products in a form their customers can actually use).

This becomes important in the EU regulatory context. Under NIS2 , the asset owner's Article 21 risk-management obligations and Article 21(2)(d) supply-chain duties land squarely on the territory 2-1 and 2-4 govern. Under the Cyber Resilience Act , Article 14 vulnerability reporting from the product supplier connects to the asset owner's patch programme that IEC TR 62443-2-3 codifies. The 2-x standards are the operational layer where EU regulatory demands meet OT reality.

This article works through each of the five sub-standards in turn, then ties them together and ends with a procurement and audit checklist.

The official standards are published by the IEC and co-branded by ISA. Primary sources for each: IEC 62443-2-1:2024 , ISA TR62443-2-2:2025 , IEC TR 62443-2-3:2015 , and IEC 62443-2-4:2015/AMD1:2018 . IEC 62443-2-5 is referenced in the family overview at ISA's 62443 series page .

The 2-x family at a glance


Part 2 — Policies & ProceduresThe management-system halfof IEC 62443
62443-2-1Security Program Requirementsfor IACS Asset Owners2024 editionAudience: Asset Owner
62443-2-2Security Program RatingsMethodology for evaluatingprotection effectivenessAudience: Asset Owner
62443-2-3Patch Management in theIACS EnvironmentTechnical Report not a StandardAudience: Asset Owner + Product Supplier
62443-2-4Security Program Requirementsfor IACS Service Providers2023 editionAudience: Service Provider
62443-2-5Implementatio n Guidancefor IACS Asset OwnersPractical how-to handbookAudience: Asset Owner

A quick orientation before we go into each in detail. Two of these — 2-1 and 2-4 — are full normative standards: they contain requirements that an organisation either meets or does not meet, and there are external certification schemes (more on these below) that can verify the claim. One of them — 2-3 — is a Technical Report, not a standard, which means it is guidance rather than auditable requirements; it is still important, but the bar for "compliance" is different. One — 2-5 — is implementation guidance: it tells you how to do what 2-1 says you must do. And one — 2-2 — is a relatively recent addition that provides a way to measure how good your security programme actually is once you have built it. Together they form a coherent management-system framework.

IEC 62443-2-1: the asset owner's security programme

IEC 62443-2-1, formally titled "Security program requirements for IACS asset owners", is the cornerstone of Part 2 and arguably the cornerstone of the asset owner's entire IEC 62443 obligation. The standard was first published in 2010 and was substantially rewritten in August 2024 as a second edition — an update that materially changed the structure of the requirements and aligns the standard more closely with how organisations actually run their security programmes today.

What it actually is

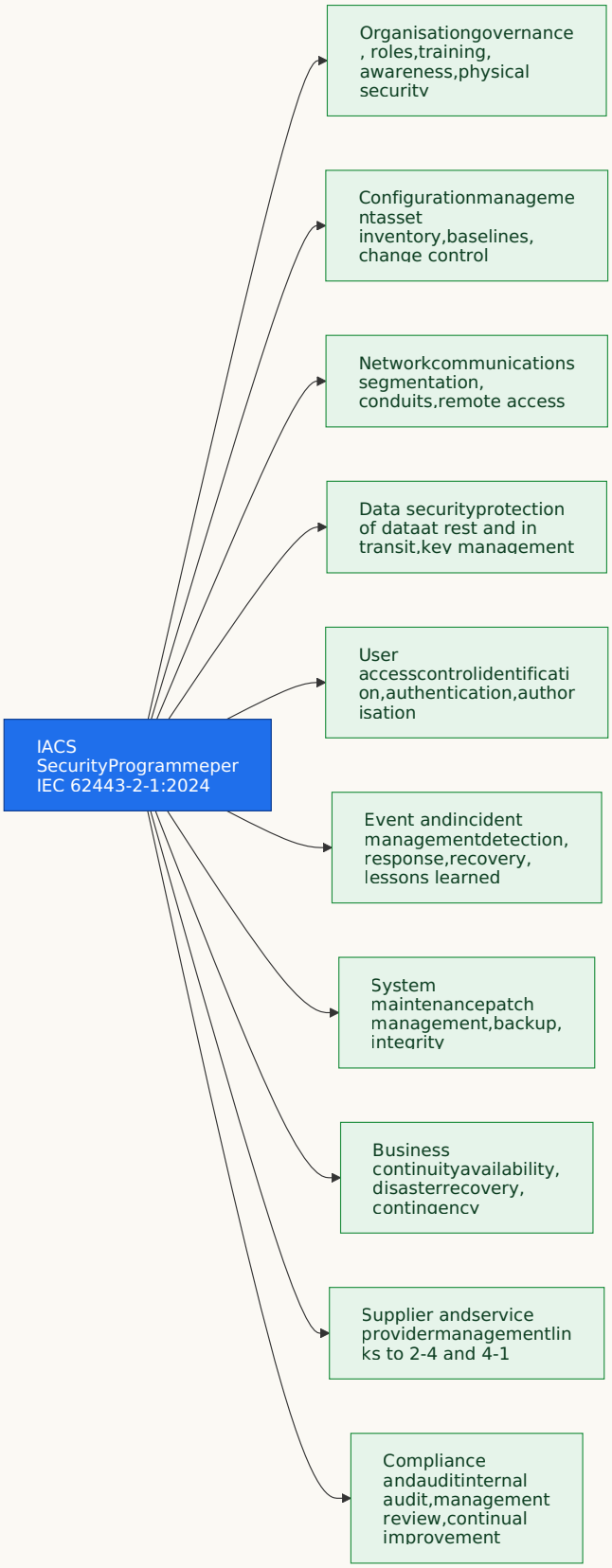
In plain English, 2-1 defines what an asset owner's **Industrial Cybersecurity Programme** must contain in order to be considered well-run. The standard does not specify how the IACS itself must be built — that is the job of 3-3 — but rather what policies, procedures, processes, training arrangements, governance structures and continuous-improvement mechanisms the asset owner must have wrapped around the IACS so that it stays secure in operation. The closest analogue from the IT world is ISO/IEC 27001's Information Security

Management System (ISMS), and the 2024 edition of 2-1 makes this analogy explicit by deliberately deduplicating its requirements against ISO 27001 so that an organisation that already has an ISMS does not have to do everything twice.

To return to the hospital analogy, 2-1 is the **clinical governance framework** — the documented system that says how the hospital is led, how clinical decisions are made and reviewed, how staff are trained and credentialled, how incidents are reported and investigated, how patient safety is monitored, how risks are tracked, how policies are kept current, and how the whole apparatus continuously improves. A hospital with sound clinical governance can deliver safe care year after year; a hospital without it is one bad day away from a Care Quality Commission notice.

The Security Program Elements

The 2024 edition of 2-1 organises its requirements into **Security Program Elements (SPEs)** rather than the looser chapter structure of the 2010 edition. Each SPE is a coherent grouping of requirements addressing a particular dimension of the security programme. The specific element names and counts in the published standard cover the organisational and governance dimension, configuration management, network communications, data protection, user access control, event and incident management, business continuity, system maintenance and other operational disciplines familiar from broader management-system practice. The headline categories an asset owner must address can be visualised as follows.



The crucial conceptual move in the 2024 edition is the introduction of a **maturity model** for evaluating these elements. Echoing the struc-

ture used in IEC 62443-4-1 for OEM development processes, the 2-1 maturity model lets an asset owner be assessed not only on whether they have a policy in place but on how consistently and effectively they are applying it across the organisation. A policy that exists on paper but is unevenly followed is at a lower maturity level than the same policy demonstrably enforced across all sites with audit evidence. The maturity model makes the standard much more useful as an external assessment instrument than the 2010 edition was, because it gives assessors a defensible scale to score against rather than a binary "have or have not".

Another important change is what 2-1 deliberately does not try to do. The 2024 edition recognises that many asset owners already operate an ISO 27001 ISMS, and rather than duplicate the policy-and-procedure scaffolding of an ISMS it explicitly defers to ISO 27001 for the generic information security management apparatus and focuses 2-1's requirements on the IACS-specific additions that an ISMS does not naturally cover. In practice this means that an asset owner with a mature ISMS can use 2-1 as a focused gap-analysis tool rather than a replacement framework, which is a substantial saving of effort and a significant improvement in clarity.

What the asset owner must objectively demonstrate

A defensible claim of compliance with IEC 62443-2-1 looks like a coherent evidence pack covering each of the Security Programme Elements at a stated maturity level, with traceability to operational practice. Concretely this means a documented IACS security policy approved at the appropriate level of the organisation, a current asset inventory of the IACS systems in scope, a risk register that links to the CRS produced under 3-2 , training records for the people who design, operate and maintain the IACS, audit reports demonstrating that policies are being followed in practice, a documented incident management process with a real history of incidents handled (or a clear track

record of monitoring with nothing significant to handle), a documented change management process governing how additions and modifications to the IACS are approved, and a management review record showing that senior leadership periodically reviews the programme's effectiveness and authorises improvements.

There is now an emerging third-party certification route for asset-owner programmes: **ISASecure ACSSA** (Automation and Control System Security Assurance), announced in 2023 and intended to cover an operational IACS at the asset owner's site against IEC 62443-2-1, 2-3 and the relevant parts of 3-3. ACSSA is newer and less widely used than its component-side cousins (SDLA and CSA), but for asset owners in regulated sectors it is likely to become an increasingly common way of evidencing a 2-1 claim. Where ACSSA is not in play, the evidence pack route — internal audit reports, external assessor reports by recognised consultancies, integration with ISO 27001 surveillance audits — is the default. In either case, the key principle is the same: a 2-1 claim is only as strong as the evidence behind it, and the evidence must be current, organisation-wide and consistent with what an outsider would actually find if they spent a day walking around the plant.

IEC 62443-2-2: rating how good the programme actually is

If 2-1 tells the asset owner what their security programme must contain, **IEC 62443-2-2** addresses the related but distinct question: how do we evaluate how well the programme is actually working? It defines a methodology for producing a Security Programme Rating — a structured, defensible scoring of an operational IACS against the requirements of the standards family.

The motivation for this is practical. An asset owner can document a beautiful security programme on paper that fails in operation; another can have a less elegant programme that is rigorously followed and

genuinely effective. Looking only at the documentation cannot distinguish them. 2-2 introduces a structured way to evaluate the operational reality — what is actually configured on the network, what is actually being logged and monitored, what is actually being patched, what is actually being tested — and to produce a rating that is comparable across sites, across business units and over time.

The hospital analogy here is the **CQC (Care Quality Commission) inspection rating** familiar to anyone who has dealt with UK healthcare. A hospital is rated Outstanding, Good, Requires Improvement or Inadequate based on a structured assessment against published criteria. The rating is comparable across hospitals, defensible to regulators and patients, and useful internally for prioritising improvement work. 2-2 plays a similar role for an industrial security programme: it produces a rating that has meaning beyond the immediate audit, with criteria that any informed assessor can re-apply.

The rating is intended to be used in several ways. Internally, it helps senior leadership benchmark sites against each other and against the company's own historical performance. Externally, it gives a way of substantiating cybersecurity claims to regulators, insurers and customers without having to publish sensitive internal documentation. In a procurement or M&A context, it provides a defensible measure of cybersecurity posture that is independent of any single vendor's product. And in the emerging ACSSA certification scheme, a 2-2-style rating is implicit in the assessment methodology.

What an asset owner must demonstrate to claim a 2-2-derived rating is the rating itself, the methodology by which it was produced, the evidence considered, and the assessor's competence. As with 2-1, a self-declared rating is much weaker than one produced by a recognised external assessor, and the value of the rating depends critically on the assessor following the methodology faithfully — which is the

same point made about any certification: the credibility of the certificate is the credibility of the certifier.

IEC TR 62443-2-3: keeping the system current

IEC TR 62443-2-3 is the patch-management member of the family. The "TR" prefix matters: this is a Technical Report rather than an International Standard. The distinction is consequential. A Technical Report is informative — it contains guidance, recommendations and good practice rather than auditable requirements. You cannot strictly be "non-compliant with 2-3" in the way you can be non-compliant with 2-1, because 2-3 does not contain shall-clauses against which to be assessed. But the practical importance of 2-3 is enormous, because patch management in an industrial context is genuinely difficult, and the absence of a coherent patch programme is the most common single weakness in an otherwise well-run IACS.

The hospital analogy here is the **medical equipment maintenance and recall handling procedure**. Hospital equipment has manufacturer maintenance schedules, periodic recalls, software updates and safety notices. Some of these can be applied instantly; some require the equipment to be taken out of service, which has clinical consequences; some require staff retraining; and some — for very old equipment — may have to be applied through compensating measures because the manufacturer has stopped issuing updates. A hospital that ignores recalls is dangerous; a hospital that blindly applies every update without testing in its clinical context is also dangerous. The discipline of doing this properly is what 2-3 codifies for the industrial cybersecurity equivalent.

The headline contribution of 2-3 is a structured account of what a real-world IACS patch management programme has to address: the asymmetric responsibilities between the **product supplier** (who must produce patches, validate them on their products, and commu-

nicate them in a usable form to their customers) and the **asset owner** (who must consume that information, assess applicability in their specific operational context, test patches in a representative environment, schedule application during maintenance windows, and verify that the patched system continues to function correctly). 2-3 also introduces standardised data structures for delivering patch information — the **VPatch** concept being the most discussed example — so that asset owners do not have to translate between every product supplier's idiosyncratic patch notification format.

For the asset owner, demonstrating a credible patch management practice means showing a documented programme that covers every component in the IACS inventory (including, importantly, the long tail of small embedded devices that are easy to overlook), a process for receiving and triaging vendor advisories, a tested approach for risk-assessing each advisory in the operational context (because not every CVE is equally relevant to every deployment), evidence of patch application during scheduled windows with verification of post-patch system behaviour, and a coherent approach for components whose vendors no longer issue patches — typically through compensating controls at the network or operational level.

For the product supplier, the demonstration runs the other way. The supplier must show that they produce patches in a timely manner for vulnerabilities affecting their products, that they communicate those patches in a usable form, that the patches have been tested in representative configurations of the product, and that they support the asset owner's testing through clear release notes, regression-test guidance and roll-back procedures. The OEM-side of 2-3 connects naturally to the obligations in 4-1's Practice 7 (Security Update Management) and to the EU Cyber Resilience Act's vulnerability-handling requirements , so for product suppliers operating in regulated markets these obligations are increasingly being baked into product roadmap discipline rather than treated as an optional extra.

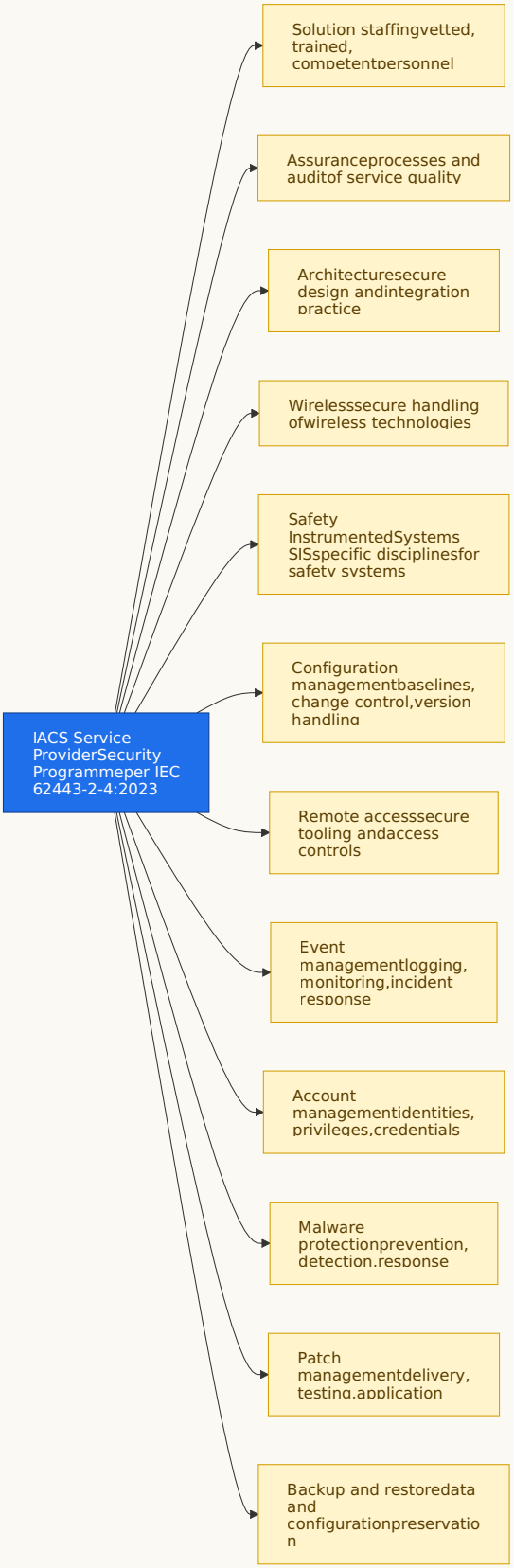
IEC 62443-2-4: the service provider's security programme

If 2-1 governs the asset owner's house, **IEC 62443-2-4** governs the conduct of everyone who comes onto the asset owner's site to design, integrate, maintain or operate the IACS. The standard is titled "Security program requirements for IACS service providers", and its current edition is the 2023 second edition. The "service provider" in 2-4 covers a wide range of organisations: system integrators (who design and build the integrated system per the asset owner's CRS), automation contractors, maintenance contractors, managed-service providers, security service providers running monitoring or incident response on behalf of the asset owner, and any organisation whose people have hands on the asset owner's IACS.

The hospital analogy here is the **medical staffing agency's accreditation and audit regime**. A hospital that allows agency nurses to work on its wards has to know that the agency vets its staff, trains them, maintains their professional registrations, audits their performance, and is itself subject to inspection. A hospital that takes agency staff with no verification of any of those things is exposed to clinical risk that has nothing to do with how well the hospital itself is run. 2-4 plays the same role for service providers in the industrial security space: it tells the asset owner what to insist on from anyone who works on their IACS, and it tells the service provider what they must demonstrate to be acceptable.

The structure of 2-4

2-4 organises its requirements into **Functional Areas** — coherent groupings of capabilities that a service provider must demonstrate. The principal Functional Areas typically referenced in the literature on the standard include the following.



The exact count and labelling of Functional Areas varies slightly between editions of the standard and between different organisations'

summaries of it, but the substantive content is broadly stable: a service provider must have demonstrable capability across the people, the process and the technical dimensions of every activity they perform on the asset owner's IACS.

Like 4-1 for OEMs, 2-4 incorporates a **Maturity Level** dimension. A service provider can be assessed at Maturity Level 1 (the practice exists but is ad hoc), Level 2 (documented and repeatable), Level 3 (consistently practised across the organisation with evidence), or Level 4 (continuously measured and improved). An asset owner specifying 2-4 compliance in their contract should specify the Maturity Level they require, just as they would specify an SL-T in 3-2.

What the service provider must objectively demonstrate

Demonstration here is well-defined because there is an established third-party certification scheme. The **IECEE CB Scheme** for industrial cybersecurity issues certificates against IEC 62443-2-4 through accredited certification bodies, and these certificates are mutually recognised across IECEE member economies. ISASecure has also operated relevant schemes in this space at various points. A service provider claiming 2-4 compliance should be able to produce a current third-party certificate naming the version of the standard, the Maturity Level achieved per Functional Area (or a single global ML where claimed), the certifying body, the issue date and the expiry date — typically three years with surveillance audits in between.

Beyond the certificate itself, the asset owner should expect the service provider to be able to produce the substantive evidence underlying the certificate: training records and competence assessments for the staff who will actually be deployed to the asset owner's site, documented procedures covering remote access, change control, incident handling, patch deployment and configuration management, evidence of internal audit and management review of those procedures, and a security incident handling capability with a track record. As with 4-1,

the scope of the certificate matters as much as the headline rating: a 2-4 certificate covering a specific business unit, a specific geography or a specific service line tells you about that scope, not about the whole organisation. Reading the scope statement carefully is the single most important verification step.

Where a service provider does not hold a third-party 2-4 certificate but claims alignment with the standard, the asset owner should ask for the gap analysis that supports the claim, the corrective actions taken, and any internal audit evidence. Self-asserted compliance is not nothing — it can be a stepping stone — but it does not carry the same weight as a certified position, and the asset owner should make a clear decision about whether they accept it for the kind of work being contracted.

IEC 62443-2-5: the practical handbook

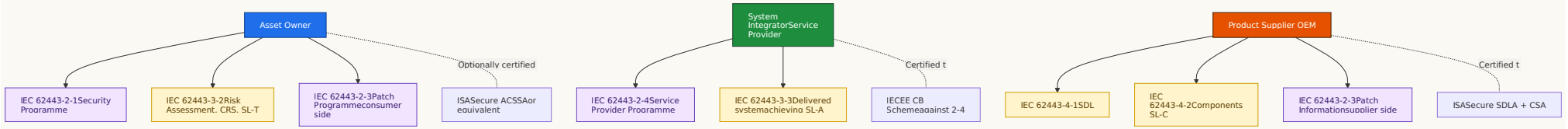
The final member of the Part 2 family, **IEC 62443-2-5**, provides implementation guidance for the asset owner. Where 2-1 says what an asset owner must have in their security programme, 2-5 advises on how to actually do it. It is a practical handbook rather than a requirements document, and its value lies in the worked examples, templates, organisational patterns and pragmatic advice it offers to asset owners who are at the start of building or modernising their security programme.

Because 2-5 is guidance, it does not generate a "compliance" question in the same way as 2-1 and 2-4. There is no certification for being "compliant with 2-5"; there is only the question of whether an asset owner has used it (and similar guidance from ISA, ENISA, NIST and sectoral bodies) to inform their implementation choices. For asset owners building their programme from scratch, 2-5 is a sensible starting point. For asset owners already further along, it is a useful sense-check.

I will not spend long on 2-5 because the substantive obligations all live in the documents above it. But for completeness, anyone working seriously with 2-1 should be aware that 2-5 exists and use it.

How 2-x fits with the rest of the standards

Pulling back at this point, here is how Part 2 sits alongside the standards covered in the previous articles. The diagram below shows the four principal parties and the standards that govern each of them, with the artefacts and certifications that flow between.


