



IEC 62443 for Industrial Automation

Engineering secure products and control systems

A practical reference for automation manufacturers, machine builders and system integrators

Understand the risks. Allocate the requirements. Demonstrate the protection throughout the lifecycle.

EXECUTIVE OVERVIEW

Security across the industrial lifecycle

IEC 62443 gives customers and suppliers a common basis for deciding what to protect, how to engineer it and how to sustain it in service.

Industrial cybersecurity reaches beyond the network. A change to controller logic can alter a physical process; an unavailable engineering workstation can delay restoration; a compromised support service can expose many installed machines. The engineering objective is to preserve the functions on which safe, reliable operation depends.

The IEC 62443 series connects those operational needs with organisational practices, system design and product capabilities. It treats an industrial automation and control system (IACS) as a combination of people, procedures and technology. A secure product is an important contribution, but its installation, maintenance and use determine how that contribution works in the plant. [1–7]

For an automation supplier, the first decision is scope. Developing a controller, integrating a production line and maintaining equipment are different activities with different obligations. One company may perform all three. Each role needs explicit requirements, accountable owners and evidence tied to the delivered version and configuration.

This paper explains the framework and applies it to a fictional packaging line. The example follows a remote-maintenance risk through zoning, requirements, product development, verification and handover. Its design choices are PRAETORIO recommendations for discussion, not a prescribed architecture or a claim of certification.

Reading guide

Topic	Pages	What it helps you decide
Industrial consequences and the standards map	2–4	Which risks and standard parts matter to your delivery
Responsibilities and system design	5–9	How to allocate protection and interpret security levels
Product and operational lifecycles	10–12	What to build, document and maintain
Evidence and implementation	13–15	How to demonstrate progress and define a credible scope
Technical sources	16	Where to verify editions and supporting information

Technical basis. Standard requirements are paraphrased and identified by part or requirement reference. Examples, suggested artefacts and the implementation roadmap are

PRAETORIO guidance. This publication is an engineering overview, not a substitute for the applicable standards or a complete conformance assessment.

01 INDUSTRIAL CONSEQUENCES

What industrial attacks reveal

Three documented incidents show why control integrity, operational dependencies and recovery deserve separate attention.

TRITON and the safety engineering path

In 2017, Mandiant investigated malware designed to interact with industrial safety controllers. Attackers had reached a safety engineering workstation and attempted to modify controller

behaviour. Some controllers entered a failed-safe state, shutting down the industrial process and triggering investigation. The account describes operational disruption; it does not report injuries or an explosion. [10]

The engineering lesson is that a safety system also has a cybersecurity boundary. Protection of its engineering tools, programming interfaces and maintenance access must be considered alongside the safety function itself. A function designed to respond to a hazardous process condition can still depend on software and configuration that an attacker may try to change.

IEC 62443-3-2 provides a basis for treating safety-related assets explicitly in the zone model. Part 3-3 addresses access, authorisation, integrity and boundary protection. The resulting design still needs review with the functional-safety team; cybersecurity controls must not obstruct essential protective functions. [4,5]

Hydro and operational dependencies

On 19 March 2019, Hydro reported that a cyberattack affected operations across several business areas and that IT systems were affected in most areas. The company was switching to manual operations where possible. That announcement establishes industrial disruption, without establishing that attackers manipulated controller logic. [11]

The practical question is how production behaves when supporting services disappear. A machine may retain local control while losing scheduling, identity services, recipes or access to the engineering files needed for restoration. These dependencies belong in the system boundary and the recovery plan.

IEC 62443 supports identifying essential functions, specifying backup and recovery capabilities, and assigning operational responsibilities. A supplier can contribute verified restoration procedures and configuration records; the asset owner must make them usable in the actual facility. [2,4,5]

Industroyer2 and legitimate protocols

ESET, working with CERT-UA, analysed a 2022 attempt to disrupt a Ukrainian energy provider's high-voltage substations. Industroyer2 used IEC 60870-5-104 communications, alongside destructive malware affecting other systems. The report describes an attempted attack and leaves the initial entry route unresolved; it does not establish a resulting blackout. [12]

The lesson is to examine who can issue a control command, even when the communication protocol itself is permitted. A trusted engineering host may become the attack source. Network boundaries, endpoint protection, command authorisation and monitoring therefore need to work together.