Asset Owner
IEC 62443-2-1Security Programme
IEC 62443-3-2Risk Assessment, CRS, SL-T
IEC 62443-2-3Patch Programmeconsumer side
ISASecure ACSSAor equivalent
Optionally certified
System IntegratorService Provider
IEC 62443-2-4Service Provider Programme
IEC 62443-3-3Delivered systemachieving SL-A
IECEE CB Schemeagainst 2-4
Certified t
Product Supplier OEM
IEC 62443-4-1SDL
IEC 62443-4-2Components SL-C
IEC 62443-2-3Patch Informationsupplier side
ISASecure SDLA + CSA
Certified t

The picture is now complete. Every party has technical-side standards (the 3-x and 4-x parts covered in the previous articles) and management-side standards (the 2-x parts covered here). Every party has at least one route to third-party certification of their respective scope. And every interface between parties is governed by a defined artefact: the CRS flows from asset owner to integrator, the SL-C vectors and patch information flow from product supplier to integrator and asset owner, the delivered system with traceability flows from integrator to asset owner, and operational practices on the asset owner's site are governed by the asset owner's 2-1 programme with service providers regulated by 2-4.

A useful diagnostic when looking at a real industrial site is to walk through each interface in this picture and ask whether the corresponding artefact exists, whether it is current, and whether it is being acted upon. Where any interface lacks its defined artefact, that interface is a chain link with no link.

Common pitfalls and red flags

The most frequent pitfall in 2-1 work is **treating it as a documentation exercise**. An organisation writes the policies, files them in a document management system, and considers itself "compliant" with 2-1. The 2024 edition's maturity model is specifically designed to counter this trap — a policy that is written but unevenly applied scores at a low maturity level, and an external assessor working to the standard will find that out. The most useful question to ask of any 2-1 claim is "show me the audit trail of the policy in operation across all sites in the last twelve months", because that is what separates a Maturity Level 1 organisation from a Maturity Level 3 one.

A second pitfall is **conflating 2-1 with ISO 27001**. The two standards overlap but are not substitutes. ISO 27001 governs information security generically; 2-1 specifically addresses the IACS context, in-

cluding the long lifetimes, legacy components, safety interactions and operational realities that ISO 27001 does not naturally cover. The 2024 edition of 2-1 deliberately defers to ISO 27001 for the generic ISMS layer, so an organisation with an ISMS should not duplicate that scaffolding, but they must add the IACS-specific layer that 2-1 requires. A claim of "we are ISO 27001 certified so we comply with 2-1" is not, in itself, accurate.

A third pitfall affects service providers and their asset owner customers: **2-4 certificates with narrow scope**. A large engineering company may have a 2-4 certificate that covers, for instance, its automation business unit in one country, while the company's marketing materials suggest the whole organisation is certified. The scope statement on the certificate is the truth. When commissioning a service provider, the asset owner should ask for a copy of the certificate and read the scope to verify that the actual team to be deployed sits within it. Where the deployed team is from a sister organisation or a recently acquired company, the scope may not cover them.

A fourth pitfall is **confusion between 4-1 and 2-4**. A product supplier may hold an SDLA certificate against 4-1 (covering their product development process) but not a 2-4 certificate (which would cover their service-delivery practices). The two address different scopes and different activities, and one is not a substitute for the other. An organisation that both manufactures products and provides services on the asset owner's site needs both certificates.

A fifth pitfall is **IT patch management practices applied unmodified to OT**. The IT world has well-established patterns for patch deployment — typically rapid, automated, frequently applied — that translate poorly to industrial environments where patches must be tested in representative configurations, scheduled around production windows, and verified for impact on real-time and safety behaviours. An asset owner whose IACS patch programme is run by an IT depart-

ment using IT patterns is at high risk of either applying patches without proper validation or, more commonly, applying nothing because the IT pattern cannot be made to fit. The discipline in TR 62443-2-3 exists precisely because OT patch management is its own discipline.

A sixth pitfall, and a particularly insidious one, is **legacy systems being quietly excluded from the security programme**. The 2024 edition of 2-1 explicitly acknowledges that legacy systems with no manufacturer support cannot meet all of the requirements directly and that compensating measures are the right response. The pitfall is when legacy systems get excluded from the inventory altogether and quietly age out of any active management. The right answer is to keep them in the programme with their compensating measures documented and reviewed, not to drop them off the asset register and hope.

A checklist for procurement, audit and self-assessment

The following can be used as a contract annex, an internal audit instrument, or a self-assessment tool. It is organised by the party demonstrating compliance.

For the asset owner's own 2-1 evidence pack

- A current, board-approved IACS cybersecurity policy referencing IEC 62443-2-1 (2024 edition) and identifying the SP elements covered.
- A documented IACS asset inventory covering all systems in scope, including legacy systems with their compensating measures explicitly noted.
- A risk register linked to the CRS produced under 62443-3-2 , with regular review cadence evidenced.
- Training records for staff with IACS responsibilities, including refresher cycles and competence assessments.

- Documented procedures for change control, incident response, patch management (per 62443-2-3), backup and restore, and access management — with evidence of operation.
- A current self-assessment or external assessment of maturity level per SP Element, with prioritised improvement actions.
- Internal audit reports covering each SP Element with evidence of corrective actions closed out.
- Management review records demonstrating senior leadership engagement at a defined cadence (typically annually).
- Where applicable, a current ISASecure ACSSA certificate or equivalent third-party assessment, with the scope statement reviewed against the actual operational footprint.

For the asset owner's evaluation of a service provider's 2-4 claim

- A current IECEE CB Scheme certificate (or equivalent) against IEC 62443-2-4:2023, with the issuing body, issue date and expiry date clearly stated.
- A scope statement on the certificate that explicitly covers the business unit, geography and service type relevant to the contract.
- A statement of the Maturity Level achieved per Functional Area (or a single global ML where claimed).
- Training and competence records for the specific personnel proposed for deployment to the asset owner's site.
- Documented procedures for the activities the service provider will perform on the asset owner's IACS, with linkage to the certified Functional Areas.
- Evidence of past performance on similar engagements with reference customers.
- A defined process for handling incidents that may arise during the engagement, with escalation paths into the asset owner's own incident management process under 2-1.

For the asset owner's evaluation of a product supplier's 2-3 contribution

- A documented vulnerability disclosure and advisory programme with a track record of issued advisories.
- A defined patch delivery format (ideally aligned with the VPatch or similar machine-readable format) and an indication of the typical lead time from vulnerability disclosure to patch availability.
- Release notes and testing guidance accompanying each patch, sufficient to support the asset owner's own testing.
- A defined support lifetime per product with a clear end-of-support date, beyond which the asset owner must rely on compensating measures.
- Where applicable, demonstrable linkage to the supplier's 4-1 SDLA certification (the underlying secure development process) and 4-2 CSA certification (the components in scope).

For the asset owner's evaluation of their own 2-3 patch programme

- A current asset inventory covering every component in the IACS, with vendor advisory channels subscribed for each.
- A documented triage process for incoming advisories with risk-based prioritisation.
- A test environment representative enough to validate patches before production deployment.
- A scheduled patch deployment cycle aligned with production maintenance windows, with verification of post-patch system behaviour.
- A documented approach for unpatchable components, with compensating controls implemented and reviewed.
- Metrics demonstrating the programme's actual performance — typical time-to-patch by criticality, percentage of advisories applied versus deferred with justification, and trends over time.

Where the 3-x and 4-x standards address the what of an IACS — what the system must do, what the components must support, what the design must achieve — the 2-x standards address the how of running it day-to-day, year after year, through the long operational life of an industrial plant. **IEC 62443-2-1** governs the asset owner's security programme and is the cornerstone of the family on the operational side. **IEC 62443-2-2** gives a way of rating how well that programme is actually working. **IEC TR 62443-2-3** codifies the discipline of patch management for both asset owners and product suppliers. **IEC 62443-2-4** governs the service providers who do work on the asset owner's site. **IEC 62443-2-5** offers practical implementation guidance to support 2-1.

The single most important mental model to carry away from this article is that **every party has both a technical-side obligation and a management-side obligation under IEC 62443**, and that defensible cybersecurity depends on both being in place. A product supplier with a brilliant SDL (4-1) but a chaotic patch advisory practice (2-3) is half a supplier; a system integrator with excellent technical capability against 3-3 but no certified service programme under 2-4 is half an integrator; an asset owner with a careful 3-2 risk assessment but no operational security programme under 2-1 has built a building with no caretaker.

The chain of evidence across all of IEC 62443 only holds up when every party can demonstrate their piece — with current certificates where they exist, with substantive evidence underlying them, and with a culture of operational discipline that keeps the certificates meaningful between audits. The standards family gives you the framework. What it cannot give you is the willingness to actually run things that way.

IEC 62443-3-2 and 3-3: what asset owners and integrators must prove

13 May 2026 · 32 min read · #compliance #security #industrial #iec-62443

The OEM-side piece in this series unpacks the two standards a product supplier has to live with: IEC 62443-4-1 (how a product is built) and IEC 62443-4-2 (what the product can actually do) — for the detailed walk-through see IEC 62443-4-1 and 4-2: what an OEM must actually prove . Those are vital, but they are only half the story. Buying certified components is one thing; turning them into a functioning industrial control system that is sized correctly to the actual threats, partitioned sensibly between zones, and delivered with hard evidence that the finished plant is as secure as the design intended, is a different discipline altogether. That discipline is governed by two more parts of the same IEC 62443 family: **IEC 62443-3-2** and **IEC 62443-3-3**.

These two standards sit one tier above 4-1 and 4-2. They live at the **system** layer rather than the **component** layer, and they answer two different but tightly coupled questions. **IEC 62443-3-2** asks "how do I work out what level of security I actually need in each part of my industrial system?" **IEC 62443-3-3** asks "if I have decided I need a particular level of security in a part of the system, what must that part of the system actually do to deliver it?" One produces the brief; the other defines what counts as fulfilling the brief. Together they sit between the asset owner's risk picture and the OEM's certified components, and this is also where the EU regulatory chain — NIS2 for the asset owner side, the Cyber Resilience Act for the product side — most often lands in real procurement contracts.

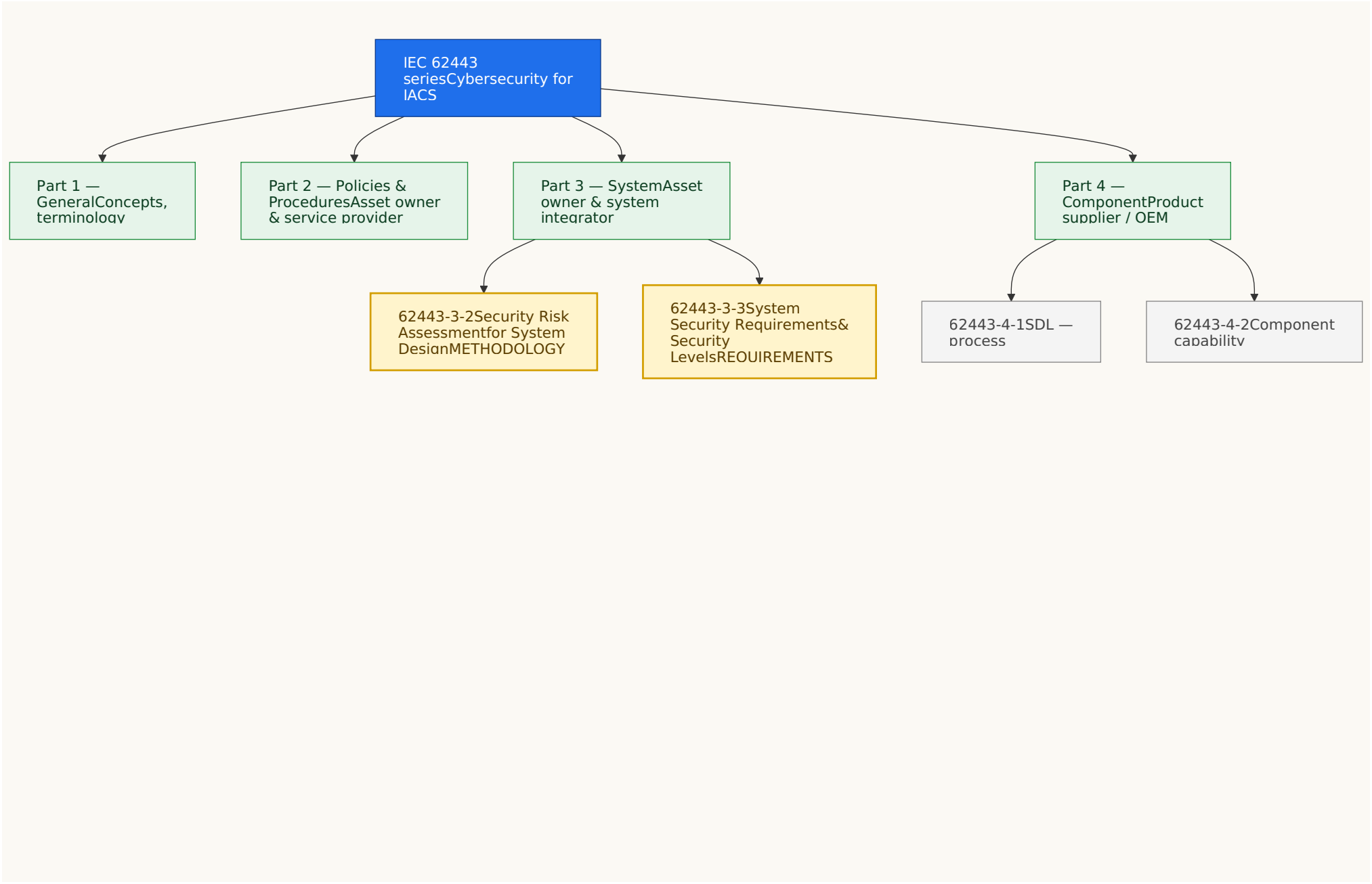
The aim is the same as last time. Anyone can claim "compliance with IEC 62443"; the question that matters is what they must objectively demonstrate to back the claim up. The standards are formal and

structured enough that the answer is genuinely knowable — provided you know what to ask for.

You can purchase the official standards from the IEC Webstore: IEC 62443-3-2:2020 and IEC 62443-3-3:2013 .

A quick orientation in the IEC 62443 family

To see where 3-2 and 3-3 fit, it helps to remember the four-tier shape of the whole IEC 62443 series. Part 1 establishes terminology and concepts. Part 2 covers policies and procedures, principally for the asset owner and their service providers — covered separately in IEC 62443-2-x: the management system behind a secure industrial plant . Part 3 — where today's two standards live — covers the system level. Part 4 covers the individual components that get integrated into the system.


IEC 62443 seriesCybersecurity for IACS
Part 1 — GeneralConcepts, terminology
Part 2 — Policies & ProceduresAsset owner & service provider
Part 3 — SystemAsset owner & system integrator
Part 4 — ComponentProduct supplier / OEM
62443-3-2Security Risk Assessmentfor System DesignMETHODOLOGY
62443-3-3System Security Requirements& Security LevelsREQUIREMENTS
62443-4-1SDL — process
62443-4-2Component capability

The two standards in the spotlight today are squarely in Part 3, and they are jointly the responsibility of the **asset owner** (the operator of the plant) and the **system integrator** (the engineering organisation that designs and builds the integrated system). The OEM's standards from Part 4 are relevant here because the components they supply must be able to combine into a system that meets 3-3, but the OEM is not themselves the audience for 3-2 and 3-3.

The extended building analogy

Before either standard goes under the microscope, an analogy will help — the rest of the article leans on it. Constructing an industrial control system is not unlike constructing a hospital. There are several distinct trades involved, each with their own discipline, and each must produce evidence appropriate to their role.

IEC 62443-3-2 is the architect's brief and the structural engineer's calculations. Before a single brick is laid, somebody decides what loads the building must bear, where the fire compartments belong, what kind of glazing the windows need given the local climate, whether the operating theatres need redundant electrical supplies, and how patient flows separate from staff flows. The output is a set of design decisions with risk-justified targets attached: this corridor must be a fire compartment boundary; this room must have positive pressure; this electrical feed must have a backup. These decisions are made by people qualified to make them and signed off by the building's owner. They are not yet a building — they are the brief against which the building will be constructed.

IEC 62443-3-3 is the building code. It is the rule book that says, given the type of building you are constructing and the design choices that flow from it, here are the specific things that must be true of the finished structure. Fire doors of a certain class must have rated hinges and self-closing mechanisms. Emergency exits must be of a

minimum width. Operating theatres in this category of facility must have such-and-such air-change rate. The code is generic — it does not know your specific hospital — but it tells the contractor what they must achieve to satisfy the design brief.

IEC 62443-4-2 is the kitemark on each brick, fire door and circuit breaker. Each individual building component has been independently tested and rated. When the contractor specifies a fire door rated to FD60, they pick a door with a certificate to that rating.

IEC 62443-4-1 is the brick factory's quality management system. It is what gives you confidence that the certified product on site is actually the same as the product that was tested for the kitemark.

Together, the four standards form a chain in which each link has a clear owner and clear evidence requirements. The asset owner produces the brief (3-2). The contractor builds against the building code (3-3) using certified components (4-2) made by quality-controlled suppliers (4-1). The asset owner inspects, certifies and operates the finished building. Each handover is a defined artefact, and each party is accountable for a defined scope.

With the analogy in place, the two standards themselves come next.

What IEC 62443-3-2 actually is

IEC 62443-3-2:2020, formally titled "Security risk assessment for system design", is the **methodology standard** for the asset owner. It does not tell you what your industrial system must look like; instead, it tells you how to figure that out for yourself, in a structured and repeatable way, based on actual risk in your actual operating context.

The standard's central contribution is a workflow — usually referred to as the **Zone and Conduit Requirements (ZCR) process** — that takes a description of the system you intend to protect and produces, as its output, a partitioned design with **Target Security Levels (SL-**

T) allocated to each part. That output is the formal input to the next stage: selecting and integrating components that can meet those targets, which is where IEC 62443-3-3 takes over.

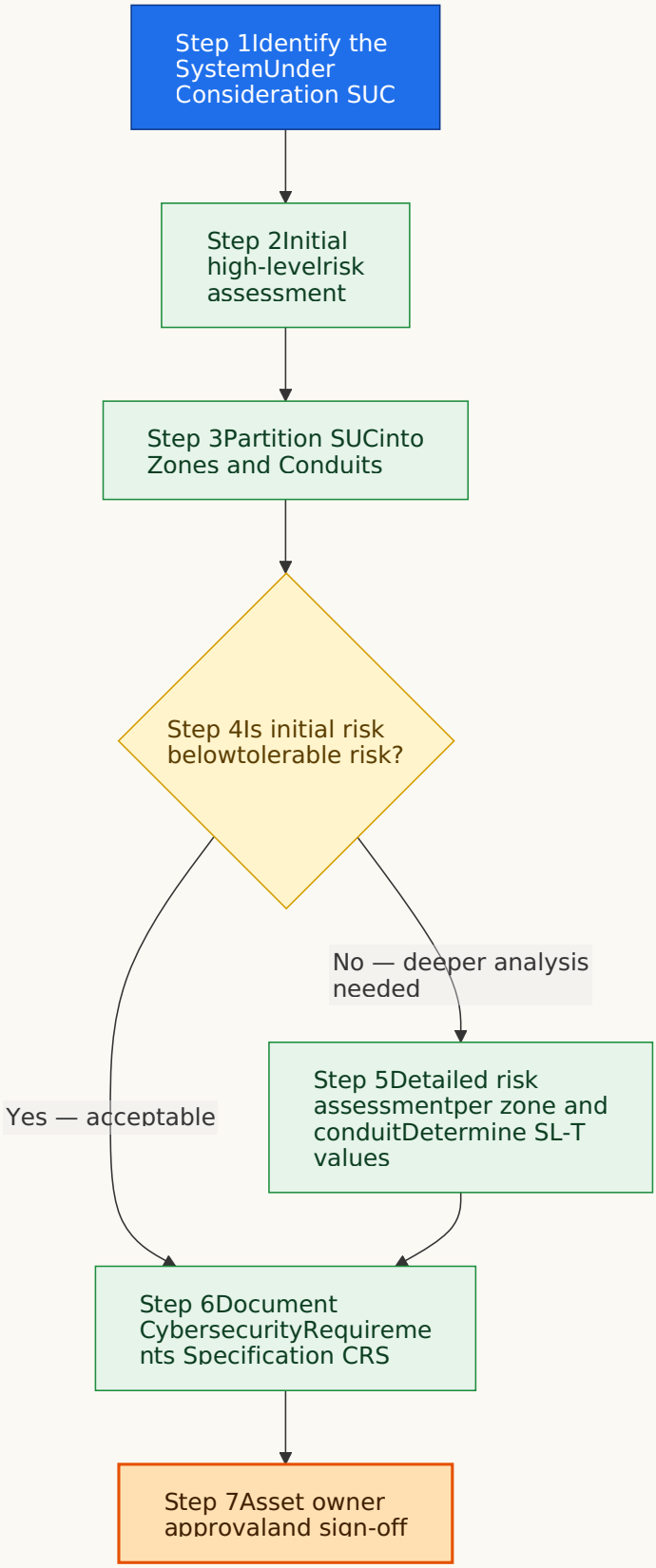
The primary audience for 3-2 is the asset owner, although they will almost always engage external help. The work demands both deep process knowledge of the plant (which the asset owner has) and specialist cybersecurity expertise (which is usually contracted in, often through a system integrator or an independent risk consultant). The ultimate accountability, however, remains with the asset owner. If a system integrator runs the ZCR workshops for you, that does not transfer accountability for the resulting design to them — it transfers responsibility for the quality of the analysis, but the decisions are yours to make and to sign off.

What 3-2 is not matters as much as what it is. It is not a risk-assessment methodology in the prescriptive sense — it does not tell you whether to use a NIST SP 800-30 approach, an ISO 31000 approach, a HAZOP-derived approach or anything else. It tells you what your risk methodology must cover and what it must produce, but it leaves the choice of underlying technique to your organisation. This makes 3-2 admirably flexible across sectors — process industries can plug it into their existing HAZOP/LOPA culture, while discrete manufacturing or utilities can use methods more familiar to them — but it also means that "compliance with 3-2" requires more than picking a methodology off a shelf. It requires demonstrating that whatever methodology you chose actually does what 3-2 asks of it.

What 3-2 means practically: the seven-step workflow

The heart of IEC 62443-3-2 is a numbered workflow. Although the standard expresses it more formally, in practice it boils down to seven steps that flow from a description of "what we are protecting"

through to "here is the documented design with risk-justified security levels".



The first step is to **identify the System Under Consideration (SUC)**. This sounds trivial but rarely is. The SUC description must be specific enough that anyone reading it later — an auditor, a successor, a regulator — can understand exactly what was assessed and what was not. In practice this means a high-level architecture diagram, an inventory of the major equipment and software in the SUC, a network map, an explicit statement of the business and safety functions the SUC supports, a list of external interfaces, and a clear note of what is out of scope. An SUC scoped too narrowly leaves dangerous assumptions about the boundary; an SUC scoped too broadly produces analyses too coarse to be useful.

The second step is an **initial high-level risk assessment** of the SUC as a whole. This is a coarse-grained, qualitative pass that asks the simple question: if the worst-case credible cybersecurity event happened to this SUC, what would the consequences be for safety, environment, production, regulatory standing and revenue? The output is usually a single "worst-credible" risk rating and an indication of whether the SUC as a whole warrants the more granular analysis that follows. In nearly every real industrial setting it does — but having the initial assessment on file makes the case for the deeper work and provides a baseline against which residual risk can later be compared.

The third step is the central design act of 3-2: **partitioning the SUC into zones and conduits**. A **zone** is a grouping of assets that share the same security requirements — typically because they have similar function, similar consequence-of-failure, similar trust level, or similar operational environment. A **conduit** is the controlled communication channel between zones. Drawing the zones and conduits is what turns an undifferentiated network diagram into a security-aware architecture. To continue the building analogy, this is the moment when the architect decides "these rooms form the operating theatre suite, this corridor connects them to the recovery ward, and the swing

doors at this point will be the fire compartment boundary." The decision is consequential because everything downstream — SL-T allocation, component selection, conduit protection mechanisms — flows from where you draw these lines.

The fourth step asks whether the initial risk assessed in step two, viewed through the lens of the proposed partitioning, already falls below the asset owner's tolerable risk threshold. If it does — perhaps because the SUC is small, isolated and low-consequence — the process can move directly to documentation. In most real industrial situations, however, it does not, and the workflow moves into the heart of the analysis at step five.

Step five is the **detailed risk assessment, performed per zone and per conduit**. This is where threats, vulnerabilities and consequences are systematically analysed for each zone and conduit using whatever risk methodology the organisation has adopted. The crucial output of this step is the **Target Security Level (SL-T)** for each zone and conduit. SL-T is expressed in the standard one-to-four scale used elsewhere in 62443 and, importantly, is usually expressed per Foundational Requirement — so a single zone may have an SL-T vector such as (3, 2, 3, 2, 2, 2, 2) across FR1 to FR7. Different zones will usually have different vectors. A zone containing the safety-instrumented system of a refinery, for example, will typically demand a higher SL-T for FR3 (System Integrity) than the engineering office's general-purpose IT network sitting in another zone.

Step six is **documentation**. The output of the whole process must be captured in a formal artefact, conventionally called the **Cybersecurity Requirements Specification (CRS)**. The CRS records the SUC description, the zones and conduits, the SL-Ts, the assumptions made (for instance "we assume the corporate firewall blocks all inbound SMB traffic to the control network"), the constraints recognised (for instance "the legacy PLC family in use does not support multi-factor

authentication, so compensating controls are applied at the conduit"), and any residual risks that have been knowingly accepted. The CRS is more than internal documentation — it is the contractual bridge between asset owner and system integrator. It is what the integrator must deliver against under 3-3.

The seventh and final step is **approval by the asset owner**. The standard is explicit that the asset owner is accountable: an integrator or consultant may have produced the document, but the asset owner must consciously accept its conclusions and the residual risk implied by them. In practice this usually means sign-off at a defined seniority level — often by someone in the operations or asset-management line who can be held responsible for the cybersecurity posture of the plant.

What the asset owner must objectively demonstrate for 3-2

When an asset owner claims compliance with IEC 62443-3-2, they should be able to produce, on request, the documentary record of having done the work properly. Compliance with 3-2 is not about a certificate on the wall — there is no widely used third-party certification scheme for asset-owner compliance with 3-2, in the way that ISASecure SDLA and CSA exist for OEMs. Instead, demonstration is about the **evidence pack**.

A credible evidence pack starts with the **SUC description** in enough detail that an external assessor could retrace what was assessed and what was deliberately excluded. It includes the **methodology** used — the explicit risk-assessment framework chosen, with its scoring rules and risk thresholds. It includes the **threat sources** considered, ideally referencing a current threat catalogue such as ENISA's ICS threat reports, MITRE ATT&CK for ICS, sectoral information sharing and analysis centres (such as the E-ISAC for electric utilities), or national CSIRT advisories. It includes the **risk register** that resulted from

steps four and five, with each zone and conduit's pre-control risk and residual risk written down. It includes the **zone and conduit diagram** itself — typically a network-style schematic overlaid with coloured zone boundaries and labelled conduits. And it culminates in the **Cybersecurity Requirements Specification**, signed off at an appropriate level of the asset owner's organisation.

The standard does not prescribe how often this exercise must be repeated, but good practice is to review the CRS whenever the SUC changes materially, whenever the threat landscape shifts significantly, or on a fixed cycle of typically three to five years. Evidence of this review cadence — meeting minutes, version-controlled CRS revisions, a documented change-control process — is itself a useful demonstration of compliance.

There is a subtlety worth dwelling on. Compliance with 3-2 is not the same as having "low risk" in the resulting system. An asset owner can fully comply with 3-2 and still consciously accept a relatively high residual risk in some zones — provided that decision is documented, justified by business context, and approved by someone with authority to do so. What 3-2 demands is evidence of having reasoned about it properly, not a particular outcome. The standard is procedural in spirit, not prescriptive about results. This is sometimes uncomfortable for auditors who expect to see a "pass/fail" verdict, but it is the right design for a standard that has to serve everything from a wastewater treatment plant to a nuclear power station.

What IEC 62443-3-3 actually is

If 3-2 asks "what level of security do I need where?", then **IEC 62443-3-3:2013** asks "what must a system at a given security level actually be able to do?" It is titled "System security requirements and security levels", and it is the **requirements-catalogue standard** for the system layer.

3-3 defines **System Requirements (SRs)** grouped under the same seven Foundational Requirements used elsewhere in IEC 62443 — Identification and Authentication Control, Use Control, System Integrity, Data Confidentiality, Restricted Data Flow, Timely Response to Events, and Resource Availability. Each SR is a capability that an integrated industrial automation and control system must support, expressed in a way that is largely independent of any particular vendor's products. Many SRs have one or more **Requirement Enhancements (REs)** that apply at higher Security Levels — the same idea as in 4-2, where a basic SR is augmented at SL 3 or SL 4 with additional rigour. The standard contains in the order of fifty-plus SRs, with the total count climbing well above one hundred once REs are included; the exact tally depends on how you count.

The audience for 3-3 is principally the **system integrator** — the engineering organisation that takes the asset owner's CRS and turns it into a delivered integrated system. The product supplier indirectly cares about 3-3 because their components, certified to 4-2 , need to combine in such a way that the system as a whole can meet 3-3's system-level requirements. The asset owner cares because they need to be able to verify that the delivered system actually achieves what was specified.

A useful mental model is that 3-3 is to the system what 4-2 is to the component. Both standards use the same seven Foundational Requirements as their organising spine. Both express requirements in a vendor-neutral way. Both grade those requirements by Security Level 1 to 4. The difference is the level of integration at which the requirement applies. A 4-2 requirement might be "the component shall support unique user authentication". The corresponding 3-3 requirement might be "the system shall enforce unique user authentication across all of its components, including federation of identities where multiple components participate in a single user session, with audit logging of authentication events that can be correlated centrally". The

component might be capable, but the integration is what makes the capability real.

What 3-3 means practically

A good way to grasp what 3-3 actually demands is to look at a few of its System Requirements through the lens of what they translate into for the engineering team building the system.

Under Foundational Requirement 1 (Identification and Authentication Control), 3-3 expects the system to provide unique account identification across all of its users and devices, to support strong authentication mechanisms appropriate to the SL, and — at higher SLs — to require multi-factor authentication for sensitive operations such as engineering changes or safety system modifications. In practical terms, this means a system at SL-T 3 cannot rely on shared logins, generic operator accounts or hard-coded device passwords; identity must be unique, traceable and cryptographically backed.

Under FR 2 (Use Control), the system must enforce role-based access, must restrict mobile-code execution, must protect audit information from tampering, and must support continuous monitoring of who did what when. This translates into a system whose engineering workstations log every parameter change to a tamper-evident audit trail, whose operator screens limit what an operator can do based on a defined role, and whose programming devices cannot run arbitrary code by accident or by a malicious USB stick.

Under FR 3 (System Integrity), the system must protect itself against unauthorised changes to firmware, configuration and data, both in motion and at rest. Communication channels between zones (the **conduits** identified during 3-2) must protect message integrity, and the system must support cryptographic verification of the software and firmware running on its components. At higher SLs, this expands

to include continuous integrity monitoring and automated detection of unauthorised changes.

Under FR 4 (Data Confidentiality), sensitive information in transit and at rest must be protected. At lower SLs this might mean transport-layer encryption for engineering sessions; at higher SLs it includes protection of credentials in storage, encryption of stored configuration data, and protection against side-channel disclosure on shared infrastructure.

Under FR 5 (Restricted Data Flow), the system must operationally support the zones-and-conduits architecture mandated by 3-2. It must support enforcement of the conduit boundaries (typically via firewalls, unidirectional gateways or data diodes in higher-SL zones), it must prevent unauthorised lateral traffic between zones, and at higher SLs it must include mechanisms to detect and alert on violations of the conduit policy.

Under FR 6 (Timely Response to Events), the system must produce, store, protect and make available a coherent set of security-relevant events — logs that allow detection, investigation and recovery. At higher SLs, this includes integration with security information and event management (SIEM) systems, the ability to support near-real-time alerting, and forensic-quality retention of evidence.

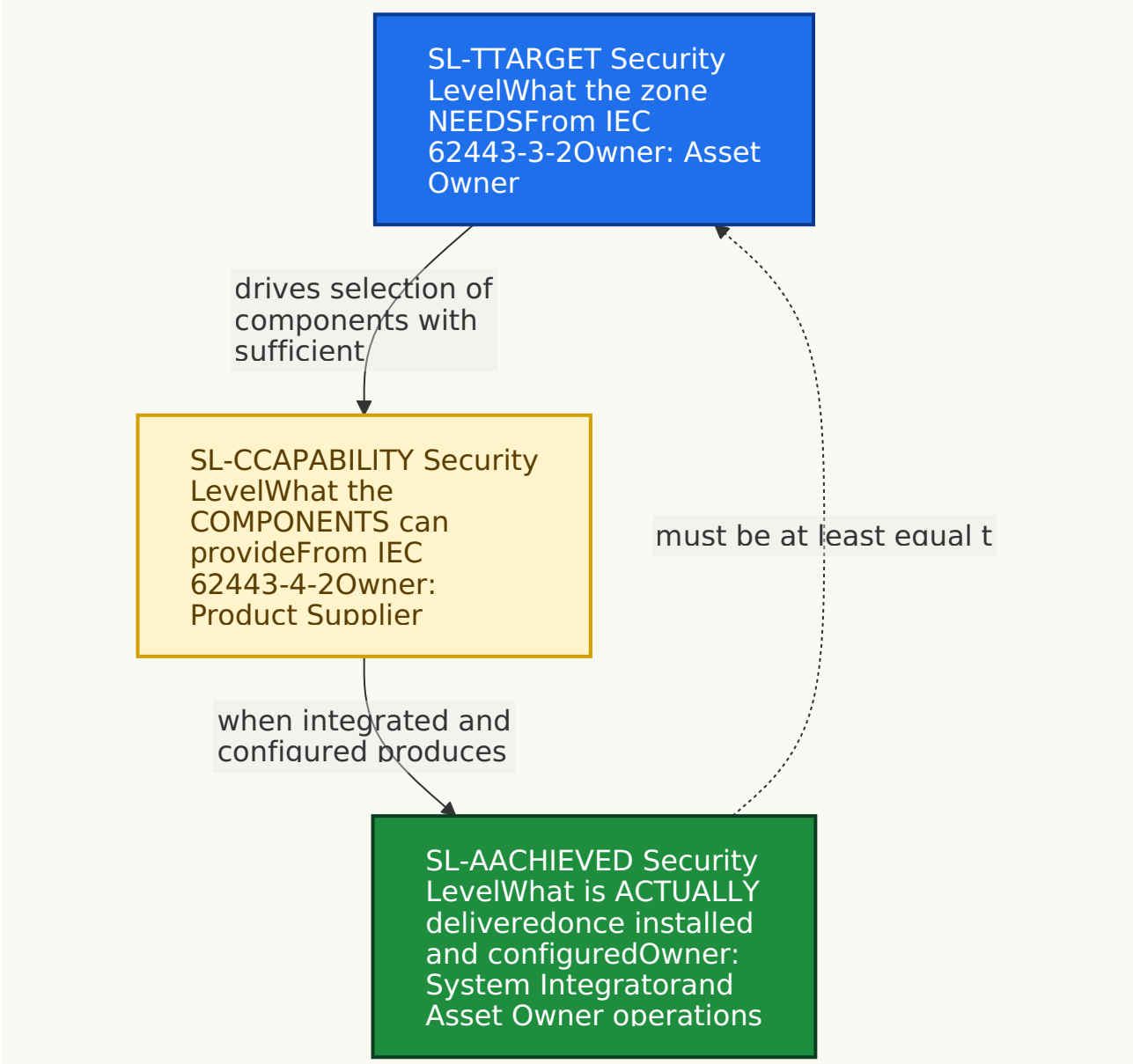
Under FR 7 (Resource Availability), the system must be resilient to denial-of-service conditions, must support backup and restore of all critical configuration and data, and must be capable of operating safely when degraded. This is where industrial-specific concerns — graceful failure modes, deterministic behaviour, prioritised emergency operations — meet generic cybersecurity availability requirements.

A useful way to picture 3-3 as a whole is as a checklist of system capabilities, indexed by SL. At SL-T 1, the bar is "protect against casual

or coincidental violation"; at SL-T 4, the bar is "protect against intentional violation using sophisticated means with extended resources, IACS-specific skills and high motivation" — broadly nation-state-class threats. The list of SRs is the same across all four SLs; what changes is the depth, rigour and resourcing of each capability. The standard is meticulous about this — for each SR, the body of the standard sets the SL 1 baseline, and the REs ratchet that up explicitly at SL 2, 3 and 4.

The most important diagram: SL-T, SL-C and SL-A

Of all the concepts in IEC 62443, the relationship between the three types of Security Level is the one most often muddled — and the one that does the most damage when misunderstood. The three are deceptively similar in their abbreviations, and procurement documents routinely conflate them. Internalising the distinction is, in my experience, the single most useful thing a buyer or operator can do when they start working with this standards family.



SL-T, the Target Security Level, comes out of IEC 62443-3-2. It expresses what the asset owner has decided is needed in each zone, based on the risk assessment. It is a statement of demand. It belongs to the asset owner.

SL-C, the Capability Security Level, comes out of IEC 62443-4-2 . It expresses what a particular product is technically able to provide when properly configured. It is a statement of supply. It belongs to the product supplier.

SL-A, the Achieved Security Level, applies to the delivered system. It expresses what the integrated, installed, configured and operationalised system actually does in the live plant. It is a statement of reality. It is jointly the responsibility of the system integrator (for as-built) and the asset owner (for as-operated).

Three rules govern how these relate, and they are rules I would recommend committing to memory. First, no zone can achieve an SL-A greater than the lowest SL-C of any component sitting in that zone — your zone is only as strong as its weakest link, and a single SL-C 1 component in an otherwise SL-C 3 zone drags the achievable SL-A back to 1 for whichever FR that component is weak in. Second, an SL-A short of the SL-T means the design has not delivered against requirements; either additional compensating controls are needed (perhaps at the conduit, perhaps procedurally), the SL-T must be re-evaluated against revised risk acceptance, or the residual risk must be formally accepted by the asset owner. Third, SL-C is a capability, not a guarantee: a component certified at SL-C 3 deployed with the security features disabled contributes nothing more than SL-C 1 to the zone, and the most common way for an SL-A to fall short of an SL-T is for SL-C-capable features to be left switched off in the field.

This three-letter trio is the backbone of any defensible 62443-based design. When a vendor brochure says "SL 3 certified", the first question must be "SL-what 3?" When a procurement specification says "the system shall be SL 2", the next question must be "SL-T 2, SL-C 2 or SL-A 2?" — because each implies a different obligation on a different party. A well-written tender separates them explicitly: "the system shall be designed and delivered to achieve an SL-A of at least 2 across FR1 to FR7, using components with documented SL-C of at least 2, in support of an SL-T of 2 as determined in the attached Cybersecurity Requirements Specification." That single sentence — combining all three SLs, naming the relevant standards, and pointing back to the CRS — collapses a great deal of potential ambiguity.

What the system integrator must objectively demonstrate for 3-3

When a system integrator claims compliance with IEC 62443-3-3 for a delivered system, the asset owner should expect a coherent evidence pack that traces from the CRS produced under 3-2, through the design and procurement decisions, to the as-built system and its commissioning tests. This evidence pack is rarely a single document; it is more usually a structured collection of artefacts that, taken together, form an auditable trail.

The integrator must demonstrate **traceability** between every SL-T in the CRS and the System Requirements of 3-3 that have been applied in the design. For each zone, the integrator must show which SRs at the relevant SL were considered, which were implemented, which were compensated for by other means, and which were formally noted as not applicable with a written justification. This is usually captured in a requirements-traceability matrix that runs alongside the design documentation and is maintained throughout the project lifecycle. The matrix is the single document an auditor will most often ask for first.

The integrator must demonstrate the **component selection rationale**: that the components chosen for each zone have an SL-C at least as high as the SL-T of that zone, for every relevant Foundational Requirement. This evidence is typically drawn from the components' own 62443-4-2 certificates (ISASecure CSA, IECEE CB Scheme, or equivalent) cross-referenced to the integrator's bill of materials. Where a chosen component does not have third-party 4-2 certification, the integrator must justify the choice and show how the corresponding 3-3 SRs are met through architectural or compensating measures — perhaps by placing the component behind a higher-SL gateway, by isolating it in a sub-zone, or by applying procedural controls.

The integrator must demonstrate that the **system has been verified and validated**. This includes design reviews against the SRs, factory acceptance testing (FAT), site acceptance testing (SAT), and security-specific testing such as configuration audits, vulnerability scanning of the as-built system, and — where the SL-T justifies it — penetration testing of representative attack paths. Test reports must be linked back, via the traceability matrix, to the SRs they verify. A pen-test that produces a hundred-page report which cannot be tied to the requirements it tested is much less useful than a tightly-scoped engagement targeting the SRs that matter.

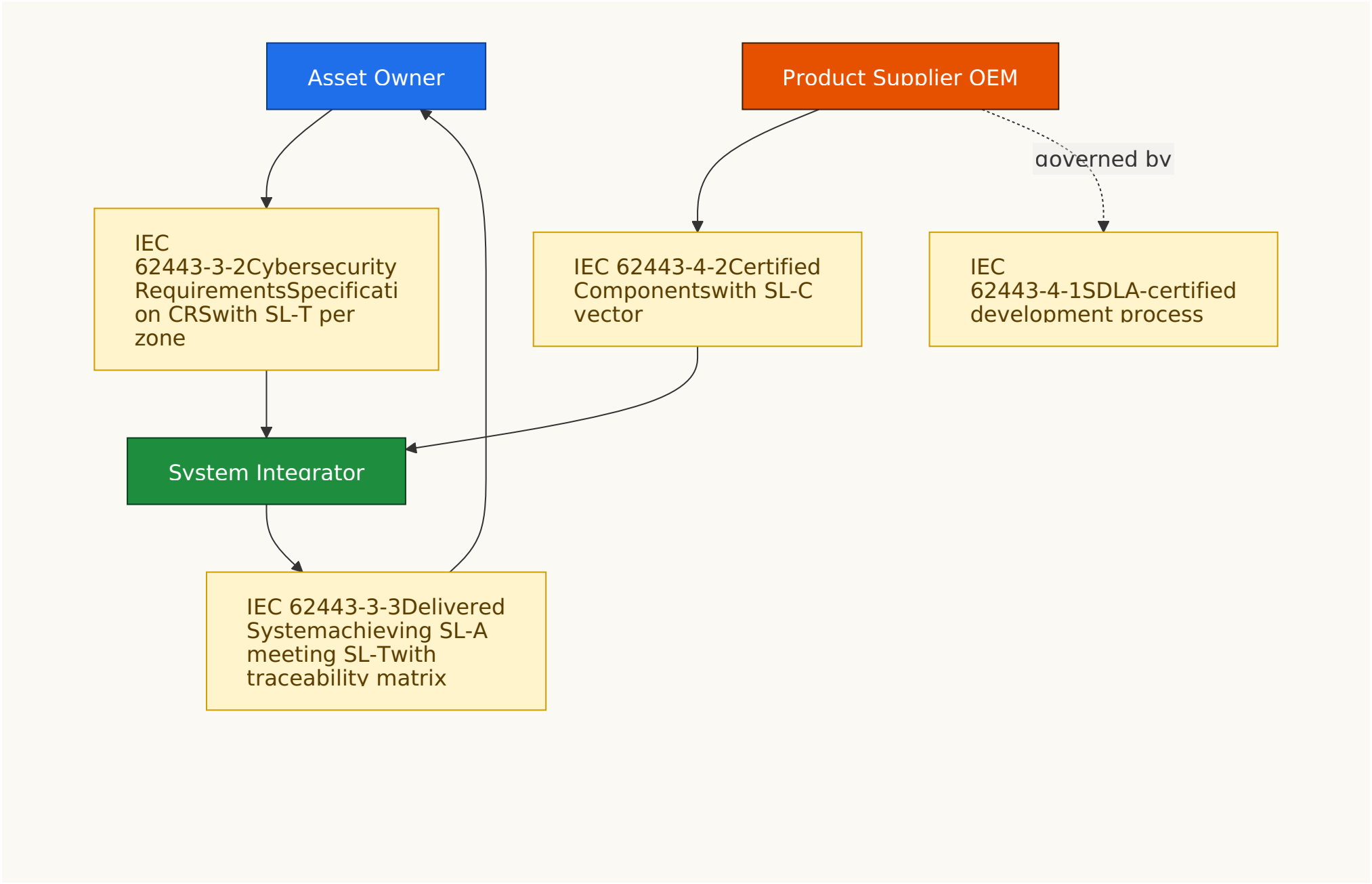
The integrator must demonstrate that the **delivered system is handed over with the documentation needed for the asset owner to operate it securely**. This means hardening guides, security configuration baselines, account inventories, log and SIEM integration documentation, backup and restore procedures, incident response runbooks tailored to the specific system, and a security operations manual that explains how each Foundational Requirement is monitored and maintained in service. The handover documentation is where SL-A becomes sustainable rather than a one-day snapshot at the end of commissioning.