The IEC 62443 response is to assess the threat scenario, restrict the permitted paths and actions, and verify the resulting protection. Segmentation alone cannot establish whether every permitted command is legitimate.

These mappings are engineering interpretations. They do not establish the victims' conformance status or prove that certification would have prevented an incident.

02 STANDARDS MAP

Choose the parts that match your work

IEC 62443 is a family of complementary publications. Its numbering separates general concepts, organisational processes, system requirements and product requirements.

The series is often called ISA/IEC 62443, reflecting its development within the ISA and IEC standards community. For a supplier, the useful starting point is the object being engineered or assessed.

Process conformance, component capability and the security of an installed automation solution answer different questions. [1,3–7]

Publication baseline	Primary purpose	Typical engineering output
IEC TS 62443-1-1:2009	Common terminology, concepts and models	Shared vocabulary and system context
IEC 62443-2-1:2024	Asset-owner security programme for operational IACS	Policies, responsibilities and operating practices
IEC 62443-2-4:2023	Service-provider security processes for integration and maintenance	Defined services and evidence of their execution
IEC 62443-3-2:2020	Security risk assessment for system design	System boundary, zones, conduits, SL-T and requirements
IEC 62443-3-3:2013	System security requirements and capability levels	System requirements allocation and verification basis
IEC 62443-4-1:2018	Secure product development lifecycle	Repeatable development and maintenance evidence
IEC 62443-4-2:2019	Component technical security requirements	Applicable component requirements and capability evidence
IEC TR 62443-2-3:2015	Patch-management guidance in the IACS environment	Supplier and owner patch-evaluation workflow

This is a working selection, not a complete catalogue. Technical Specifications (TS), Technical Reports (TR) and Publicly Available Specifications (PAS) have distinct publication types; they should not be presented as interchangeable certification requirements. For example, IEC PAS 62443-2-2:2025 provides guidance on security protection schemes across design, validation, operation and maintenance. [8,9]

Record the agreed editions, corrigenda, contractual additions and assessment-scheme rules in the project baseline. This paper uses the 2024 asset-owner edition; the older 2010 structure should not be labelled as the current edition. The IEC listings include corrigenda for parts 3-3 and 4-2. [2,5,7]

03 SHARED RESPONSIBILITY

Connect the product to the operating plant

Requirements move towards the supplier. Evidence, limitations and deployment conditions return to the parties responsible for integration and acceptance.

A component is an identifiable product such as a controller, network device or software application. A control system combines components. An automation solution is the configured implementation for a particular application, including the complementary measures it needs. The operational IACS also includes the people and work processes that sustain it. [1,3,6,7]

Consider a machine builder supplying a packaging line with purchased programmable logic controllers (PLCs), a human-machine interface (HMI), its own gateway software and a remote-maintenance service. The builder integrates a solution, develops a product and supplies services. The customer operates the line and decides whether the residual risk is acceptable.

The customer provides operating constraints and risk-acceptance criteria. The integrator translates these into a system design and allocates security requirements. Product suppliers return supported capabilities and installation conditions. Service providers define how access, changes, patches and support will be managed. Outsourcing an activity does not remove the asset owner's responsibility for its security programme. [2–7]

Make the interfaces contractual

Agree who approves a remote session, administers identities, evaluates vulnerabilities, tests updates, retains backups and authorises restoration. Specify the information exchanged and the response expected. Product manuals and certificates cannot resolve an unassigned operating duty. The same responsibility record should be reviewed at design approval, handover and material change.