The third-party certification route for systems is **ISASecure SSA** (System Security Assurance), which certifies a specific system implementation against IEC 62443-3-3. Like CSA for components, SSA carries the prerequisite that the supplier has an underlying SDLA-certified process for any components they produce in-house. SSA is materially less common than CSA in part because every system installation is bespoke, but it is the closest thing to a "kitemark" for integrated systems in the 62443 world, and worth asking for when the system in question is one of a vendor's standard product offerings (a packaged SCADA solution, for instance) rather than a one-off integration.

There is also an emerging companion scheme — ISASecure SDA (Site Deployment Assurance) — which is intended to cover the deployed installation in a way SSA does not. As of writing, SDA is at varying stages of pilot across the industry. Asset owners should watch this space because it potentially closes the assurance gap between "the supplied system" (SSA) and "the system as actually operating on my site" (SL-A in its truest sense).

How 3-2, 3-3, 4-1 and 4-2 all fit together

A clean way to visualise the relationship between all four standards is to think of four parties handing each other defined artefacts, with each party accountable for a defined scope and each handover backed by evidence that an outside assessor could check.


Asset Owner
Product Supplier OEM
governed by
IEC 62443-3-2Cybersecurity RequirementsSpecification CRSwith SL-T per zone
IEC 62443-4-2Certified Componentswith SL-C vector
IEC 62443-4-1SDLA-certified development process
System Integrator
IEC 62443-3-3Delivered Systemachieving SL-A meeting SL-Twith traceability matrix

The asset owner does the risk assessment under 3-2 and produces the CRS. The system integrator takes the CRS and delivers a system that complies with 3-3, using components certified to 4-2 by product suppliers whose development processes are certified to 4-1. Each party hands the next a defined artefact — a CRS, an SL-C vector with a certificate, a system with traceability — and each party is accountable for a defined scope.

A useful test of any specific deployment is to ask, for any given control objective, three questions in sequence: who owns this, what standard governs it, and what evidence proves it? If any of those three answers is fuzzy, the chain has a weak link. If all three answers are crisp, you have a defensible position whether you are looking at it as the asset owner, the integrator, the regulator, or the insurer.

Two other parts of 62443 also sit alongside these four. **IEC 62443-2-1** governs the asset owner's broader cybersecurity management system — the policies, procedures, training and governance that wrap around the technical work covered in 3-2 and 3-3. **IEC 62443-2-4** governs the security capabilities of service providers (typically system integrators and maintenance contractors) — the people, processes and competencies they bring to bear on your site. Both are covered in detail in IEC 62443-2-x: the management system behind a secure industrial plant . A complete picture for any single industrial site usually demands evidence under several of these parts simultaneously, with 3-2 and 3-3 forming the technical core of the design and delivery story.

The EU regulatory backdrop also bears mentioning here. Under NIS2 , asset owners in scope of Annex I sectors (energy, transport, water, manufacturing, etc.) are required to implement supply-chain security measures under Article 21(2)(d); a documented 3-2 CRS with SL-T allocation is the most defensible way to evidence that the supply-chain demands are risk-justified rather than arbitrary. Under the

Cyber Resilience Act , industrial products with digital elements placed on the EU market must meet Annex I essential requirements, which in practice are most easily evidenced through 4-2 certification with the corresponding 4-1 development process — exactly the upstream of the chain that 3-3 then integrates.

Common pitfalls and red flags

The most frequent pitfall in 3-2 work is doing the partitioning before the risk assessment. The temptation is enormous: take the existing network diagram, draw some boxes around what is already segmented at Layer 3, and call those the zones. This produces a zone map that reflects historical wiring decisions rather than current risk, and it tends to under-protect new high-consequence assets while overprotecting low-consequence legacy ones. The risk assessment must drive the partitioning, not the other way round. A useful diagnostic is to look at the zone boundaries and ask: do these boundaries align with consequence categories, or with VLAN tags? If the latter, the zoning has been done backwards.

A second common pitfall is conflating SL-T with SL-C in procurement documents. A specification that says "the system shall be SL 3" without qualification leaves the supplier to interpret whether that means components capable of SL 3 (SL-C 3), an as-built system that achieves SL 3 (SL-A 3), or a target driven by risk (SL-T 3). These imply quite different cost structures and quite different obligations. As discussed earlier, the discipline of separating the three SL types in tender language pays back many times over in the clarity of the resulting deliverable.

A third pitfall is assuming that 4-2-certified components automatically yield a 3-3-compliant system. They do not. The integration matters at least as much as the components. Insecure conduit choices, badly configured authentication systems, unprotected jump hosts, unmoni-

tored logging, shared service accounts created during commissioning and never removed — any of these can drag an SL-C 3 component set down to an SL-A 1 reality. The presence of certified components is necessary but not sufficient.

A fourth red flag is claims of "IEC 62443 compliant" without a part number. The standard has many parts, each with a defined audience. A claim of compliance from a system integrator should name 62443-3-3 (and probably 62443-2-4 for their service-delivery practices). A claim from a product supplier should name 62443-4-1 and 62443-4-2 . A claim from an asset owner should name 62443-2-1 and 62443-3-2. Any claim that does not name a part is, at best, imprecise — and usually a signal that the speaker is not familiar with how the standards family is organised.

A fifth pitfall is stale CRS documents. A CRS produced ten years ago for an SUC that has since added a new plant, two new control networks and a fleet of remote-access laptops is no longer a credible document. Refresh cycles matter, and the evidence pack should show them. A CRS without a version history or a defined review schedule is a CRS in name only.

A sixth and more subtle pitfall is the **zone scope drift**: zones that were defined narrowly during the 3-2 analysis but which, through the lifetime of the plant, have quietly absorbed additional assets through small change orders that individually seemed reasonable. The total effect is that the SL-T originally allocated to the zone no longer covers everything in the zone. Healthy asset management practice — change control that explicitly references the CRS, re-assessment when assets cross zone boundaries — is what prevents this.

A checklist for procurement and audit

The following can be used as a contract annex, a supplier questionnaire, or an internal audit checklist.

For the asset owner's own 3-2 evidence pack

- A current, version-controlled **System Under Consideration (SUC) description** with scope explicitly stated.
- An explicit **risk assessment methodology** document referencing the framework chosen (NIST SP 800-30, ISO 31000, sector-specific, or other) with scoring rules.
- A **threat catalogue** drawn from credible sources (ENISA, MITRE ATT&CK for ICS, sectoral ISACs, national CSIRT advisories) with a stated date of currency.
- A **zone and conduit diagram** showing the partitioning, with zones and conduits unambiguously labelled.
- A **risk register** capturing pre-control and residual risk per zone and per conduit.
- A **Cybersecurity Requirements Specification (CRS)** containing the SL-T vector for each zone and conduit, the assumptions, the constraints and any compensating measures relied upon.
- **Asset-owner sign-off** of the CRS at a defined seniority level, with date.
- A **review cadence** for the CRS, with evidence of past reviews and the date of the next scheduled review.

For the system integrator's 3-3 deliverable evidence pack

- A **requirements-traceability matrix** linking each SL-T in the CRS to specific System Requirements of 62443-3-3 and to the design elements that satisfy them.
- A **bill of materials** with each component's 62443-4-2 certificate referenced (or, where a component is uncertified, a written justification and the compensating controls applied).
- A **design documentation set** showing zone implementation, conduit protection mechanisms, authentication architecture,

logging architecture, backup and restore architecture, and operational interfaces.

- **Factory Acceptance Test (FAT) reports** with security-specific test cases linked to the SRs they verify.
- **Site Acceptance Test (SAT) reports** including configuration audit, vulnerability scan output, and any penetration testing performed.
- A **handover pack** including hardening guides, configuration baselines, account inventories, SIEM/logging integration documentation, backup and restore procedures, and a security operations manual.
- A **change management process** for the as-built system, defining how subsequent modifications will preserve the achieved SL-A and how the CRS will be re-consulted.
- Where applicable, an **ISASecure SSA certificate** for the system or its core platform, with scope, level and validity date.

Questions to put to a system integrator in writing

- Which version of IEC 62443-3-3 has the proposed system been engineered against?
- For each zone in our CRS, what is the proposed SL-C profile of the components selected, and how does it map onto our SL-T?
- Which components in your proposed bill of materials hold a current third-party 62443-4-2 certificate? For each, what is the certificate number, the issuing body, the certified firmware/software version, and the expiry date?
- For any component without third-party 62443-4-2 certification, what compensating measures will deliver the relevant System Requirements?

- Will the deliverable include a traceability matrix linking SL-T to SR to design element to verification test? Can we see a sample from a previous project?
- What change-management process will apply to the system after handover so that modifications do not erode the achieved SL-A?
- Are your service-delivery practices certified or assessed against IEC 62443-2-4 ?

IEC 62443-3-2 is the standard that tells the asset owner how to figure out, in a structured and defensible way, what security level each part of their industrial system actually needs. **IEC 62443-3-3** is the standard that tells the system integrator what an integrated system at that security level must actually do. Together, they sit between the asset owner's risk picture and the OEM's certified components, and they are where the chain of evidence either holds together or breaks.

Treat 3-2 as the document that justifies the entire downstream programme. A clear CRS, signed off at the right level and reviewed on a sensible cadence, is the single most important artefact an asset owner can produce — because it is the lens through which every subsequent procurement, every system upgrade, every security audit and every incident response is interpreted. Treat 3-3 as the spec against which an integrator's work is judged. A traceability matrix from CRS through to SR through to verified test result is the integrator's defence in any future dispute about whether the system was delivered as specified. And remember always that components with the right SL-C, integrated into the right zones and conduits, only become a real SL-A when somebody operates the system day after day with the security features switched on. Standards bodies cannot enforce that part — only good operations can.

IEC 62443-4-1 and 4-2: what an OEM must actually prove

13 May 2026 · 22 min read · #compliance #security #industrial #iec-62443

If you buy, specify or operate industrial kit — a PLC, an RTU, an HMI, an industrial switch, a SCADA gateway, an engineering workstation — you have almost certainly seen a supplier brochure that claims to be "compliant with IEC 62443", "aligned with 62443-4-2", or "designed to 62443 principles". Those phrases can mean almost anything, from a well-audited international certification to little more than wishful thinking on a slide deck.

The two parts of the standard that almost always get name-checked are **IEC 62443-4-1** (about how the product was built) and **IEC 62443-4-2** (about what the product can do). This article explains both in plain English, and — most importantly — sets out what an OEM must objectively demonstrate to back up a compliance claim, so that you can verify it rather than trust it.

This piece sits in the OEM/product corner of the IEC 62443 family. The system layer — how an asset owner sizes the security requirement (3-2) and how the system integrator delivers against it (3-3) — is covered in IEC 62443-3-2 and 3-3: what asset owners and integrators must prove . The management-system layer — the policies, programmes, service providers and patch discipline that wrap around the technical work — is covered in IEC 62443-2-x: the management system behind a secure industrial plant .

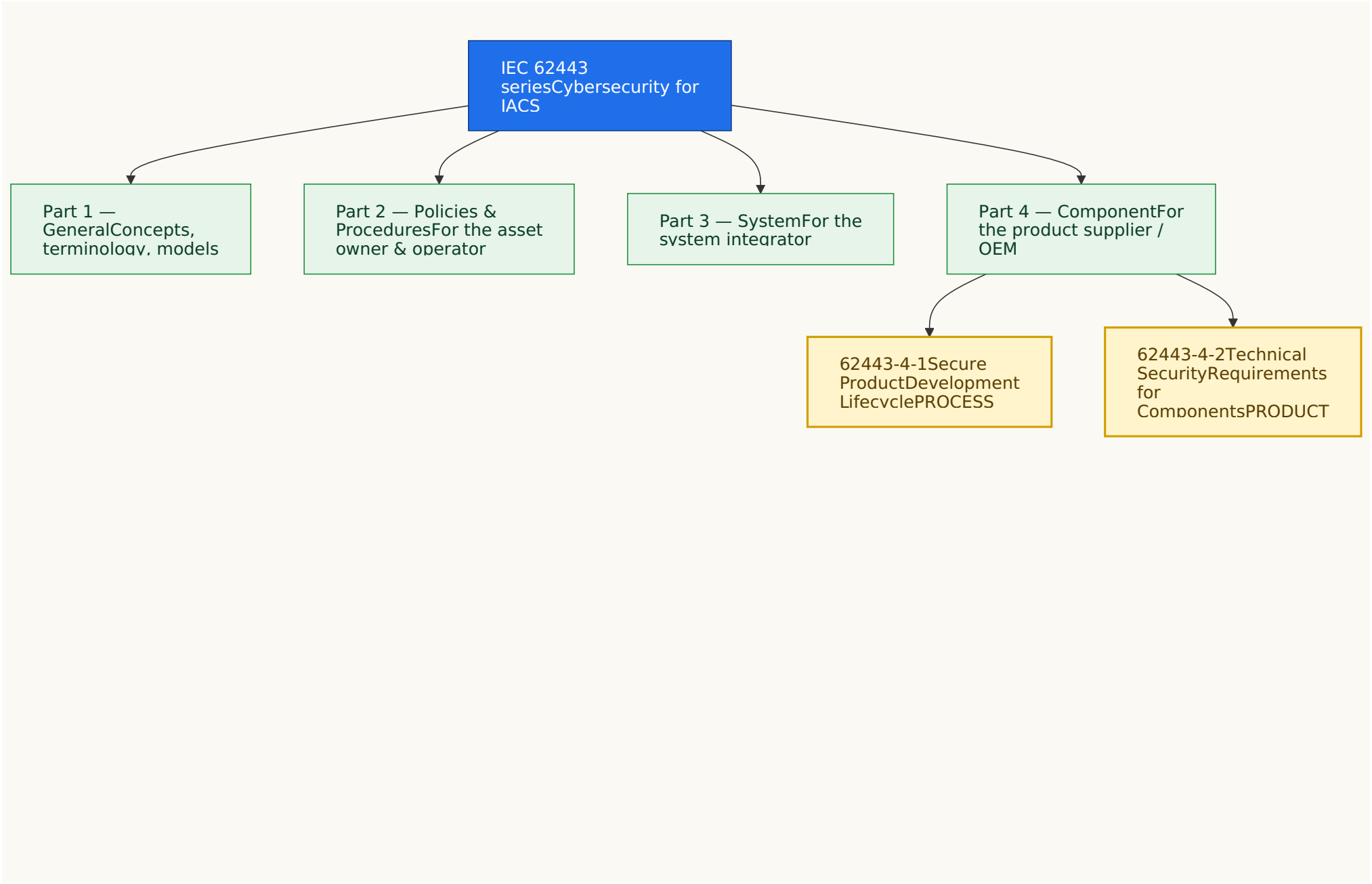
It also sits alongside two regulatory companions: the entity-side scope question, Does NIS2 apply to your EU project? , and the product-side scope question, Does the Cyber Resilience Act apply to your product? . When an industrial OEM ships into the EU, the CRA's essential requirements increasingly lean on IEC 62443-4-1/4-2 evidence

as the practical proof, and NIS2 asset-owners under Annex I cascade those same demands back through their supply-chain contracts. The documents are different audiences, but the chain of evidence runs through all of them.

You can purchase the official standards from the IEC Webstore: IEC 62443-4-1:2018 and IEC 62443-4-2:2019 .

A two-minute orientation: the IEC 62443 family

IEC 62443 is a series of standards for the cybersecurity of Industrial Automation and Control Systems (IACS). It is published jointly by the International Electrotechnical Commission (IEC) and the International Society of Automation (ISA), and it is organised into four tiers, each aimed at a different audience.


IEC 62443 seriesCybersecurity for IACS
Part 1 — GeneralConcepts, terminology, models
Part 2 — Policies & ProceduresFor the asset owner & operator
Part 3 — SystemFor the system integrator
Part 4 — ComponentFor the product supplier / OEM
62443-4-1Secure ProductDevelopment LifecycIePROCESS
62443-4-2Technical SecurityRequirements for ComponentsPRODUCT

The two we care about here both sit in **Part 4 — Component**, and they are the product supplier's responsibility:

- **IEC 62443-4-1** governs **how the product is developed** — the engineering process, the people, the controls behind the scenes.
- **IEC 62443-4-2** governs **what the product itself can technically do** — its built-in security features.

Think of it this way: 4-1 is the kitchen and the chef; 4-2 is the meal on the plate. A hygienic kitchen does not guarantee a brilliant meal, and a tasty-looking meal can still come from a filthy kitchen — which is why serious buyers want assurance about both.

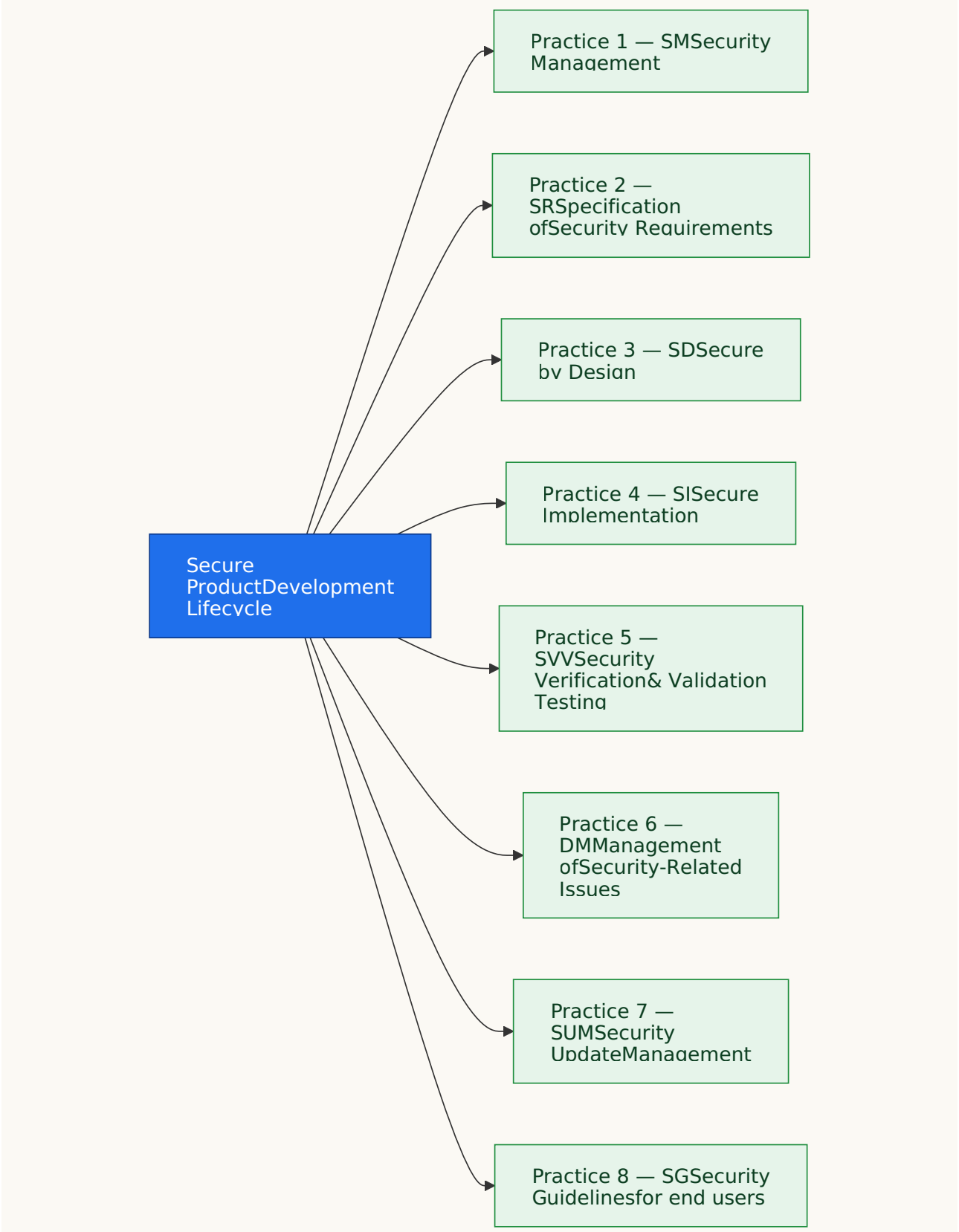
What IEC 62443-4-1 actually is

IEC 62443-4-1:2018, titled "Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements", defines a **Secure Development Lifecycle (SDL)** for industrial products. According to the IEC's own description, the standard covers "security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life" and applies to the developer and maintainer of the product, not to the integrator or end user.

In other words: 4-1 is **process-focused**. It does not ask "is the firmware secure?" It asks "did you build it in a way that makes secure firmware likely, repeatable and improvable over time?"

The 8 Practices

The standard groups its requirements into eight named **Practices**. Together they cover the entire arc from initial product idea through to end-of-support.



Across these eight Practices, the standard defines **47 top-level requirements**, which in turn unfold into hundreds of sub-requirements.

The certification body Baker Hughes notes this explicitly in its public white paper on its own IEC 62443-4-1 process assessment: "there are a total of 47 top-level requirements, this actually consists of hundreds of sub-requirements" — and helpfully publishes its own scoring against all 47.

Maturity Levels 1 to 4

IEC 62443-4-1 borrows from the Capability Maturity Model Integration (CMMI) tradition. Rather than asking "do you do X?" it asks "how well do you do X?" There are four Maturity Levels (MLs):

ML	Name	What it means in plain English
ML 1	**Initial**	The practice happens, but it is ad hoc and largely undocumented. Different teams may do things differently.
ML 2	**Managed**	Written policies and procedures exist. Staff are trained on them. The practice is repeatable.
ML 3	**Defined (Practiced)**	The documented practice is demonstrably and consistently followed across the whole organisation, with auditable evidence of use on real projects.
ML 4	**Improving**	The organisation gathers metrics about the practice, monitors its effectiveness and demonstrably uses those metrics to make it better.

A critical point that catches many buyers out: under 62443-4-1 you do not "cherry pick" — to claim a given Maturity Level, all the relevant requirements must be satisfied at that level. ML 2 across some practices and ML 3 across others is not "ML 3 overall"; it is at best ML 2 organisation-wide.

What 4-1 means practically for an OEM

Translated out of standards-speak, here is what each Practice means for the people building the product.

1. Security Management (SM) — "Someone is in charge, and it's their day job"

The OEM must have appointed roles for product security, allocated budget, defined responsibilities, and integrated security activities

into the formal product development plan. Confidential information (source code, signing keys, threat models) must be controlled. Sub-contractors and suppliers must be held to the same standard.

Analogy: it is the difference between a factory where someone is the named Safety Officer with authority, training and a budget, and one where "safety" is whoever happens to think of it that week.

2. Specification of Security Requirements (SR) — "Write down what 'secure' means for this product"

For every product (or product family), the OEM must produce a written security context: where will this device live, what threats does it face, what trust boundaries does it cross, what data flows in and out, what target Security Level (SL-T) is expected? These requirements must be approved and version-controlled.

3. Secure by Design (SD) — "Bake security in, don't bolt it on"

This is where **threat modelling** lives. The architecture and detailed design must be analysed for threats (STRIDE, attack trees, or equivalent), and the resulting mitigations must be designed in before a line of production code is written. Defence-in-depth, least privilege and secure default settings must be explicit architectural choices, not afterthoughts.

Analogy: in modern car-making, crumple zones, airbags and ABS are designed into the chassis from the first sketch. You cannot achieve the same crash safety by welding extra plates onto a finished car at the end of the line. Same logic.

4. Secure Implementation (SI) — "Write the code properly, and check the writing"

Adopted coding standards (e.g. CERT C, MISRA, SEI guidance), peer code review, static application security testing (SAST) and rules about handling untrusted input. Crucially, this also covers **third-par-**

ty and open-source components: the OEM must know what is in the product, where it came from and whether it is still supported.

5. Security Verification & Validation Testing (SVV) — "Try to break it before someone else does"

A documented testing programme that includes, at minimum: functional security testing, **vulnerability scanning**, **fuzz testing**, **penetration testing**, and **attack surface analysis**. The results are written up, defects are tracked and the test plan is repeatable.

6. Management of Security-Related Issues (DM, defect management) — "When something is found, what happens?"

A documented vulnerability handling process: how reports are received (a published security contact, ideally a coordinated disclosure policy), how they are triaged, how root-cause analysis is done, how fixes are produced and tracked, and how customers are informed. CVE assignment and a track record of CVE handling are key forms of evidence here.

7. Security Update Management (SUM) — "Patches that actually reach the field"

A documented patch and security-update process. This must cover testing of patches before release, secure delivery (signed updates), customer notification, support timelines and end-of-life policy.

8. Security Guidelines (SG) — "Tell the user how to use it securely"

User-facing documentation: hardening guides, secure configuration guidance, defence-in-depth recommendations, account-management advice, decommissioning instructions and a clear statement of which security functions exist and how to turn them on. This is the practice that most directly links 4-1 to 4-2 — because 4-2 capabilities are only useful if the customer can find and configure them.

What an OEM must objectively demonstrate for 4-1

Demonstrating compliance with IEC 62443-4-1 is the heart of the OEM's claim — and it should not be a marketing assertion. It should be a position the OEM can defend with documents on the table. Here is what those documents look like.

Documentary and procedural evidence

- A **written, version-controlled Secure Development Lifecycle policy** that maps onto all eight Practices and the 47 requirements.
- An **organisation chart** showing who owns product security, with named roles, training records and security expertise of key staff (developers, testers, architects).
- **Security training records** for development, test and product-management staff — typically annually refreshed.
- A **product security plan** for the specific product in scope, including the security context, target SL, threat model and trust boundaries.
- A **threat model document** for each product in scope (STRIDE, DREAD, attack trees or equivalent) with traceability into design and tests.
- **Security requirements traceability** from the threat model → design decisions → implementation → test cases. A buyer can ask: "Show me how threat T-17 in the threat model is mitigated in the design, where in the code, and which test confirms it."
- Written **secure coding standards** that staff use, plus **code review records** and **static analysis tool output**.
- **Software Composition Analysis (SCA)** records or an SBOM-style inventory of third-party / open-source components, with evidence of vulnerability monitoring against them.

- A documented **testing programme** with reports: vulnerability scans, fuzz test campaigns, penetration test reports, attack-surface review.
- A **published vulnerability handling and coordinated disclosure policy**, plus a track record of CVEs handled (timelines, advisories, fixes shipped).
- A **patch and security-update procedure** with a real history of advisories and updates.
- **End-user security guidelines, hardening guides and product security advisories** that the OEM publishes and maintains.

Third-party certification — the gold standard

The most credible objective evidence is a third-party certificate issued by an accredited certification body. For 62443-4-1, the two principal schemes are:

- **ISASecure SDLA** (Security Development Lifecycle Assurance), operated by the ISA Security Compliance Institute (ISCI). According to the ISASecure scheme description, SDLA "applies to the development lifecycle processes of suppliers for control system products" and "certifies compliance to ISA/IEC 62443-4-1". SDLA is offered at four levels — **SDLA Level 1, 2, 3 and 4** — corresponding to the four Maturity Levels of the standard. The certifier "evaluates the specific documented version of the organization's process to assess whether it meets the requirements stated in the SDLA specification" and "reviews representative artifacts to verify that each ISASecure SDLA requirement is being followed for products under the scope of the process."
- The **IECEE CB Scheme** for industrial cybersecurity, which provides equivalent certificates of conformity issued by IECEE-recognised CBTLs (Certification Body Test Laboratories). See www.iecee.org .

Two scope traps to watch for

Two details on any 4-1 certificate matter more than the headline:

1. **The scope of the process** — exactly which development site, which business unit and which product line is covered. A vendor that operates in five countries may only have one site certified. The certificate will say so; the brochure usually won't.
2. **The Maturity Level claimed** — and whether the assessor recorded any practices as "out of scope" or "not applicable". The Baker Hughes public certificate, for example, transparently states it was assessed at **ML 2** and that **46 of the 47** practices were in scope (one was excluded, with rationale). That is the kind of clarity to look for and to ask for.

What IEC 62443-4-2 actually is

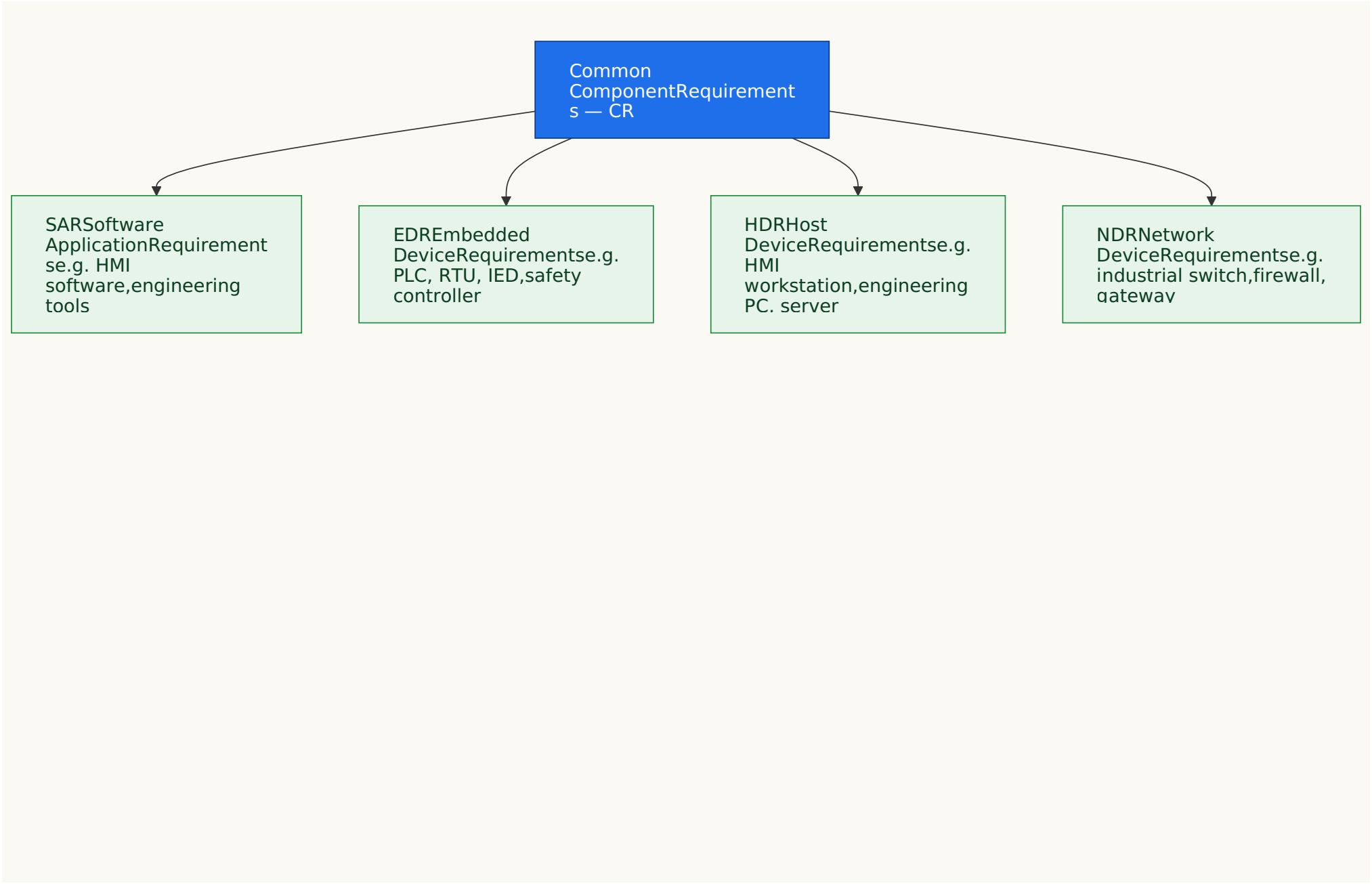
IEC 62443-4-2:2019, "Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components", defines what an individual industrial **component** must technically be able to do to claim a given Security Level. Per the IEC's own scope statement, it "provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs)" and defines the **Capability Security Level** for components, **SL-C(component)**.

Where 4-1 looks at the development organisation, **4-2 looks at the product itself** — its identification mechanisms, its access control, its cryptography, its logging, its update mechanism, its hardening, its resilience.

The four component types

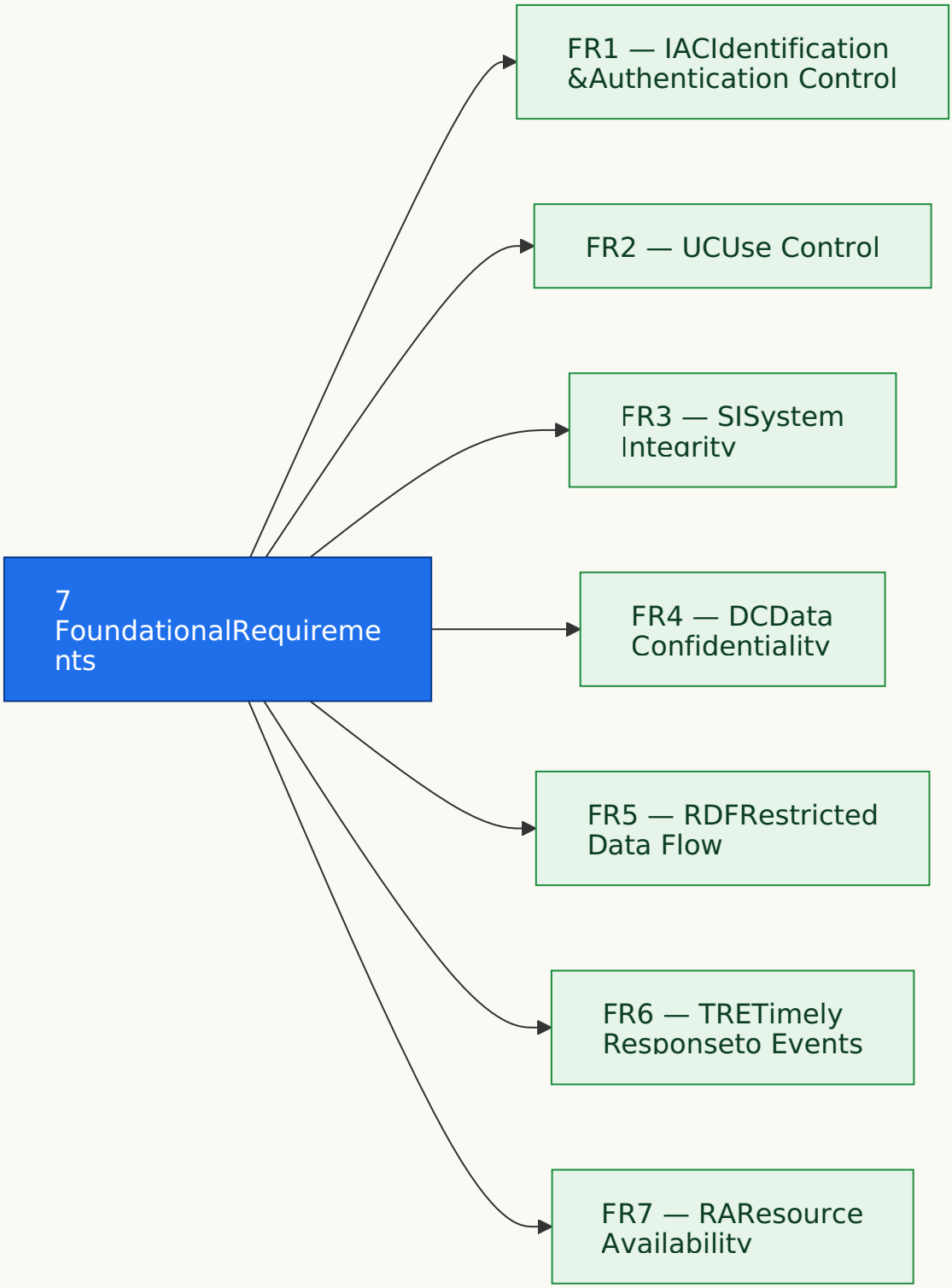
The standard recognises that "a PLC" and "a Windows engineering workstation" are not the same animal, and not all requirements apply equally to both. So requirements are split into a common core (desig-

nated **CR**, for Component Requirement) plus a layer of type-specific requirements:


Common ComponentRequirements — CR
SARSoftware ApplicationRequirement se.g. HMI software,engineering tools
EDREmbedded DeviceRequirementse.g. PLC, RTU, IED,safety controller
HDRHost DeviceRequirementse.g. HMI workstation,engineering PC. server
NDRNetwork DeviceRequirementse.g. industrial switch,firewall, gateway

The seven Foundational Requirements

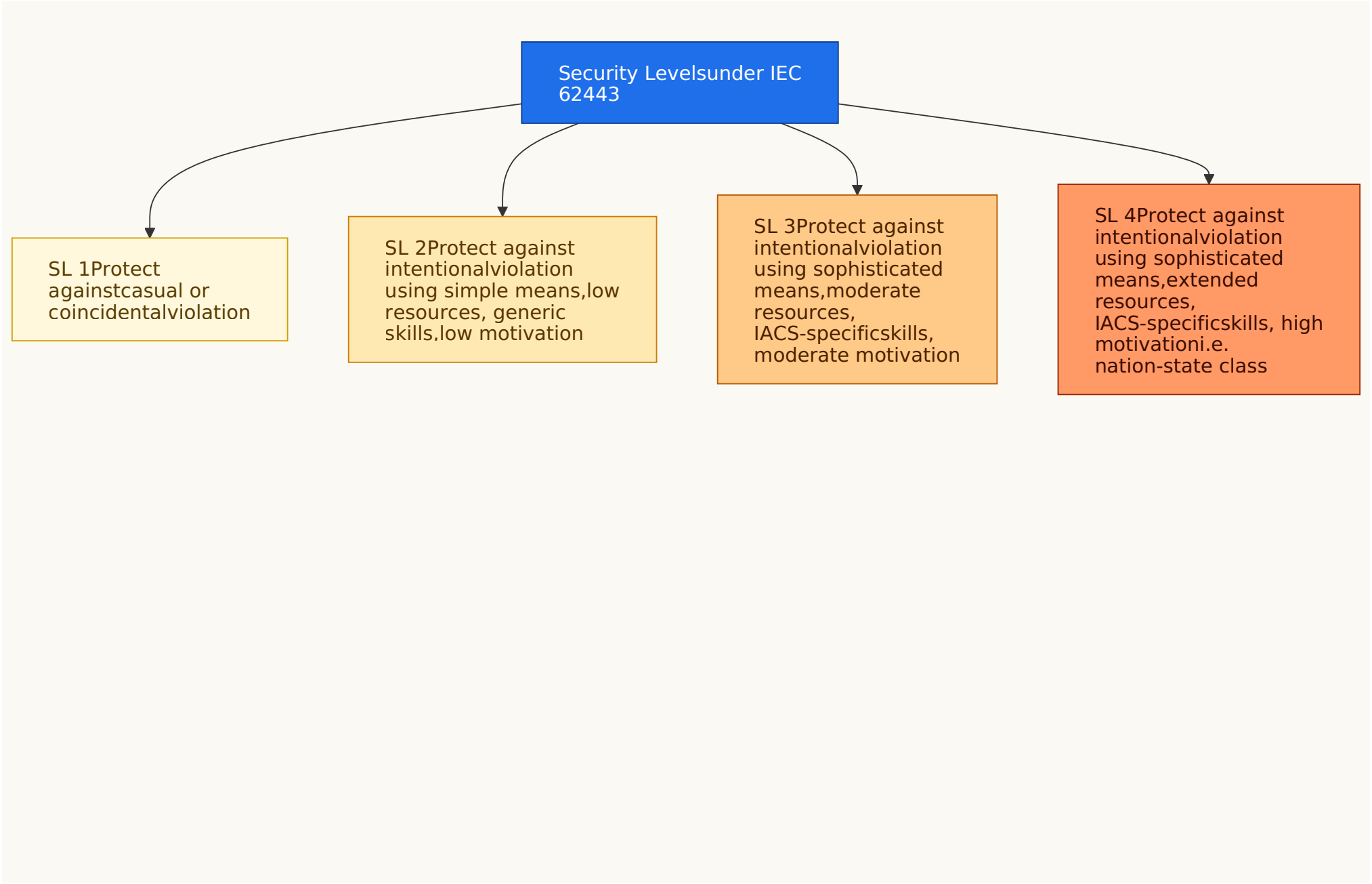
All requirements in 4-2 are derived from the **seven Foundational Requirements (FRs)** introduced way back in IEC TS 62443-1-1:



Under each FR sit a number of **Component Requirements (CRs)**, each of which may have one or more **Requirement Enhancements (REs)** that kick in at higher Security Levels. The total number of CRs is around **60–70** (commonly cited as 67) before counting REs and component-type-specific variants; the precise count depends on how you tally type-specific EDR/HDR/NDR/SAR rules. Some published summaries (such as Security Compass's overview) refer to "more than 140 specific cybersecurity requirements" when REs and component variants are included.

Security Levels 1 to 4 — graded by threat model

The genius of 4-2 is that the same requirement can apply with increasing strictness depending on who you expect to attack you. The four Security Levels are:


Security Levelsunder IEC 62443
SL 1Protect againstcasual or coincidentalviolation
SL 2Protect against intentionalviolation using simple means,low resources, generic skills,low motivation
SL 3Protect against intentionalviolation using sophisticated means,moderate resources, IACS-specificskills, moderate motivation
SL 4Protect against intentionalviolation using sophisticated means,extended resources, IACS-specificskills, high motivationi.e. nation-state class

Analogy: think of Euro NCAP crash-test ratings for cars. A one-star car is street-legal, but you do not want to put your family in it on the motorway. A five-star car is engineered to absorb a serious impact. SL 1 to SL 4 work the same way: you pick the level your operating environment justifies, and you pay (in cost, complexity and configuration overhead) accordingly. For most general industrial environments, ISASecure has publicly argued that **SL 2 is a sensible minimum baseline** for new procurement.

What 4-2 means practically for an OEM

Each FR translates into product features that a user can actually see and configure. A non-exhaustive selection:

- **FR 1 – Identification & Authentication Control (IAC):** unique user accounts, role-based identities, multi-factor authentication, password policy, account lockout, device-to-device authentication using cryptographic credentials, public-key infrastructure support.
- **FR 2 – Use Control (UC):** role-based access control, session management, session timeout, restricted execution of mobile code, USB-port control, wireless access management, **audit log** generation and protection.
- **FR 3 – System Integrity (SI):** signed firmware, **secure boot**, integrity-protected updates, malware protection, input validation, error handling that does not leak internals, tamper detection.
- **FR 4 – Data Confidentiality (DC):** encrypted communications (TLS or equivalent), protection of cryptographic keys, encryption of data at rest where relevant.
- **FR 5 – Restricted Data Flow (RDF):** zoning, segmentation, the ability to participate in a Zones & Conduits architecture, restriction of unnecessary network services.

- **FR 6 – Timely Response to Events (TRE):** audit logging with sufficient detail, log time-stamping, log forwarding (e.g. to syslog/SIEM), continuous monitoring hooks.
- **FR 7 – Resource Availability (RA):** denial-of-service resistance, fail-secure behaviour, resource exhaustion protection, backup and restore.

What changes between SL 1 and SL 4 is essentially the rigour and depth of those mechanisms. SL 1 might require "the component shall support authentication"; SL 3 will require unique per-user authentication with cryptographic mechanisms; SL 4 will add tamper-resistant credential storage and resistance to sophisticated attack.

The **component type** also matters. A PLC (EDR) is expected to have integrity-protected firmware and a hardware root of trust; an HMI workstation (HDR) is expected to support enterprise account management, anti-malware and OS hardening. Requirements are scoped to what is reasonable for the device class.

What an OEM must objectively demonstrate for 4-2

For 4-2 the evidence is **per-product and per-version**. There is no such thing as "our company is 4-2 certified" — only "this exact product, at this exact firmware version, achieves SL-C n against IEC 62443-4-2".

What "good" looks like

- The **specific product identifier**: model number, hardware revision, firmware/software version.
- A statement of the **claimed Security Level Capability (SL-C)** — usually one SL-C value per FR, sometimes published as a vector such as **SL-C (2, 2, 2, 1, 2, 2, 2)** across FR1–FR7.

- A **declaration of which component type** the product is assessed as (SAR, EDR, HDR or NDR) — and if it is a composite device, how the parts have been classified.
- **Test reports** demonstrating that each applicable CR and RE is met. Independent test reports are far stronger than self-declarations.
- A **Security Functional Specification** for end users: what each security feature does, how to enable it, and what residual risks remain if it is disabled.
- A **hardening / secure configuration guide** that tells the integrator exactly how to deploy the product so that the SL-C claim is achievable in the real installation.