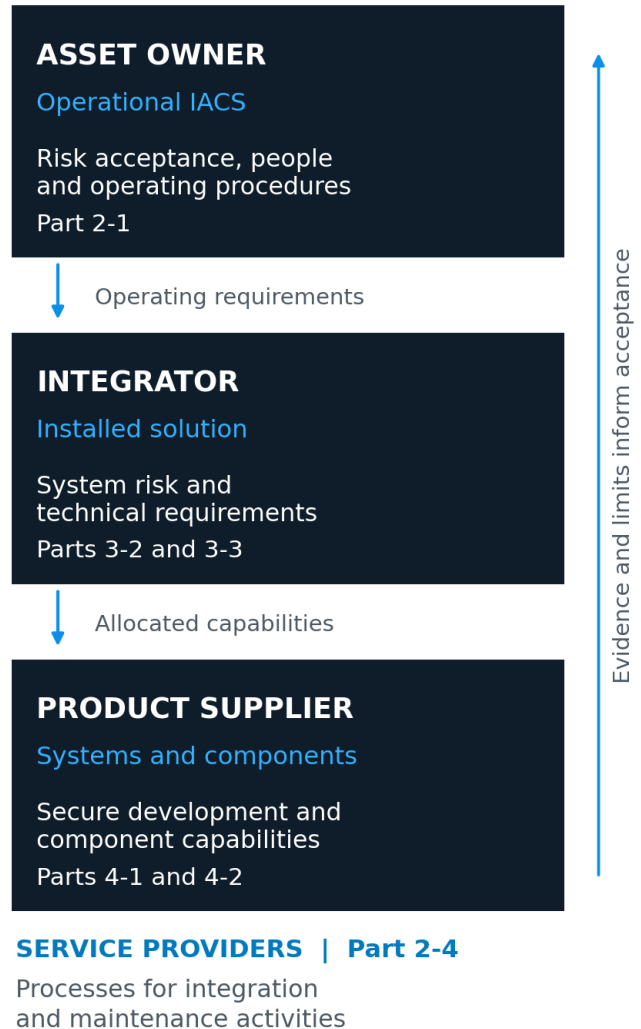


Figure 1. Original responsibility model. The standards apply to activities and objects; a company may occupy more than one role.

04 SYSTEM RISK ASSESSMENT

Turn process consequences into requirements

IEC 62443-3-2 links the system under consideration, tolerable risk, zones and conduits, target security levels and a documented requirements basis. [4]



Figure 2. Simplified engineering interpretation of the part 3-2 workflow. Risk assessment and zoning are iterative; this is not a reproduction of the normative process.

Define the system under consideration (SUC) before assessing it. Include the equipment or process being controlled, the automation assets and every relevant access point. Remote services, temporary engineering devices and external dependencies deserve explicit treatment, even where they sit outside the supplier's delivery boundary.

The initial assessment identifies severe consequences and supports prioritisation and zoning. Where initial risk exceeds the organisation's tolerable risk, detailed assessment examines threats, vulnerabilities, consequences and likelihood for the relevant zones and conduits. Existing countermeasures are then evaluated, residual risk is reconsidered and additional treatment is selected as necessary. Avoid assigning a target security level directly from a vulnerability severity score.

For the packaging line, a credible scenario is misuse of a maintenance identity to alter a production recipe or control programme. Consequences depend on the process: rejected product, equipment damage and safety-related effects must be examined separately. The risk assessment determines the required protection; the example alone does not justify a particular level.

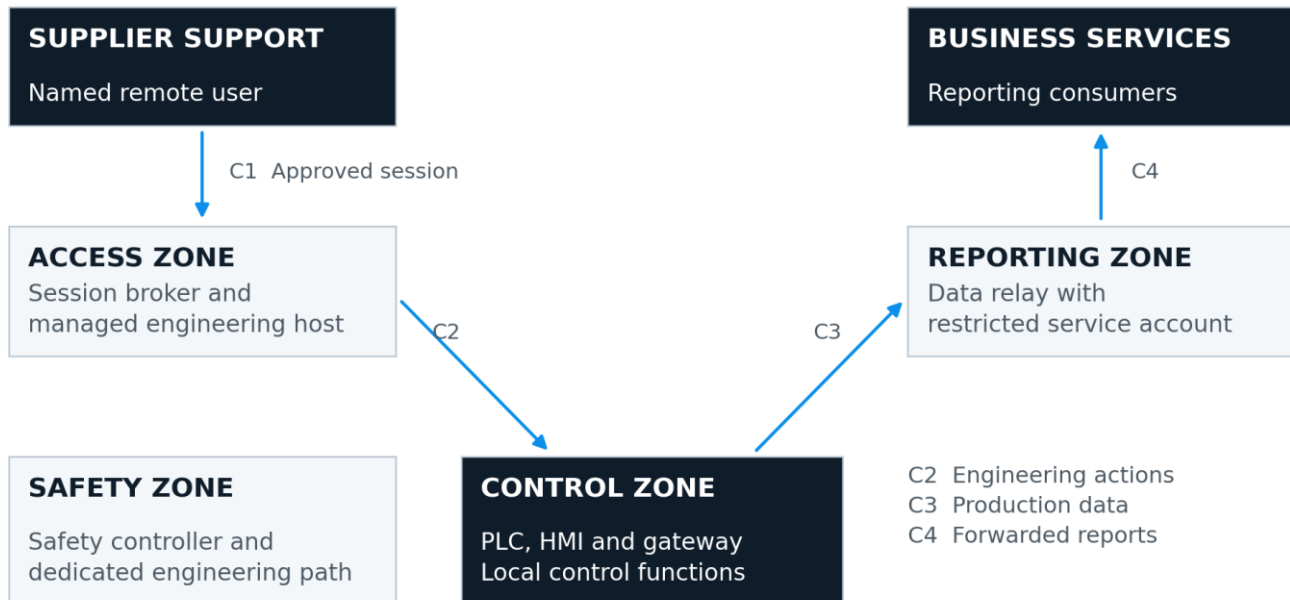
Create an actionable requirements basis

The cybersecurity requirements specification (CRS) captures the SUC, zone and conduit drawings and characteristics, access points, data flows, SL-T, applicable requirements, operating assumptions, threat context, tolerable risk and relevant policy or regulatory constraints. It may be a controlled set of linked records. Part 3-2 also requires approval of the assessment results by accountable asset-owner management; a consultant's analysis does not itself constitute risk acceptance. [4, ZCR 6 and ZCR 7]

05 SECURITY ARCHITECTURE

Design boundaries around operating needs

A zone groups assets with common security requirements. A conduit groups the communication channels between zones and the requirements protecting those channels.



Safety engineering is separately authorised; no remote programming route is shown.

Figure 3. Illustrative packaging-line architecture. Arrows indicate intended service or data direction, not one-way hardware enforcement. Protocols, return traffic and boundary devices require detailed design. PLC: programmable logic controller; HMI: human-machine interface.

In this example, remote access terminates in a managed access zone; it does not provide unrestricted connectivity to the control network. The engineering conduit permits only approved maintenance actions. Reporting uses a separate service path and identity. Safety engineering is treated separately rather than inheriting the general remote-maintenance permissions.

For each conduit, record source and destination, permitted services, identities, direction, operational purpose, monitoring and behaviour on failure. A VLAN can support separation but does not, by itself, prove enforcement of the required boundary.

Zones need not align with a Purdue level, a building or a supplier's equipment list. Their security rationale comes from the assessed functions and risks. [4,5]

Defence in depth adds independent barriers and detection, while least privilege and least functionality reduce what a compromised asset can do. Check for shared credentials, shared administration or a common engineering host that could defeat several layers at once. Validate loss of external connectivity without obstructing local control or essential safety functions. [5]

06 TECHNICAL PROTECTION

Apply the seven foundational requirements

Parts 3-3 and 4-2 organise system and component requirements around the same seven foundational requirements. They provide a structured way to test whether the design covers more than perimeter security. [5,7]