The SL-C / SL-T / SL-A distinction — vital to understand

These three abbreviations get mixed up constantly and cause real procurement mistakes:

- **SL-C (Capability)** — what the product is technically able to provide when properly configured. This is what 4-2 and ISASecure CSA certify.
- **SL-T (Target)** — what the asset owner has decided is needed in a given zone of their plant, based on their risk assessment.
- **SL-A (Achieved)** — what is actually delivered once the product is installed, configured and integrated into the live system.

A product can be **SL-C 3 capable** but deployed as **SL-A 1** if the asset owner switches off the features. Conversely, you cannot exceed your weakest component: a zone built from SL-C 2 components cannot achieve SL-A 3 just by wishful thinking.

Third-party certification — the gold standard

The principal scheme is **ISASecure CSA (Component Security Assurance)**. From the ISASecure CSA-100 scheme document: CSA "fo-

cuses on the security of software applications, embedded devices, host devices, and network devices, as defined by the ISA/IEC 62443-4-2 standard" and is "designed to certify to international standards ISA/IEC 62443-4-2 and ISA/IEC 62443-4-1". The programme defines **four certification levels — CSA Capability Security Level 1, 2, 3 and 4** — and the certification examines three things in addition to the development process:

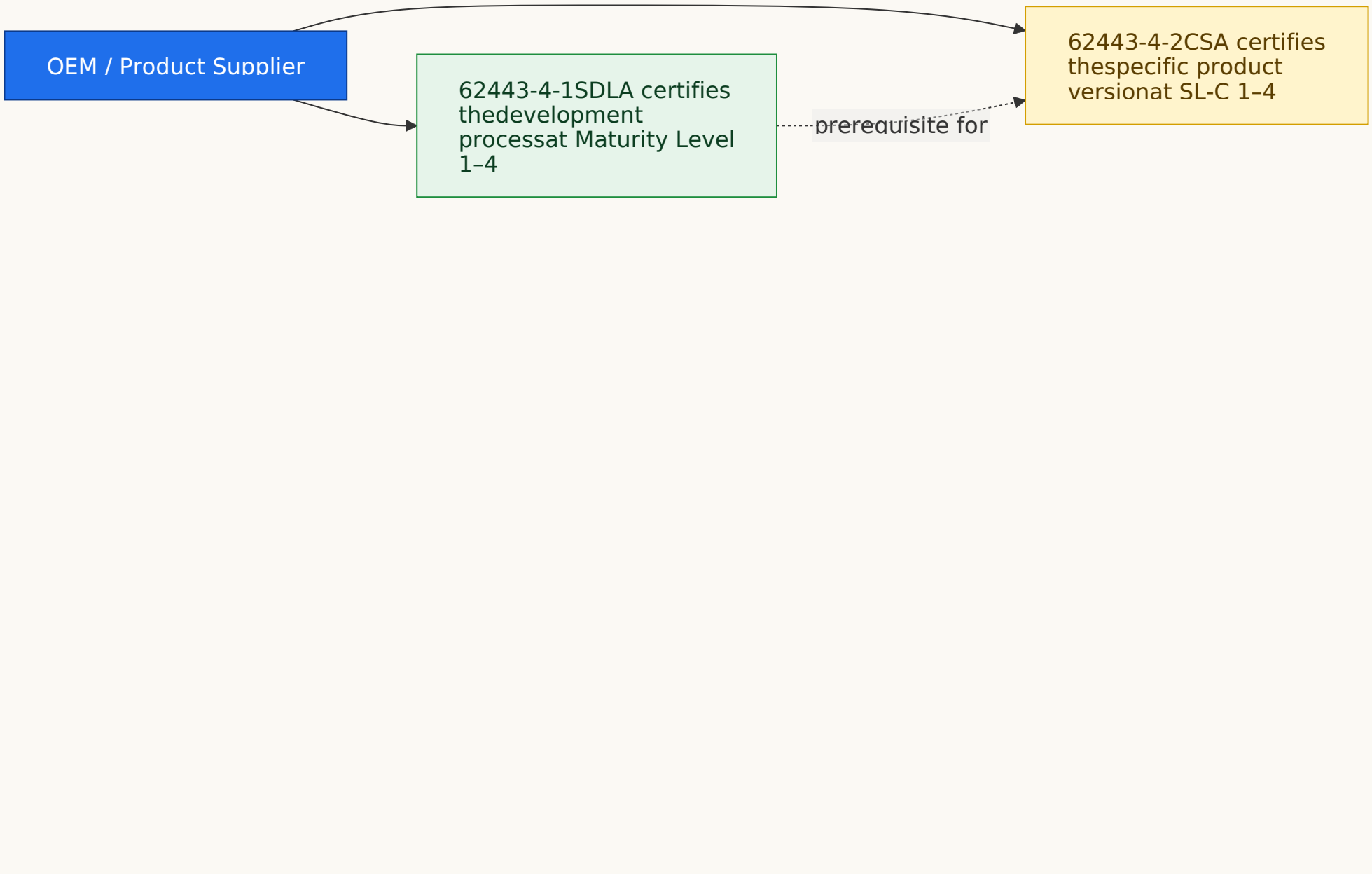
- **SDA-C (Security Development Artifacts for Components)** — the development outputs for this product.
- **FSA-C (Functional Security Assessment for Components)** — the security capabilities the product actually exposes.
- **VIT-C (Vulnerability Identification Testing for Components)** — scanning the product for known vulnerabilities.

Crucially, the CSA scheme requires the supplier to **hold a current ISASecure SDLA certification** for the development process. As the ISASecure SDLA documentation puts it: "application of ISA/IEC 62443-4-1 practices as verified by SDLA certification is intended to provide confidence that the component or system has security commensurate with its expected level of risk throughout the product's life-cycle." In short: **no SDLA, no CSA.**

A live registry of CSA-certified components is maintained at isasecure.org/end-users/iec-62443-4-2-certified-components — a good first stop for any verification exercise. There is also an IIoT-specific extension, **ISASecure ICSA**, for IIoT components and gateways, with Core and Advanced tiers.

The **IECEE CB Scheme** also issues certificates against 62443-4-2 and 62443-4-1, recognised internationally between IECEE member bodies.

How 4-1 and 4-2 fit together


OEM / Product Supplier
62443-4-1SDLA certifies thedevelopment processat Maturity Level 1–4
prerequisite for
62443-4-2CSA certifies thespecific product versionat SL-C 1–4

Two practical truths follow:

1. You can in principle imagine a 4-2-compliant product from a vendor without 4-1 certification, but in real third-party schemes — and in ISASecure CSA in particular — the development process must be assessed too. CSA explicitly requires SDLA (or equivalent SDLPA-C process assessment) as a prerequisite. So the question to ask a supplier is rarely "either 4-1 or 4-2"; it is "show me both".
2. A vendor that holds only SDLA tells you their process is sound, but not that any particular product reaches a particular SL-C. A vendor that claims CSA without underlying SDLA is making a claim that does not fit the certification scheme — treat with caution.

This is also where the EU regulatory chain joins up. Under the Cyber Resilience Act , Annex I essential requirements for products with digital elements lean heavily on demonstrable secure development and component capabilities — exactly what 4-1 and 4-2 codify for the industrial domain. And under NIS2 Article 21(2)(d), the asset owner's supply-chain security obligations cascade contractual demands back through their suppliers: in practice, that often arrives at the OEM as a request for 4-1 and 4-2 evidence.

Common pitfalls and red flags

Certain phrases and situations in an OEM's compliance claim should slow a buyer down before the contract is signed.

Red flag	Why it matters
"Designed to comply with 62443-4-2"	This is self-declaration. It is not certification. There is no independent test report.
"Compliant with IEC 62443" (no part number)	The standard has many parts addressed at different audiences. A supplier "compliant with 62443" should be able to name the specific part(s) — typically 4-1 and/or 4-2 for an OEM.
"Aligned with" or **"based on"**	Marketing language. It is not certification. Ask for the certificate.
A claim without an SL-C	4-2 is meaningless without a stated SL-C. "62443-4-2 compliant" alone tells you nothing about strength.
Vague product scope	"Our product range is 62443-4-2 certified" is almost never true — typically one model at one firmware version is. Demand the model and version.
Out-of-date certificate	ISASecure certificates have validity periods and surveillance audits. A certificate from 2019 covering firmware that has since had 25 patches may not reflect what is in the box.
Maturity Level claim without third-party audit	Self-asserted ML 3 or ML 4 carries little weight. ISASecure SDLA or an IECEE certificate is the credible artefact.
Confusion with 62443-3-3 or 62443-2-4	3-3 is a system standard for integrators; 2-4 is for service providers; 4-2 is the component standard. Suppliers sometimes wave a 3-3 certificate at a 4-2 question, or vice versa.
"Certified to SL 4" with no detail per FR	Real certificates state SL-C per FR (often as a vector). A flat "SL 4" claim across the board is suspicious.
No published hardening guide or security advisory page	Practices 7 and 8 (SUM and SG) of 4-1 require these; their absence is informative.

A buyer's checklist for procurement

Use this as a contract annex or as a supplier questionnaire.

Questions to put to the OEM in writing

1. Does the company hold a current **ISASecure SDLA** certificate (or equivalent IECEE 62443-4-1 certificate)? At what **Maturity Level**? Issued by which certification body, on which date, expiring when?
2. What is the **scope** of that SDLA certificate — which development sites, which business units, which product lines?

3. For the specific product being quoted, does it hold an **ISASecure CSA** certificate (or equivalent IECEE 62443-4-2 certificate)?
4. What is the **exact model number and firmware/software version** covered by the certificate?
5. What is the **claimed SL-C** for each of the seven Foundational Requirements (the SL-C vector)?
6. Which **component type** has been certified — SAR, EDR, HDR or NDR?
7. Please provide the **certificate PDF**, the **public certification report** (where available), and the **hardening guide / security functional specification** for the product.
8. Please provide the **vulnerability disclosure policy URL** and a list of CVEs handled in the last 24 months for this product family.
9. What is the **support and patch lifetime** of the product, and the documented end-of-life policy?
10. Please describe the **SBOM** or third-party component inventory available for this product.

Documents to demand on file

- SDLA / IECEE 62443-4-1 certificate.
- CSA / IECEE 62443-4-2 certificate per product and version.
- Product Security Functional Specification.
- Hardening / secure configuration guide.
- Vulnerability disclosure policy.
- Sample security advisory (to confirm a real disclosure process exists in practice).

Verification steps

- Cross-check the certificate number on the **ISASecure certified products registry** at isasecure.org/end-users/iec-62443-4-2-certified-components .

- For IECEE certificates, verify on the IECEE CB Scheme certificate database at iecee.org .
- Confirm the **certificate is in date** and the scope statement matches the model and firmware you are actually buying.
- Compare the SL-C vector against your own SL-T from your risk assessment.
- Ask for evidence that the product as shipped to you matches the certified version — patches and minor releases can move the product outside the certified scope.

IEC 62443-4-1 asks the OEM "Are you the sort of organisation that can build secure products, repeatably, and keep them that way?" **IEC 62443-4-2** asks the same OEM "Does this exact product, at this exact version, have the technical security features needed to resist the threats in its operating environment?"

Together they form one of the most rigorous answers the industrial world has to "how do I know this OEM is serious about cybersecurity?" — but only if you read past the brochure to the certificate, and past the certificate to its scope.

Treat them as the foundation, not the finish line. A certified product, badly deployed and never patched, is no more secure than an uncertified one. And an uncertified product, however well-intentioned the vendor, is asking you to take all the assurance on trust.

Mapping IEC 62443 controls to NIS2 Article 21 measures

14 May 2026 · 31 min read · #compliance #security #industrial #iec-62443 #nis2

Picture a Nordic wind operator that receives two reports back-to-back: an IEC 62443 capability assessment from a well-known classification society, and a NIS2 gap analysis from a Big Four firm. The 62443 report says the organisation is sitting comfortably at Security Level 2 across most zones, with a credible path to SL-3 on the SCADA zone. The NIS2 report says there are "material gaps" in supply-chain governance, incident-reporting timelines and management-body accountability. Same plants. Same people. Same week.

Which one is wrong?

Neither. They are measuring different things — and the load-bearing assumption underneath the question ("if we're 62443-compliant we're NIS2-compliant") is one of the most expensive misunderstandings in operational technology security today. This post is the long-form answer to that question: a measure-by-measure walk through NIS2 Article 21(2)(a) through (j), mapped to specific clauses of the IEC 62443 series , with an honest rating of how tight the fit really is and a list of what an asset owner — particularly a renewable-energy asset owner — still has to produce on top of any 62443 evidence pack.

TL;DR

If you read nothing else: **IEC 62443 and NIS2 Article 21 overlap heavily at the technical-control level — roughly 70% — but NIS2 adds three things that IEC 62443 simply does not cover: legal incident-reporting timelines (24 hours, 72 hours, one month), explicit management-body liability, and a supply-chain notification regime.** A clean `IEC 62443-3-3` SL-2 system will satisfy

most of measures (a), (c), (e), (g), (h), (i) and (j) on its technical face, but the asset owner still has to produce the policy artefacts, the legal-evidence trail and the reporting playbook on top. Treat 62443 as the engineering substrate and NIS2 Article 21 plus Commission Implementing Regulation (EU) 2024/2690 as the governance and reporting overlay — never the other way round.

1. Why this mapping matters — and the load-bearing assumption everyone makes

In OT security reviews across solar parks, onshore wind farms, run-of-river hydro plants and grid-tied battery energy storage systems (BESS), one assertion comes up reliably: "We're moving to 62443, so we'll be NIS2-compliant by default."

It is roughly true at the technical-control level. The seven Foundational Requirements (FRs) of `IEC 62443-3-3:2013` — identification and authentication control, use control, system integrity, data confidentiality, restricted data flow, timely response to events, resource availability — line up reasonably well with the technical pillars of NIS2 Article 21(2). If you can demonstrate SL-2 across all seven FRs on the operational zone of a wind farm, you have evidence for a substantial portion of what Article 21 expects.

It is wrong everywhere else. NIS2 is a piece of EU law: a directive that, once transposed by each Member State, creates obligations on **legal persons**, on **management bodies** and on **incident notification flows to a national CSIRT**. IEC 62443 is a voluntary technical standard authored by IEC TC 65/WG 10 and ISA99; it has no view on whether you have a registered legal entity, no view on whether the board has approved your risk-management measures, and no concept of an early warning to a Computer Security Incident Response Team within 24 hours.

A reminder on NIS2 scope before we go further: the directive applies to **essential** and **important** entities, with energy listed as a sector of "high criticality" in Annex I. Generators of electricity, system operators, distribution and transmission operators, and — relevantly for the renewable space — operators of district heating, hydrogen and oil and gas all fall in scope where they meet the size thresholds (typically 50+ headcount or EUR 10 million turnover, with sector-specific exceptions). I have walked through scope in more detail in the NIS2 applicability post — go and read that first if you are still working out whether your group is in scope at all.

2. The five differences in shape before we even start mapping

Before mapping a single control, it is worth being honest about the structural mismatch between the two documents. Five differences in **shape**, not content, account for most of the friction:

(i) Risk-management orientation versus capability orientation. NIS2 Article 21(1) is explicit that entities "shall take appropriate and proportionate technical, operational and organisational measures to manage the risks". The directive cares about outcomes. `IEC 62443-3-3` and `-4-2`, by contrast, give you a catalogue of capabilities at four Security Levels and let you choose, via `IEC 62443-3-2` zoning, where to apply them. The 62443 audit asks "does this zone deliver the SL-T?". The NIS2 audit asks "have you reduced the risk to your essential service to an acceptable level?". Both questions are reasonable; they are not the same question.

(ii) Timing obligations. Article 23 of NIS2 imposes a three-stage reporting cadence — early warning within 24 hours, incident notification within 72 hours, final report within one month — that has no equivalent anywhere in the 62443 series. SR 6.2 "Continuous monitoring" tells you to detect events; it tells you nothing about whom to call.

(iii) Management-body responsibility. Article 20 of NIS2 makes management bodies of essential and important entities **personally** accountable for approving the cybersecurity risk-management measures and overseeing their implementation, and requires them to follow training. `IEC 62443-2-1:2024` expects senior management commitment — the new Security Programme Element structure makes that explicit — but it does not, and cannot, compel personal legal liability.

(iv) Supply-chain reach. NIS2 Article 21(2)(d) requires entities to manage the security of "the relationships between each entity and its direct suppliers or service providers". `IEC 62443-2-4:2023` is the obvious near-match — it specifies the security programme for IACS service providers — but only the asset owner can contractually impose it, and only NIS2 makes the failure to do so a legal matter.

(v) Voluntary versus enforced. IEC 62443 compliance is something you choose, sometimes certify, and use to win tenders. NIS2 is something the national supervisory authority — in Norway's case the National Security Authority (NSM, Nasjonal sikkerhetsmyndighet) — will eventually audit you against and fine you for missing. In Norway specifically, as of May 2026, this is still a moving target: the current `digitalsikkerhetsloven` (LOV-2023-12-20-108) entered into force on 1 October 2025 and implements the **NIS1** regime. NIS2 itself has not yet been incorporated into the EEA agreement and is expected to be transposed during 2026, likely in a new combined cyber/CER law that will supersede the present digitalsikkerhetslov. The five differences above apply whether the Norwegian transposition lands in June 2026 or December 2026 — they are baked into the directive itself.

With that out of the way, on to the ten measures.

3. Measure (a) — policies on risk analysis and information system security

> "policies on risk analysis and information system security"

Primary IEC 62443 parts: `IEC 62443-2-1:2024`, `IEC 62443-3-2:2020`.

Specific clauses. In the 2024 second edition of `-2-1`, the Security Programme Elements (SPEs) covering this measure are ORG 1 "Security programme management" and ORG 2 "Risk management". The risk-assessment methodology that the asset owner is required to operate sits in `IEC 62443-3-2:2020` — zone and conduit partitioning of the System under Consideration (SuC), assessment of cybersecurity risk per zone, and derivation of the Target Security Level (SL-T) for each zone and conduit. Annex A of `-3-2` provides a worked example of the methodology.

Fit: tight. `IEC 62443-3-2` is genuinely a risk-management methodology. If you have done the SuC partitioning for a 250 MW solar park — separated the inverter control zone from the SCADA zone from the corporate IT zone, derived SL-T values per zone, and documented the residual risk — you have produced almost exactly what NIS2 Article 21(2)(a) asks for. The ENISA Technical Implementation Guidance published in June 2025 explicitly recognises ISO/IEC 27001 and "relevant sector standards" as bases for the policy; `IEC 62443-3-2` is one of those relevant sector standards in the OT space.

What you must prove on top. Three things. First, a board-approved written policy (not just a methodology) that says how risk analysis is performed, by whom, on what cadence, and what the acceptance criteria are. Second, traceability — the risk register must show what risks were identified, what controls were applied, and which residual risks the management body has accepted. Third, periodic review — Annex 2.1 of `(EU) 2024/2690` calls for "regular" review, which the ENISA

guidance interprets as at least annually. A common failure mode on a hybrid solar-plus-BESS site is beautiful 62443 zone diagrams sitting alongside a nine-month-stale risk register; the gap, when it appears, is governance, not engineering.

Renewable-energy specific note. The risk picture changes when you bolt a 100 MWh BESS onto a 50 MW solar plant: a single zone in your 2022 SuC partitioning becomes three zones overnight. Re-run `-3-2` whenever the plant topology changes, and capture the change in the risk register that NIS2 will want to read.

4. Measure (b) — incident handling

> "incident handling"

Primary IEC 62443 parts: `IEC 62443-2-1:2024`, `IEC 62443-3-3:2013` Foundational Requirement 6.

Specific clauses. In `-2-1:2024` the relevant SPE is the incident-handling element (formerly clause 4.3.4.5 in the 2010 edition; in the 2024 edition the requirements are restructured under an SPE that covers identification, response, recovery and post-incident review). On the technical side, `IEC 62443-3-3:2013` provides FR 6 "Timely response to events" — specifically SR 6.1 "Audit log accessibility" and SR 6.2 "Continuous monitoring" — together with SR 2.8 "Auditable events", SR 2.9 "Audit storage capacity", SR 2.10 "Response to audit processing failures" and SR 2.11 "Timestamps" from FR 2. Component-level mirroring is in `IEC 62443-4-2:2019` CR 2.8 through CR 2.12 and CR 6.1, CR 6.2.

Fit: partial. Two halves, one fits, one doesn't. The detection and analysis half of incident handling is well-covered: 62443 gives you the logging, monitoring and forensic capability needed to know an incident has happened. The reporting and external communication half is essentially absent. IEC 62443 says nothing about the 24-hour early-

warning duty, nothing about CSIRT contact, nothing about cross-border notification, and nothing about the content of a final report.

What you must prove on top. A documented incident-response plan that explicitly names the national CSIRT (in Norway, NSM via the National Cyber Security Centre, NCSC), defines the trigger criteria for a "significant incident" using the thresholds in `(EU) 2024/2690` Article 3 (where applicable) or the national transposition, and assigns named roles to draft and send the 24-hour early warning, the 72-hour notification and the one-month final report. The plan must be tested. Records of tabletop exercises that include the reporting path, not just the technical response, are the artefact auditors will look for. The familiar failure mode on a wind-farm tabletop is that the technicians know exactly how to isolate the affected turbine SCADA segment within an hour, but nobody on shift has the NSM portal login or knows the threshold definitions. That is the gap NIS2 will fine you for.

5. Measure (c) — business continuity, backup, disaster recovery and crisis management

> "business continuity, such as backup management and disaster recovery, and crisis management"

Primary IEC 62443 parts: `IEC 62443-2-1:2024`, `IEC 62443-3-3:2013` Foundational Requirement 7.

Specific clauses. `-3-3` FR 7 "Resource availability" gives you SR 7.1 "Denial of service protection", SR 7.2 "Resource management", SR 7.3 "Control system backup", SR 7.4 "Control system recovery and reconstitution", SR 7.5 "Emergency power" and SR 7.6 "Network and security configuration settings". Component-level: `-4-2` CR 7.1 through CR 7.6. On the management-system side, `-2-1:2024` contains business-continuity-management requirements as an SPE covering backup policy, restoration testing and continuity exercises.