Foundational requirement	Question for the packaging line	Illustrative evidence
FR 1 Identification and authentication control	Can the system establish who or what is connecting?	Identity configuration; tests of valid, invalid and revoked access
FR 2 Use control	What may an authenticated user or process do?	Role-permission matrix; denied-action tests; event records
FR 3 System integrity	Can unauthorised changes or malformed inputs undermine control?	Integrity checks; input-validation and tampering tests
FR 4 Data confidentiality	Which information needs protection from disclosure?	Data classification; protected secrets and communication tests
FR 5 Restricted data flow	Are only the required paths available across boundaries?	Conduit rules; prohibited-path tests; boundary configuration
FR 6 Timely response to events	Can relevant events be detected and acted upon?	Accessible audit records; monitoring and escalation exercise
FR 7 Resource availability	Can required functions be sustained and restored?	Load and failure tests; verified backup and restoration results

The table offers review questions and example evidence, not a complete compliance checklist. Within each foundational requirement, the applicable system requirements (SRs), component requirements (CRs) and requirement enhancements (REs) must be selected using the relevant standard, security level and context. A single control can support several objectives, but that does not eliminate the need to verify each applicable requirement.

Keep identification separate from authorisation. A valid maintenance account should not automatically permit a control-programme download. Similarly, an encrypted connection protects information in transit but does not establish that its destination is permitted to alter the process. The architecture, permissions and verification plan must address these relationships.

Requirement enhancements add specific capabilities. For example, part 3-3 SR 5.2 addresses zone-boundary protection, while its first enhancement adds a default-deny approach with explicitly permitted exceptions. Check the relevant level mapping; a recommendation in an example must not be mistaken for a universally applicable base requirement.

Protect essential functions

Part 3-3 places constraints on security measures so that they do not undermine essential functions. Examine account lockout, authentication-service failure, loss of logging, network congestion and boundary isolation with the control and safety engineers. A generic IT setting can have unacceptable consequences in an operational system. Record and test the required degraded behaviour. [5, Clause 4]

07 LEVELS AND MATURITY

Specify the protection being claimed

A security level is meaningful only with its scope, requirement basis and operating assumptions. It is not a universal score for a company or a plant.

Target capability and achieved protection

SL-T is the target selected through risk assessment for a zone or conduit. It describes the protection sought and informs the requirements baseline. It is not established by purchasing a product with a matching label. [4]

SL-C describes the native capability of a system or component when correctly configured, for the applicable technical requirements. Part 3-3 addresses system capability; part 4-2 addresses component capability. Read the scope and deployment conditions of any supporting assessment. [5,7]

SL-A concerns the protection actually achieved in the implemented setting. It depends on integration, configuration and sustained operating measures. Do not claim an achieved level by averaging component ratings or assuming that the lowest component rating completely characterises the installation. Evaluate the relevant requirements and evidence for the actual scope.

Levels describe increasing resistance

In simplified terms, level 1 addresses casual or coincidental violations. Level 2 addresses intentional violations using simple means, low resources, generic skills and low motivation. Level 3 adds sophisticated means and IACS-specific skills with moderate resources and motivation. Level 4 addresses sophisticated means with extended resources, IACS-specific skills and high motivation. Level 0 expresses no specific requirement for that aspect. [5,7]

These are protection categories, not predictions of attack frequency, a guarantee against a named actor, or an instruction to select level 4 everywhere.

Use the vector where it matters

The seven foundational requirements need not have identical target levels. A vector records them separately in the order IAC, UC, SI, DC, RDF, TRE and RA. For example, SL-T = (2, 2, 3, 1, 3, 2, 3) would indicate different targets for integrity, confidentiality and availability.

That vector is illustrative only. It is not a recommended target for packaging machinery. The actual choice must follow the assessed risks and be translated into applicable requirements and enhancements. A higher number for one foundational requirement does not compensate for a missing requirement in another. [4,5]

Process maturity answers another question

A maturity assessment examines how consistently an organisation defines, performs and improves its security processes. The models used in parts 4-1 and 2-4 distinguish initial, managed, defined or practised, and improving processes. Their detailed assessment rules need to be read in the relevant part and scheme. [3,6]

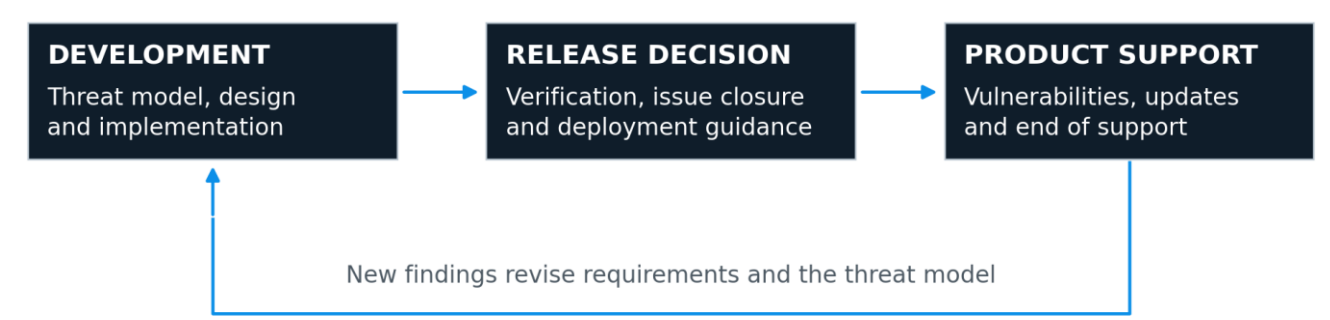
For a product supplier, a written vulnerability-handling procedure is different evidence from a completed case showing assessment, remediation and customer communication. Metrics and corrective actions demonstrate a further ability to improve the process.

A mature development process does not imply that every product has the same technical capability. Conversely, a product that passes a set of tests does not establish a repeatable development organisation. Keep process maturity and technical security-level statements separate in proposals, evidence reports and marketing.

08 SECURE PRODUCT DEVELOPMENT

Build a lifecycle that produces evidence

IEC 62443-4-1 covers how products are developed and maintained. Its eight practices connect management, engineering, verification and support. [6]



Security management governs all activities and their evidence throughout the lifecycle.

Figure 4. Original product-lifecycle view. Security findings and changes feed back into engineering after release.

Practice	What it should make visible in a product project
Security management	Accountable roles, competence, protected development environment and release governance
Security requirements	Intended environment, threat model, capabilities and acceptance criteria
Secure design	Trust boundaries, defence in depth and design review decisions
Secure implementation	Implementation rules, review findings and treatment of vulnerable code
Security verification and validation	Requirements, threat-mitigation, vulnerability and penetration-testing evidence
Security-related issue management	Received findings, affected releases, assessment, treatment and disclosure
Security update management	Qualified updates, delivery protection and clear deployment information
Security guidelines	Hardening, secure operation, external measures and disposal guidance

For the gateway, the threat model should include the web interface, update path, field protocols, service credentials and trust placed in external software. It should evolve when interfaces or deployment assumptions change. A list of known vulnerabilities cannot replace analysis of abuse of intended functions. [6, SR-2]

Manage third-party dependencies and signing keys as engineering assets. Keep a component inventory

linked to released versions so that new findings can be assessed. A software bill of materials is a useful implementation artefact; its presence alone does not prove that dependency risks have been evaluated. Release decisions need evidence that applicable activities are complete and security issues are addressed under the defined process. [6, SM-7 to SM-12]

09 COMPONENT CAPABILITIES

Translate requirements into product behaviour

IEC 62443-4-2 distinguishes software applications, embedded devices, host devices and network devices. The component category and claimed capability determine which requirements must be evaluated. [7]

A PLC is typically considered as an embedded device; an industrial firewall as a network device; and an engineering application as software. Classification must follow the actual functions and definitions. A product spanning more than one category may need more than one set of requirements. Start with all exposed interfaces, including local service ports and recovery functions, rather than evaluating only the normal network interface.

For the packaging-line gateway, the product specification should state which identities can connect, which operations each identity can perform, how configuration and updates are protected, what events are recorded and how the device behaves under resource pressure. The following examples show how to make those statements testable. They are project-specific guidance, not substituted normative text.