Fit: tight (for IACS scope) — but with one important caveat. SR 7.3 and SR 7.4 are excellent: they require not just that backups exist, but that they are verified, that recovery to a known-good state is achievable, and that the recovery process itself is documented and tested. This goes beyond what most ISO 27001 backup controls demand. NIS2 Article 21(2)(c) and the corresponding section in the `(EU) 2024/2690` Annex (point 4) ask broadly the same thing.

The caveat: 62443 is scoped to the IACS. Business continuity under NIS2 covers the essential service — for a renewable operator that means delivering power to the grid, which depends on the IACS, the SCADA back-haul, the energy management system, the dispatch interface to the TSO, the metering chain, and so on. A perfect SR 7.3/7.4 implementation on the wind farm SCADA does not save you if the corporate-IT dispatch portal is encrypted by ransomware. The asset owner needs a continuity plan whose scope is the essential service, with the IACS portion satisfied by the 62443 controls.

What you must prove on top. A documented business-continuity and disaster-recovery (BCDR) plan covering the essential service end-to-end; defined recovery time objectives (RTOs) and recovery point objectives (RPOs) per critical process; offline, immutable backups of SCADA configurations, PLC logic and historian data (SR 7.3 evidence); records of at least annual restoration tests on representative assets; a crisis-management procedure that names roles, escalation paths and external communications. On a 200 MW onshore wind farm, "we back up the SCADA database nightly" is not enough — auditors will want to see the last successful restoration test of the actual turbine controller logic onto a spare unit.

6. Measure (d) — supply chain security

> "supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers"

Primary IEC 62443 parts: `IEC 62443-2-4:2023`, `IEC 62443-4-1:2018`, `IEC 62443-2-1:2024`.

Specific clauses. `IEC 62443-2-4:2023` is the security programme for IACS service providers — it defines what an integrator or maintenance provider must do across staffing, training, scope of services, hardening, network architecture, wireless, malware protection, patch management, backup/restore, project staffing, secure remote access and so on. For product suppliers, `IEC 62443-4-1:2018` defines the Secure Product Development Lifecycle requirements across eight practices: SM (security management), SR (specification of security requirements), SD (secure by design), SI (secure implementation), SVV (security verification and validation testing), DM (management of security-related issues), SUM (security update management) and SG (security guidelines). On the asset-owner side, `-2-1:2024` has a procurement/SPE covering supplier selection, contract security requirements and onboarding.

Fit: partial — but the strongest partial in the standard. `-2-4` and `-4-1` are by far the most direct technical answer to NIS2's supply-chain measure that exists in any voluntary standard today. If you require your wind-turbine OEM to operate to `-4-1` and your SCADA integrator to operate to `-2-4`, you have done most of the technical heavy lifting. The Annex to `(EU) 2024/2690` (section 5) on supply chain security overlaps substantially with `-2-4`'s service-provider requirements. The deeper walkthrough of `-2-4` and `-4-1` lives in the OEM-side post .

Where it falls short: NIS2 expects the asset owner to take a **risk-based** view of suppliers, including non-IACS suppliers (cloud providers, ICT outsourcers, managed security service providers), to consider the supplier's own vulnerability to a threat, and to factor in the European Coordinated Risk Assessment results published periodically by ENISA and the NIS Cooperation Group. None of that is in `-2-4`. Furthermore, `-2-4` only binds you if you make it binding by contract; NIS2 makes it binding by law.

What you must prove on top. A documented supplier risk-management policy, a tiered supplier register with risk classifications, contractual security clauses in every relevant supplier contract (including incident notification clauses with timelines that allow you to meet your own 24-hour duty), evidence that critical suppliers' security claims have been reviewed (e.g. an `IEC 62443-4-1` Maturity Level certificate, an ISO/IEC 27001 certificate, a SOC 2 Type II report), and ongoing monitoring. For a hybrid renewable site with three OEMs (turbines, PV inverters, BESS), three integrators and a remote SCADA-as-a-service provider, the supplier register alone is non-trivial.

Renewable-energy specific note. This is the measure where the EU's Cyber Resilience Act (CRA, Regulation (EU) 2024/2847) will eventually do you a favour. Once CRA bites in late 2027, product suppliers placing inverters, SCADA gateways and BESS controllers on the EU market will be required to ship them with documented vulnerability handling, an SBOM and a security-update channel — see the CRA applicability post for the detail. Until then, you contract for it.

7. Measure (e) — security in acquisition, development and maintenance, including vulnerability handling and disclosure

> "security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure"

Primary IEC 62443 parts: `IEC 62443-4-1:2018`, `IEC TR 62443-2-3:2015`, `IEC 62443-2-1:2024`, `IEC 62443-3-3:2013` FR 3.

Specific clauses. Vulnerability handling and disclosure for product suppliers is `-4-1` practice DM "Management of security-related issues" (DM-1 through DM-6) and practice SUM "Security update management" (SUM-1 through SUM-5). For the asset owner, patch management is covered in `IEC TR 62443-2-3:2015`, which defines the exchange format and process between asset owner and product supplier for security patches. Software-integrity controls at the system level are `-3-3` SR 3.4 "Software and information integrity"; at component level, `-4-2` CR 3.4. The acquisition policy itself lives in `-2-1:2024` under its procurement SPE.

Fit: tight on the technical mechanics, partial on the policy and disclosure. The technical machinery of vulnerability handling — receiving a CVE notification, assessing applicability to a specific firmware version, scheduling a patch through a maintenance window, verifying integrity of the patch before installation — is well-specified in `-4-1` DM/SUM and `IEC TR 62443-2-3`. The 2024 `-2-1` similarly covers patch-management policy for the asset owner.

Where it gets thinner: NIS2 expects a **coordinated vulnerability disclosure** (CVD) capability — somewhere a researcher can responsibly report a vulnerability in your environment, with a defined process for triage and acknowledgement. `IEC 62443-4-1` DM addresses this for the product supplier, but for an asset owner running custom integration code or in-house engineering applications, the CVD obligation sits with you and the standard does not give you a process. NIS2 also expects you to monitor public vulnerability sources (ENISA's EU vulnerability database , national CSIRT advisories, CISA ICS advisories) — `IEC TR 62443-2-3` mentions this in passing but does not specify the monitoring cadence.

What you must prove on top. A documented patch-management procedure with SLAs by criticality (e.g. CVSS ≥ 9.0 patched within 30 days of OEM availability, or formally risk-accepted with compensating controls); a coordinated vulnerability disclosure policy with a published contact (security.txt or a security@ address); evidence that you subscribe to and triage advisories from your OEMs and from at least one national CSIRT; change-management records showing patches applied and tested. On the maintenance side, evidence that maintenance interventions — e.g. an OEM service engineer connecting to a turbine controller — follow secure remote-access procedures (`-2-4` SP.05 and SP.06).

8. Measure (f) — policies and procedures to assess the effectiveness of cybersecurity risk-management measures

> "policies and procedures to assess the effectiveness of cybersecurity risk-management measures"

Primary IEC 62443 parts: `IEC 62443-2-1:2024`.

Specific clauses. This measure is essentially "do you check that the other measures are working?" — the equivalent of ISO 27001 clauses 9.1 to 9.3 (monitoring/measurement, internal audit, management review). In `-2-1:2024` the relevant SPEs cover monitoring, measurement, internal audit and management review of the IACS Security Programme; the 2024 edition introduces a maturity model (Maturity Levels 1 to 4) that is specifically designed to be used as the measurement scale. The full walkthrough of those SPEs is in the management-system post . `IEC 62443-3-3` Annex A gives you the SL-Achieved derivation that is the technical equivalent.

Fit: tight at the management-system level — but only in the 2024 edition. The 2010 edition of `-2-1` was vague here; the 2024 second edition fixes it. The SPE structure and the maturity model

give you a defensible methodology for measuring effectiveness. The Annex to `(EU) 2024/2690` (point 7) maps directly onto this.

What you must prove on top. Less than you might think, if you have moved to `-2-1:2024`. You need: an annual internal audit programme covering the IACS security programme, with documented findings and corrective actions; a management-review schedule with minuted decisions; KPIs/metrics tied to the maturity model; evidence that the metrics drive change. The element NIS2 will scrutinise most heavily is whether the management body actually receives and acts on the review output — this connects directly to Article 20.

9. Measure (g) — basic cyber hygiene and cybersecurity training

> "basic cyber hygiene practices and cybersecurity training"

Primary IEC 62443 parts: `IEC 62443-2-1:2024`, `IEC 62443-2-4:2023`.

Specific clauses. In `-2-1:2024` there is a dedicated SPE for personnel security and awareness training — covering role-based training, awareness refresh cadence, and competence assessment. `-2-4:2023` mirrors this on the service-provider side: SP.02 "Staffing" requires the integrator to demonstrate that its personnel are trained and assessed. The hygiene side — password rules, software whitelisting, endpoint hardening, secure browsing — is implied by various `-3-3` SRs (SR 1.7 "Strength of password-based authentication", SR 2.4 "Mobile code", SR 3.2 "Malicious code protection") and explicit at component level in `-4-2`.

Fit: tight at the workforce level, weak at the management-body level. The hygiene controls are well-covered. Training of operations staff and engineers is well-covered. What IEC 62443 does not give you is the **board-level** training duty that NIS2 Article 20(2) imposes

on members of management bodies — that training is sui generis to the directive.

What you must prove on top. Training records by individual, by role, with curriculum content mapped to the Article 21(2) measures; refresh frequency (typically annual); a separate, evidenced training programme for management body members covering their governance duties under Article 20 and the entity's incident-reporting flow. Phishing simulation results, while not required, are useful evidence. The piece most often missing in NIS2-readiness audits is not the technician training — that has usually been running for years — but the absence of any board-level cyber risk briefing in the last twelve months of board minutes.

10. Measure (h) — cryptography and, where appropriate, encryption

> "policies and procedures regarding the use of cryptography and, where appropriate, encryption"

Primary IEC 62443 parts: `IEC 62443-3-3:2013` FR 4, `IEC 62443-4-2:2019`.

Specific clauses. At system level: SR 3.1 "Communication integrity", SR 3.8 "Session integrity", SR 4.1 "Information confidentiality", SR 4.3 "Use of cryptography". At component level, `-4-2` CR 3.1, CR 3.8, CR 4.1, CR 4.3, plus `-4-2` CR 1.8 "Public key infrastructure certificates" and CR 1.9 "Strength of public key-based authentication" where applicable. `-2-1:2024` provides the SPE for key-management policy. The deeper system-side context is in the system-design post .

Fit: partial. The 62443 controls tell you what needs to be protected (communications, sessions, stored data, authenticators) and that cryptography is the means. They are largely silent on which algorithms, which key lengths, crypto-agility or post-quantum readiness. NIS2's Annex 2.4 in `(EU) 2024/2690` and the ENISA guidance both ex-

pect a documented cryptography policy that names approved algorithms, prohibits deprecated ones (3DES, MD5, SHA-1, RC4), defines key lifecycle and addresses crypto-agility.

What you must prove on top. A cryptography policy that lists approved algorithms (typically referencing BSI TR-02102 , NIST SP 800-131A Rev. 2 or ENISA's algorithm recommendations); a key-management procedure covering generation, distribution, storage, rotation and destruction; an inventory of where cryptography is used in the IACS (think: PROFINET Security, OPC UA endpoints, IPsec/VPN tunnels back to the NOC, BESS controller TLS, smart-meter authentication, signed firmware verification); evidence of compliant configurations. **Crucially, NIS2 does not require you to encrypt every OT link** — IEC 62443 is correct that on a deterministic real-time bus, encryption can be the wrong answer. The policy must document where you have decided encryption is not appropriate and why.

Renewable-energy specific note. Inverter-to-controller traffic on a PV site, turbine-to-park-controller traffic on a wind farm, and BMS-to-PCS traffic in a BESS are common areas where bandwidth and latency push you away from TLS. Document the decision; do not pretend it does not exist.

11. Measure (i) — HR security, access control and asset management

> "human resources security, access control policies and asset management"

Primary IEC 62443 parts: `IEC 62443-2-1:2024`, `IEC 62443-3-3:2013` FRs 1 and 2, `IEC 62443-4-2:2019`.

Specific clauses. This measure is a trio. Access control is `-3-3` FR 1 "Identification and authentication control" (SR 1.1 through SR 1.13) and FR 2 "Use control" (SR 2.1 through SR 2.12), with their compo-

nent counterparts in `-4-2`. Asset management lives in `-2-1:2024` under a dedicated SPE — the 2024 edition is much sharper here than the 2010 edition, with CM (Configuration Management) elements covering asset inventory baselines, configuration baselines and change control. HR security — joiner/mover/leaver, screening, NDAs, termination — is an SPE in `-2-1:2024` (personnel security).

Fit: tight. This is probably the cleanest mapping in the directive. If you have SL-2 on FR 1 and FR 2, an up-to-date IACS asset register with configuration baselines, and an SPE-compliant joiner/mover/leaver process, you have ticked the boxes for NIS2 Article 21(2)(i).

What you must prove on top. Three artefacts. First, an asset inventory that is current — auditors will sample. For a 50-turbine wind farm, "current" means the inventory reflects the firmware version actually running on each turbine, not the version that was deployed at commissioning. Second, role-based access control matrices showing who has what privilege on which zone, with evidence of periodic recertification (NIS2 expects at least annually, more often for privileged accounts). Third, evidence that leavers' access is revoked promptly — a stale account belonging to a contractor who left two years ago is the kind of finding that surfaces routinely under access-recertification scrutiny.

12. Measure (j) — multi-factor authentication, secured communications

> "the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate"

Primary IEC 62443 parts: `IEC 62443-3-3:2013` FR 1, `IEC 62443-4-2:2019`.

Specific clauses. Multi-factor authentication appears explicitly in `-3-3` SR 1.1 RE 1 "Unique identification and authentication" and is required by SL-2 and above for human users accessing the control system from untrusted networks (SR 1.13 "Access via untrusted networks"). At component level, `-4-2` CR 1.1, CR 1.7, CR 1.13 carry the same requirements. Secured communications channels are FR 3 and FR 4 territory (see measure (h)).

Fit: partial. MFA mapping is tight at SL-2 and above for remote access. Where the fit weakens is on "secured voice, video and text communications and secured emergency communication systems" — that bullet was clearly drafted with telecom, public-administration and emergency-services entities in mind. IEC 62443 has nothing about hardened voice or radio comms. For most renewable operators this is read as "ensure your operational comms — radio between substation and control centre, Teams or comparable used for operational coordination, satellite or 4G/5G backhaul from a remote wind farm — uses appropriate confidentiality and integrity controls" and is satisfied through `-3-3` FR 3/FR 4 plus a procurement decision on the comms platform.

What you must prove on top. MFA enforcement evidence for all remote access (vendor maintenance, engineering access, SCADA-from-laptop): exported configuration showing MFA is required, not optional. A continuity plan for the operational comms channel — what happens to your radio fallback or satellite link if the primary fails. For "secured emergency communications", a procedure showing how the operations team will reach NSM/NCSC, the OEM, and the TSO if the corporate comms platform is itself compromised — this is one of the NIS2 obligations most likely to catch operators out, because most assume their normal Teams or email channel will be available during an incident.

13. Where IEC 62443 has controls NIS2 doesn't ask for explicitly — the reverse mapping

It is worth turning the question around for a moment. Where does IEC 62443 go beyond NIS2 Article 21?

Zoning and SL-T derivation. `IEC 62443-3-2` is foundational to the 62443 approach but is not literally named in NIS2. You will not get a NIS2 finding for failing to partition your SuC into zones and conduits — provided your risk assessment produces an equivalently rigorous result. But if you have done `-3-2` properly, you have the most defensible artefact for Article 21(2)(a) that any OT auditor will ever ask to see. The standard's discipline is more rigorous than NIS2 strictly demands.

Capability/maturity model. Security Levels (SL-C, SL-T, SL-A) on the technical side and Maturity Levels 1 to 4 on the programme side are 62443-specific constructs. NIS2 has nothing equivalent — the directive does not ask "what SL did you achieve on your wind park's safety zone?". For internal benchmarking and for tender responses to other 62443-aware buyers, SL/ML matters; for the NIS2 audit, it is supporting evidence at best. The terminology trail back to the foundation documents is in the IEC 62443-1-x foundations post .

Component-level certification. `IEC 62443-4-2` certification of individual devices (offered by labs accredited under the ISASecure or IECEE CB schemes) is voluntary in 62443. NIS2 does not require it. The forthcoming European Cybersecurity Certification Schemes under the Cybersecurity Act and the Cyber Resilience Act will pick this up — see the CRA applicability post for how `-4-2` overlaps with CRA Annex I — but as of May 2026, component certification remains a "nice to have, not a must".

Patch-information exchange format. `IEC TR 62443-2-3` defines a specific XML-based exchange format for patch metadata between OEM

and asset owner. NIS2 does not care what format you use, as long as vulnerability handling happens; the format itself is a 62443 nicety.

14. What NIS2 obligates that 62443 cannot help with at all

The honest "absent" column of the mapping. These are the obligations a 62443 audit pack will not touch, and where the asset owner has to build separate evidence from scratch:

Article 23 incident-reporting timelines. The 24-hour early warning, the 72-hour incident notification, the optional intermediate report on request and the one-month final report are pure NIS2 obligations. The Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 gives technical and methodological detail for the digital-infrastructure subset of entities (DNS providers, cloud, CDN, MSP/MSSP, marketplaces, search engines, social networks, trust service providers) — energy entities are **not** within its direct scope, but national supervisory authorities and ENISA's June 2025 Technical Implementation Guidance treat its Annex as the authoritative interpretive guide for Article 21 across all sectors. Read it; do not assume it does not apply to you in spirit even if it does not apply to you in law.

Article 24 European cybersecurity certification. NIS2 reserves the option for the Commission to require entities to use ICT products, services and processes certified under Regulation (EU) 2019/881 (the Cybersecurity Act) schemes — EUCC (the European Common Criteria-based scheme adopted in 2024) is the first, with EUCS (cloud services) and EU5G in development. IEC 62443 is not, as of May 2026, a European scheme; it remains a useful technical reference but does not by itself discharge any future Article 24 obligation.

Article 25 standardisation references. Article 25 names ENISA's role in promoting convergence on standards. It does not mandate IEC 62443 by number. Be cautious of vendor marketing claims that "we

are NIS2-compliant because we are 62443-compliant" — neither the directive nor any implementing act draws that equivalence.

Articles 32 and 33 supervisory regime and penalties. Penalty levels — up to EUR 10 million or 2% of total worldwide annual turnover for essential entities, up to EUR 7 million or 1.4% for important entities — and the supervisory toolkit (on-site inspections, ad-hoc audits, security scans, requests for information, binding instructions) are not anything IEC 62443 has a view on. The asset owner has to be ready to host an NSM inspection in the same way they would host a DSB or Petroleumstilsynet inspection on the safety side.

15. A practical evidence pack — what to hand to the audit

If you are heading toward your first NIS2-aligned audit and you already have an active IEC 62443 programme, the question becomes: what additional artefacts do I need to assemble? The table below is what I would put in front of the auditor. The left column is the NIS2 measure; the middle column is the 62443 evidence that already exists; the right column is the NIS2-specific delta.

NIS2 Article 21(2) measure	62443 evidence likely already in place	NIS2-specific evidence to add
(a) Risk analysis & ISMS policy	`-3-2` SuC zoning, SL-T derivations, risk register; `-2-1` ORG 2 records	Board-approved policy document; annual review minutes; residual-risk acceptance log
(b) Incident handling	`-3-3` FR 6 logging/monitoring evidence; `-2-1` IR SPE procedure	Named CSIRT contact; 24h/72h/1mo reporting playbook; tabletop test records covering reporting
(c) Business continuity	SR 7.3/7.4 backup & recovery test records; `-2-1` BCM SPE	Essential-service BCDR plan; RTO/RPO per process; crisis-management procedure with named roles
(d) Supply chain	`-2-4` integrator audits; `-4-1` ML certificates from OEMs; `-2-1` procurement SPE	Tiered supplier register; contractual incident-notification clauses; ENISA coordinated-risk-assessment awareness
(e) Acquisition, development, maintenance, vulnerability handling	`-4-1` DM/SUM evidence; `IEC TR 62443-2-3` patch records	CVD policy with public contact; advisory-monitoring subscription list; patch SLA
(f) Effectiveness assessment	`-2-1` internal-audit and management-review records; ML scores	KPIs reported to management body; corrective-action tracker visible to the board
(g) Hygiene & training	`-2-1` training SPE records; `-2-4` SP.02 records	Article 20(2) management-body training records; phishing simulation results (optional)
(h) Cryptography	`-3-3` FR 4 / `-4-2` CR 4.x design evidence	Algorithm catalogue policy; key-lifecycle procedure; documented non-applicability decisions
(i) HR, access, asset mgmt	`-3-3` FR 1/FR 2 evidence; CM SPE asset inventory	Periodic access recertification log; joiner/mover/leaver audit trail
(j) MFA & secured comms	SR 1.13 / CR 1.13 MFA enforcement evidence	Out-of-band emergency-comms procedure; documented MFA exception process

16. Summary table — single-page reference

NIS2 measure	Primary 62443 part(s)	Key SR / CR / clause	Fit	NIS2-specific evidence on top of 62443
(a) Risk analysis & policies	`-2-1:2024`, `-3-2:2020`	ORG 1, ORG 2; entire `-3-2` methodology	Tight	Board-approved policy; annual review; residual-risk acceptance
(b) Incident handling	`-2-1:2024`, `-3-3:2013`	SR 2.8–2.11, SR 6.1–6.2; IR SPE	Partial	CSIRT playbook; 24h/72h/1mo reporting procedure; test evidence
(c) Business continuity / DR	`-2-1:2024`, `-3-3:2013`	SR 7.1–7.6; BCM SPE	Tight (IACS scope)	Essential-service BCDR plan beyond IACS; RTO/RPO; crisis mgmt
(d) Supply chain	`-2-4:2023`, `-4-1:2018`, `-2-1:2024`	All of `-2-4`; `-4-1` SM, DM, SUM	Partial	Supplier risk register; contract clauses; ENISA CRA awareness
(e) Acquisition, dev, maintenance, vulnerability	`-4-1:2018`, `IEC TR 62443-2-3:2015`, `-3-3:2013`	`-4-1` DM, SUM; SR 3.4; `TR 2-3` exchange	Partial	CVD policy; advisory feeds; patch SLA
(f) Effectiveness assessment	`-2-1:2024`	Internal-audit & management-review SPEs; ML model	Tight	Board-visible KPIs; corrective actions
(g) Hygiene & training	`-2-1:2024`, `-2-4:2023`	Personnel-security SPE; SP.02	Tight (workforce); loose (board)	Article 20(2) management training records

NIS2 measure	Primary 62443 part(s)	Key SR / CR / clause	Fit	NIS2-specific evidence on top of 62443
(h) Cryptography	`-3-3:2013`, `-4-2:2019`	SR 3.1, 3.8, 4.1, 4.3; CR 4.x	Partial	Algorithm policy; key-lifecycle procedure
(i) HR, access, assets	`-2-1:2024`, `-3-3:2013`, `-4-2:2019`	FR 1, FR 2; CM SPE; personnel SPE	Tight	Periodic access recertification; J/M/L audit trail
(j) MFA & secured comms	`-3-3:2013`, `-4-2:2019`	SR 1.1 RE 1, SR 1.13; CR 1.13	Partial	Out-of-band emergency-comms procedure
Cross-cutting: Art 20 management body	none	n/a	**Absent**	Board approval & training records, board minutes
Cross-cutting: Art 23 reporting timelines	none	n/a	**Absent**	24h/72h/1mo playbook with named roles
Cross-cutting: Art 32/33 supervision	none	n/a	**Absent**	Audit-readiness procedure; document register

17. Reading list and cross-references

If you are following this series, the prerequisite reading is the IEC 62443 foundations post , which sets out the concepts and the parts; the management-system walkthrough , which goes deep on `-2-1:2024`; the system-design post on `-3-2` and `-3-3`; and the OEM-side post on `-4-1` and `-4-2`. On the regulatory side, NIS2 applicability is the scop-

ing companion to this post, and CRA applicability covers the product-side regulation that overlaps with `-4-1` / `-4-2`.