Product decision	Engineering example	Verification example
Administrative access	Separate status viewing from configuration and service administration.	Attempt configuration changes with the viewing role and verify rejection.
Software integrity	Define trusted update sources and integrity or authenticity checks for the applicable requirement.	Provide an altered or untrusted update and verify the specified rejection and recovery behaviour.
Audit information	Record security-relevant actions with enough context for investigation.	Exercise access and configuration actions; inspect event content, time handling and storage limits.
Resource availability	Specify behaviour during excessive requests and loss of external services.	Test the defined resource limits and confirm essential functions remain as required.

Document the operating conditions

Some capabilities are provided locally; others rely on integration with system services. Part 4-2 recognises documented compensating countermeasures, but an unspecified external firewall is not a universal answer to every component gap. Identify the particular requirement, the measure and the integration conditions; assess any capability or certification claim against the

applicable rules. [7, common component security constraints]

The integrator needs a usable security manual: supported configurations, required services, hardening steps, account handling, update and recovery procedures, known limitations and end-of-support conditions. Test important instructions on the released version. A secure factory configuration can be weakened during commissioning if the deployment guidance is incomplete.

10 OPERATION AND MAINTENANCE

Preserve protection after handover

Operational security depends on recurring activities, available evidence and people who can act. The asset-owner and service-provider programmes connect these duties. [2,3]

The asset-owner programme

IEC 62443-2-1:2024 specifies policies and procedures for the asset owner's security programme for an operational IACS. The owner also includes the operator in this context. For suppliers, the practical implication is that equipment and services must fit the customer's continuing arrangements, rather than ending the security discussion at site acceptance. [2]

Establish who reviews accounts, approves connections, receives advisories, monitors relevant events and can authorise isolation or restoration. PRAETORIO recommends recording these duties with the required information, review frequency and escalation contact. Link them to existing maintenance and management-of-change practices.

Service delivery needs its own controls

Part 2-4 addresses the security processes a service provider can offer during integration and maintenance. Its subject areas include staffing, architecture, configuration, remote access, event and account management, malware protection, patching and backup or restoration. Agreed scope and applicable profiles determine the service being assessed. [3]

For remote maintenance, approve a specific purpose and window, identify the engineer, restrict permissions, retain appropriate records and close access when the work ends. Confirm the approved configuration afterwards. A subcontractor or temporary service account must be included in the same responsibility model.

PRAETORIO recommends testing an urgent support scenario before an incident: can the supplier assist without bypassing the customer's access and change controls?

Patch decisions are engineering decisions

Patch management in an industrial environment balances exposure against the risk of a change affecting control, compatibility or availability. IEC TR 62443-2-3 provides guidance for supplier and asset-owner activities; part 4-1 addresses the supplier's security update process. [6,8]

For each relevant advisory, establish the affected product and version, exposure in the deployed configuration, supplier qualification information and the installation constraints. Test the proposed update and define restoration or rollback before deploying it. Record the result and verify that the asset inventory reflects the new state.

If immediate patching is not feasible, record the risk decision, responsible owner, interim measures and review trigger. Deferral without a reviewed treatment can become an indefinite exposure. Unsupported components need a lifecycle decision, not repeated postponement.

Recovery must include the process

A backup file is not proof that production can be restored. Recovery may require firmware, application code, recipes, licences, certificates, keys, network configuration and compatible engineering tools. Preserve these with access controls and a documented restoration sequence.

Exercise recovery with the responsible personnel. Check integrity, interlocks, configuration and safe restart conditions before returning equipment to service. Agree and validate the recovery objective in the relevant environment. [5, SR 7.3 and SR 7.4]

Reassess after material changes to connectivity, firmware, process hazards or support status. Maintain the risk basis and evidence as the installation evolves.

11 VERIFICATION AND ASSURANCE

Make every claim traceable

A useful evidence package explains the assessed object, the applicable requirement, the implemented measure and the observed result.