Primary regulatory sources used throughout: Directive (EU) 2022/2555 (NIS2) ; Commission Implementing Regulation (EU) 2024/2690 ; the ENISA Technical Implementation Guidance of June 2025. Norwegian transposition: `digitalsikkerhetsloven` LOV-2023-12-20-108 . Standards: IEC webstore for the 62443 series . Cross-reference: NIST SP 800-82 Rev. 3 "Guide to Operational Technology (OT) Security" — useful as a vendor-neutral second opinion on most of the technical mappings above.

18. FAQ

Does IEC 62443 satisfy NIS2? Not on its own. IEC 62443 is the strongest available technical answer to most of NIS2 Article 21's control obligations and will get you a long way through measures (a), (c), (e), (g), (h), (i) and (j) on the technical face. It does not satisfy the management-body responsibility in Article 20, the 24-hour/72-hour/one-month reporting timelines in Article 23, the European certification reference in Article 24, or the supervisory regime in Articles 32 and 33. Treat 62443 as the engineering substrate and NIS2 as the governance and reporting overlay.

What does NIS2 Article 21 require? Article 21(1) requires essential and important entities to take "appropriate and proportionate technical, operational and organisational measures" to manage cyber risk to their network and information systems. Article 21(2) lists ten minimum measures: risk-analysis policy, incident handling, business continuity, supply-chain security, acquisition/development/maintenance with vulnerability handling, effectiveness assessment, hygiene and training, cryptography, HR/access/asset management, and MFA/secured communications. Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 elaborates the technical and method-

ological requirements — directly binding for digital-infrastructure entities and used as the authoritative interpretive guide everywhere else.

How do NIS2 incident-reporting deadlines map to IEC 62443? They don't. IEC 62443 has no equivalent timing obligation. The 24-hour early warning, 72-hour incident notification and one-month final report under Article 23 are pure NIS2 — you build a separate playbook for them, naming the national CSIRT (NSM/NCSC in Norway), defining the significance thresholds, and rehearsing the end-to-end flow at least annually.

Is IEC 62443 mandatory under NIS2? No. Neither the directive nor any current implementing act names IEC 62443 as mandatory. Recital and Article 21(5) of NIS2 direct Member States and the Commission to encourage the use of "European and international standards", and IEC 62443 is the dominant such standard in OT — but compliance with it is voluntary. The forthcoming Cyber Resilience Act will create a stronger pull toward `-4-1` and `-4-2` for product suppliers placing devices on the EU market.

How does Commission Implementing Regulation (EU) 2024/2690 relate to IEC 62443? `(EU) 2024/2690` lays down technical and methodological requirements for the ten Article 21(2) measures, with a 13-section Annex that fleshes out each one. Its formal scope is digital-infrastructure and digital-provider entities (DNS, cloud, CDN, MSP/MSSP, marketplaces, search engines, social networks, trust service providers), so an energy operator is not legally bound by it directly. In practice, supervisory authorities and ENISA's June 2025 implementation guidance treat the Annex as the reference interpretation of Article 21 across all sectors. IEC 62443 controls map cleanly onto most Annex sections — risk management, asset management, access control, cryptography, network security, vulnerability handling — and ENISA's mapping spreadsheet acknowledges this. Where the

Annex goes beyond IEC 62443 (legal-entity governance, public CVD contact, supplier register against ENISA coordinated risk assessments), the asset owner adds the missing artefacts on top of the existing 62443 evidence.

What about Norway specifically — when does NIS2 actually bite for a Norwegian renewable operator? As of 14 May 2026, the answer is: not yet, but soon. The current Norwegian `digitalsikkerhetsloven` (LOV-2023-12-20-108) entered into force on 1 October 2025 and implements **NIS1**, not NIS2. NIS2 has not yet been incorporated into the EEA agreement and Norway is expected to transpose it during 2026, likely through a new combined cyber-and-CER law that will supersede the present digitalsikkerhetslov. The directive's substantive obligations are stable, however — Article 21 and Article 23 will not change between now and Norwegian entry into force. Building the evidence pack laid out above is the right preparation today, and most Norwegian renewable operators of any size will need it before the end of 2026.

If you found this useful, the rest of the series is linked above; if you spot a clause-reference error or a transposition update I have missed, ping me — corrections welcome.

IEC 62443 evidence pack: one-page version

15 May 2026 · 14 min read · #compliance #security #industrial #iec-62443

Picture a Stage-2 audit at a 120 MW solar park. Three minutes in, the auditor asks the quiet part out loud: "That's interesting — now show me the evidence." The programme manager opens a SharePoint folder labelled `62443_compliance`. Inside are eleven PDFs. Nine are vendor marketing brochures with the words "62443-ready" splashed across the top. One is a screenshot of a CSV. The eleventh is the signed contract with the EPC. The auditor closes the laptop, smiles politely, asks for a coffee, and writes seventeen non-conformities into the follow-up letter.

This post exists so that does not happen to you.

TL;DR

If you cannot produce a specific document on demand, you are not actually `IEC 62443` compliant — regardless of what your supplier's glossy says. This is the **one-page evidence pack**: a tight, opinionated checklist of the artefacts an auditor will ask for under each of the four numbered groups of the standard (`IEC 62443-2-x`, `-3-x`, `-4-x`), plus a small set of cross-cutting items. Pick the pack that matches your role, print it, and walk into your next project with it in hand. The five-question pre-audit self-test at the end is the most useful 100 words in this post.

Who this is for

The `ISA/IEC 62443` series defines four principal roles — asset owner, integrator, service provider, and product supplier — and every artefact below maps to one of them. If you have not already read the IEC 62443-1-x foundations post , start there: the role definitions and the

Industrial Automation and Control System (IACS) lifecycle model in `IEC TS 62443-1-1:2009` are the scaffolding everything else hangs from.

- **Asset owners** (the operators — utilities, generators, plant owners): your pack is `-2-1` + `-3-2`.
- **Integrators and service providers** (EPCs, system integrators, maintenance contractors): your pack is `-2-4`.
- **Product suppliers** (PLC, RTU, gateway, HMI, inverter, BMS vendors): your pack is `-4-1` + `-4-2`.
- **Everyone** owes the cross-cutting artefacts in section 5.

A deeper walkthrough of each lives in the `-2-x` management-system post , the `-3-2` and `-3-3` post , and the `-4-1` and `-4-2` post . This one is the cheat sheet.

1. The hierarchy of 62443 evidence

Auditors — the good ones, anyway — think in three tiers. You should too.

- **Tier 1: policy and procedure documents.** What you intend to do. Security programme charter, risk-assessment procedure, change-management policy. Cheapest to produce, easiest to fake, weakest as evidence.
- **Tier 2: records and operational evidence.** What you actually did. Signed minutes, training attendance lists, ticket exports, test reports, patch logs, audit findings with closure dates. This is where audits are won or lost.
- **Tier 3: independent certifications.** What an accredited third party verified. ISASecure CSA / SSA / SDLA certificates, IECEE CB Scheme test reports, or accredited-body audits against `IEC 62443-2-4` for service providers. Most expensive, hardest to argue with.

A mature programme has all three. A defensible programme has at least Tiers 1 and 2 across the board, with Tier 3 sitting under the highest-risk components. A "marketing PDF" programme has none of the above and several brochures.

For product-side Tier 3 in particular, ISASecure operates the three product/process schemes most often cited in tenders — `CSA` to `IEC 62443-4-2`, `SSA` to `IEC 62443-3-3`, and `SDLA` to `IEC 62443-4-1` — all under `ISO/IEC 17065` . The IECEE CB Scheme provides the parallel international conformity-assessment route through `IEC 62443` and is the one most European buyers will recognise.

2. Asset-owner evidence pack — for `IEC 62443-2-1:2024` and `IEC 62443-3-2:2020`

The 2024 edition of `IEC 62443-2-1` replaced the old Cyber Security Management System (CSMS) language with eight **Security Programme Elements** (SPEs) and added a maturity model. Risk methodology still lives in `IEC 62443-3-2:2020` , which defines the System under Consideration (SuC), the zone and conduit drawing, and the Target Security Level (SL-T) derivation.

Group your evidence by SPE. If an auditor cannot find any of the following on demand, expect a finding.

#	Artefact	What the auditor will sample	Red flag
1	Security programme charter / policy document	Approval signature, scope statement, applicable IACS sites	More than 24 months old with no revision history
2	Board / management-body approval minutes	Date of approval, named accountable executive	Approver is the same person who wrote it
3	Risk assessment per `IEC 62443-3-2` for each SuC	SuC definition, threat catalogue, consequence rating	A single global risk assessment used for unrelated plants
4	Zone and conduit diagram per SuC	Versioned drawing, asset-to-zone allocation	No conduit list, or conduits drawn but not enumerated
5	SL-T vector derivation per zone	Per-Foundational-Requirement (FR) vector — seven values, not one	A single "SL 2" or "SL 3" claim with no FR breakdown
6	Risk register with residual-risk acceptance	Owner, treatment, residual rating, sign-off	Residual risks accepted by the same engineer who rated them
7	Asset inventory baseline (SPE 2 — `CM 1.1`)	Hardware, firmware versions, software, network ports	Firmware versions that do not match what's running in the field
8	Configuration management baselines	Golden image, baseline diff procedure	Baselines that pre-date the last firmware update
9	Internal audit reports	Scope, findings, corrective actions, closure dates	No internal audit in the last 12 months
10	Management review minutes	Inputs reviewed, decisions taken, actions assigned	A meeting with no decisions recorded
11	Training records (SPE 1)	Role-based training matrix, completion dates per person	Generic "cyber awareness" certificates with no OT content
12	Supplier register (with `-2-4` assessment status)	Last assessment date, scope, gaps	Suppliers listed with no assessment date
13	Incident response procedure + exercise records	Tabletop minutes, real-incident post-mortems	Procedure exists, but no exercise in the last 18 months
14	Business continuity and disaster recovery (BCDR) plan + restore test evidence	Last successful restore test, RTO/RPO achieved	"Backup runs nightly" with no restore test on record

#	Artefact	What the auditor will sample	Red flag
15	Exception / deviation register	Each exception linked to a compensating control and an expiry date	Open-ended exceptions with no review date

Most of the artefact map above sits inside SPEs 1 through 8 — organisational security, configuration management, network and communication protection, component protection, data protection, user access control, event-and-incident management, and system integrity and availability. The ISA Global Cybersecurity Alliance (ISAGCA) Quick Start Guide is the cleanest free reference to the SPE structure if you do not have the IEC text in front of you.

3. Integrator and service-provider evidence pack — for `IEC 62443-2-4:2023`

`IEC 62443-2-4:2023` — Edition 2.0, published December 2023 — defines the security capabilities a service provider offers an asset owner during integration and maintenance, organised into Security Programme (SP) topics `SP.01` through `SP.12` (staffing, assurance, architecture, wireless, configuration management, hardening, malware protection, patch management, backup/restore, monitoring, event management, account management, remote access). The 2023 revision converted many former "capabilities" into required **processes** with documented outputs — meaning evidence is now non-negotiable.

#	Artefact	Maps to	Red flag
1	Staffing and competence records	`SP.01`	Personnel listed with no OT-specific training
2	Scope-of-services document per contract	`SP.02`	A boilerplate scope reused across unrelated contracts
3	Secure architecture handover package	`SP.03`	No zone/conduit overlay agreed with the asset owner
4	Wireless configuration records	`SP.04`	Wireless used but no rogue-device detection process
5	Hardening baselines applied per device class	`SP.06`	Baselines from a previous firmware generation
6	Malware-protection deployment evidence	`SP.07`	AV signatures last updated months before commissioning
7	Patch-management records	`SP.08`	Patches approved by the asset owner but never deployed
8	Backup and restore test evidence	`SP.09`	Backups exist, restore never tested on the target hardware
9	Remote-access procedure + session logs	`SP.11`	Jump-host logs that do not record commands or session video
10	Change-management records	Cross-cutting	Changes implemented before approval signatures

`SP.05` (assurance) and `SP.12` (event management) sit underneath the above as cross-cutting controls and should be picked up by the cross-cutting pack in section 5.

4. Product-supplier evidence pack — for `IEC 62443-4-1:2018` and `IEC 62443-4-2:2019`

`IEC 62443-4-1:2018` defines a Secure Development Lifecycle (SDL) built around **eight practices**: Security Management (`SM`), Specification of Security Requirements (`SR`), Secure by Design (`SD`), Secure Implementation (`SI`), Security Verification and Validation Testing (`SVV`), Management of Security-related Issues (`DM`), Security Update Management (`SUM`), and Security Guidelines (`SG`). `IEC 62443-4-2:2019` then defines the technical Component Requirements (CRs) per Foundational Requirement, with capability Security Levels `SL-C 1` to `SL-C 4`.

#	Artefact	Maps to	Red flag
1	SDL policy and training records	`SM-1` … `SM-13`	A policy that exists but no developer has been trained against it
2	Threat model per product	`SR-2`	Threat model written once at launch, never refreshed
3	Security requirements traceability matrix	`SR-1` … `SR-5`	Requirements with no test case mapped
4	Secure-coding evidence (SAST, DAST)	`SI-1`, `SI-2`	Scan reports with critical findings marked "accepted" without rationale
5	Security testing report (functional, fuzz, pen test)	`SVV-1` … `SVV-5`	No evidence of tester independence
6	Vulnerability handling procedure with coordinated-disclosure (CVD) contact	`DM-1` … `DM-6`	No `security@` mailbox, no PSIRT, no published policy
7	Software Bill of Materials (SBOM) — CycloneDX or SPDX	`SM-9`, `DM-1`	An SBOM with no version, no hashes, no update channel
8	Security guidelines / hardening guide for asset owners	`SG-1` … `SG-7`	A "user manual" with one paragraph on security
9	Security-update channel evidence	`SUM-1` … `SUM-5`	Patches released but no documented delivery channel
10	Support end-of-life (EOL) policy	`SUM-5`, `SG-7`	EOL dates that move quietly when convenient

For `IEC 62443-4-2:2019`, add a per-FR test evidence pack mapping each CR claim to a result, summarised by an accredited certification body's report. A clean way to do this is to attach the ISASecure CSA certificate plus the underlying Functional Security Assessment (FSA-C) and Vulnerability Identification Testing (VIT-C) reports, or the equivalent under the IECEE CB Scheme . For development-process certification only — without a product certificate — `ISASecure SDLA` or an IECEE `IEC 62443-4-1` assessment is the equivalent. Note that the `SDLA` scheme allows a supplier to scope out individual sub-practices, so always read the certificate's scope statement, not just the logo.

5. Cross-cutting artefacts

These are the ones programmes routinely forget — and they are the ones auditors enjoy asking for, because they reveal whether the programme is actually run or merely written down.

1. **Risk acceptance log signed by the management body.** Not a project manager. Not a "responsible engineer". The accountable executive named in the SPE 1 charter, with a date and a residual-risk value.
2. **Compensating-countermeasure register.** Where a control could not be implemented natively, the compensating measure is named, its rationale documented per the `IEC TS 62443-1-1:2009` definition, and its effectiveness reviewed on a stated cadence. `IEC 62443-2-1:2024` explicitly allows compensating controls for legacy systems — but only if they are documented.
3. **Exception / deviation register.** Every deviation from a policy or baseline, with an owner, an expiry, and a compensating control.
4. **SL-T → SL-C → SL-A traceability matrix per zone.** The asset owner derives SL-T per `-3-2`. The product supplier publishes SL-C per `-4-2`. The integrator delivers SL-A (achieved) in the as-built configuration. Auditors love this matrix because gaps fall out of it visually.
5. **Evidence-pack version-control log.** The evidence itself needs version control. If the audit folder is "live SharePoint" with no revision history, your evidence has no integrity.
6. **Time-synchronisation evidence.** Often missed. `IEC 62443-3-3:2013` SR 2.11 (Timestamps) requires components to provide reliable, synchronised timestamps for audit records. If your PLC, jump host, and SIEM clocks drift, your audit trail is not legally usable. NIST SP 800-82 Rev. 3 makes the same point in OT terms.

6. What does NOT count as evidence

A short, opinionated red-flags list. None of the following will survive an audit on its own:

- **Marketing PDFs that say "62443 compliant" without a part number.** `IEC 62443` is a series, not a single standard. "Compliant" with which of the thirteen-plus documents? At what edition year? Against which SL? Without those, the claim is decorative.
- **Single-number SL claims.** "We're SL 3" is meaningless. `IEC 62443-3-3` and `-4-2` express security levels as a seven-element vector — one per FR (Identification & Authentication Control, Use Control, System Integrity, Data Confidentiality, Restricted Data Flow, Timely Response to Events, Resource Availability). A vector like `SL-C (3,2,3,1,3,2,3)` is the proper form.
- **Vendor certificates without a scope statement.** The `ISASecure SDLA` certificate, for example, only tells you the process was assessed for the sub-practices in scope — which can legitimately be a subset. Always read the scope annex.
- **Compliance matrices that are not signed, dated, or version-controlled.** A Word document that has been edited by six people with track-changes off is not evidence; it is a rumour.
- **Test reports from before the most recent major firmware update.** A penetration-test report against firmware v4.2 does not certify v4.7. The supplier owes a delta assessment or a re-test.

7. The five-question pre-audit self-test

The most useful 100 words in this post. Run this five-question test before the auditor crosses your threshold. If you cannot answer "yes, here it is" to all five, fix that first.

1. Can you produce the **SL-T vector** for every zone, derived per `IEC 62443-3-2`, signed within the last 24 months?

2. Can you produce a **complete asset inventory** whose firmware versions match what is actually deployed at the plant today?
3. Can you produce an **internal-audit finding** from the last 12 months that resulted in a corrective action that is now formally closed?
4. Can you produce evidence that a **maintenance service provider** has been assessed against `IEC 62443-2-4` in the last contract cycle?
5. Can you produce the **residual-risk acceptance log**, signed by the relevant management-body member, dated and current?

Five "yes" answers is not compliance — but five "no" answers is definitely non-compliance.

8. How to use this as a project tool

Three concrete uses, in order of how often each typically surfaces:

- **On a new project.** Pick the pack that matches the role you are playing — owner, integrator, or supplier — and use it as a deliverables list in your project plan. Each row becomes a work-package output.
- **On an audit.** Produce the right pack and check the age of each artefact. Anything older than 12 months is a question waiting to be asked; anything older than 24 months is a finding waiting to be written.
- **On procurement.** Hand the supplier a tailored version of the product-supplier pack as a tender annex. "Submit each of items 1–10 with your bid, or the bid is non-responsive." This single tactic raises the floor of supplier responses faster than any contractual clause.

The same logic underpins the NIS2 mapping post — where the NIS2 Directive (EU) 2022/2555 requires "appropriate and proportionate technical, operational and organisational measures", these are the

artefacts that demonstrate them. And for products placed on the EU market after December 2027, the Cyber Resilience Act applicability post walks through where the product-supplier pack here doubles as a CRA conformity dossier.

FAQ

What's the difference between a `-4-1` certificate and a `-4-2` certificate? `-4-1` certifies the process — the supplier has a documented, audited Secure Development Lifecycle. `-4-2` certifies the product — a specific component, at a specific firmware version, meets the technical Component Requirements at a stated capability Security Level. You need both; a supplier with `-4-2` only has a tested product but no guarantee the next release will be developed the same way. A supplier with `-4-1` only has a clean process but no certified product on the shelf.

How long should I retain evidence for? Match the longer of: the IACS lifetime (typically 15–25 years for a renewables plant), the regulator's retention period (under NIS2 transposition this often lands at six years post-incident), and the group records-retention policy. Timestamped audit logs from `SR 2.11`-relevant systems should be retained at least three years on warm storage, longer on cold storage. Never delete an artefact while an open finding references it.

Do I need `ISASecure` or `IECEE CB` to comply with `-4-1`? No. `IEC 62443-4-1` compliance can be self-declared, second-party assessed (by a customer), or third-party certified. Self-declared evidence is acceptable to many auditors if it is tier-2-grade: SBOMs, test reports, traceability matrices, training records. Third-party certification via ISASecure SDLA or an IECEE CB Scheme `IEC 62443-4-1` assessment simply shortcuts the conversation. For products sold into critical-infrastructure tenders in Europe, third-party is increasingly the de facto requirement.

Where does NIS2 evidence sit in this pack? NIS2 evidence is a superset that consumes the 62443 pack, not a replacement. The NIS2 applicability post covers who's in scope; the NIS2 mapping shows which 62443 artefacts satisfy which Article 21 measures. Practically: an asset owner's `-2-1` pack covers most of NIS2 Article 21(2)(a)–(j); the integrator's `-2-4` pack covers (d) supply-chain security; the product-supplier's `-4-1`/`-4-2` pack underpins the rest. Add NIS2-specific items — the 24-hour early-warning template, the competent-authority registration record, and the management-body cyber training attestation — and you have a NIS2-defensible position built on a 62443 foundation.

If this checklist saved you one finding, the post has paid for itself. To argue with item 6 in any of the tables, LinkedIn is the way to find me.