The packaging-line example starts with a maintenance user attempting an unauthorised change. The table traces that scenario into concrete evidence. The SR references identify relevant

topics in IEC 62443-3-3:2013; the wording and acceptance tests are illustrative project requirements. Additional requirements and enhancements may apply. [5]

Project requirement	Relevant topic	Acceptance evidence
R-01 Viewing users cannot download a control programme.	SR 2.1 Authorisation enforcement	Test permitted viewing and denied downloads for each defined role; record identity and configuration.
R-02 Engineering traffic uses only the approved conduit and destinations.	SR 5.2 Zone boundary protection	Demonstrate permitted traffic and attempts to bypass the boundary, including temporary access paths.
R-03 Defined security-relevant access and change events are recorded.	SR 2.8 Auditable events	Trigger the agreed events and verify recorded context, retrieval and response to storage or logging failure.
R-04 The approved control configuration can be restored.	SR 7.3 and SR 7.4 Backup and recovery	Restore a representative system and verify configuration integrity and operational restart conditions.

Requirements testing establishes specified behaviour; threat-mitigation testing examines the intended defences; vulnerability testing searches for weaknesses; penetration testing examines exploitable combinations. These activities answer different questions. Part 4-1 treats them separately and includes tester-independence requirements. A penetration-test report alone does not demonstrate the whole lifecycle. [6, SVV-1 to SVV-5]

Retain the tested version, environment, configuration, procedure, result, findings and approval. Track deviations to a treatment decision and retest affected requirements after changes. For an operational plant, use agreed test windows, safety constraints and restoration arrangements;

disruptive tests generally need a representative environment or specific operational authorisation.

Read certification within its boundary

Independent certification can provide assurance for a defined development process, component, system or other scheme-specific scope. Verify the standard editions, covered versions, level or maturity claims, conditions and continuing obligations. A process certificate is not a component-capability certificate; a component certificate does not certify the installed IACS. Self-assessment, independent assessment and certification are distinct forms of evidence and should be labelled accordingly.

12 IMPLEMENTATION ROADMAP

Start with a representative delivery

A bounded pilot makes responsibilities, gaps and evidence visible before the approach is extended across a product portfolio or installed base.

Establish the baseline

Choose one product family, machine or system with representative interfaces and support obligations.

Gather the architecture, asset and software inventories, existing risk work, customer requirements, manuals, test records and support

arrangements. Agree the applicable standard parts and editions and the object of any intended claim.

Resolve unknown boundaries early. A customer's request for "SL 2" is incomplete until the scope, target or capability meaning, requirement basis and deployment assumptions are clear. Record decisions in a short scoping document that engineering, commercial staff and the customer can use consistently.

Assess the gaps and dependencies

Review existing evidence against the applicable requirements. Distinguish absent controls, missing evidence and unclear ownership: they require different treatment. A well-implemented feature may need a test record; an unsupported interface may require redesign or a changed deployment architecture.

Prioritise according to risk and project dependencies. Product changes, supplier lead times, operational access and test facilities often determine the critical path. Assign an owner, acceptance evidence and milestone to every action.

Implement and demonstrate

Integrate security work into the existing requirements, design, change and release processes. Produce evidence as work is performed. Verify both the intended function and the behaviour when access is denied, services fail or inputs are abnormal.

Before customer handover, reconcile the as-built configuration with the assessed design and resolve the responsibilities needed to maintain it.

Make effort estimable

For a quotation, quantify the number of product variants, sites, distinct architectures, interfaces,

software platforms and external suppliers. Establish documentation quality, available test environments, access restrictions, required languages and the expected form of independent assessment.

Separate the effort for assessment, remediation, verification and certification support. A gap assessment can define the next work package; it cannot responsibly promise a fixed remediation effort before the gaps and dependencies are understood. Agree what customer participation and existing evidence the estimate assumes.

PRAETORIO recommends milestone-based planning: scope agreed, risk and requirements approved, design accepted, evidence reviewed, and handover completed. The duration depends on the technical gaps and the operational setting. There is no universal 90-day route to compliance.

Connect regulatory work carefully

IEC 62443 engineering can support product risk analysis, secure development and vulnerability handling relevant to the EU Cyber Resilience Act. Legal scope, product classification, conformity assessment and other obligations still need their own analysis. Presumption of conformity depends on the applicable legal mechanism and the coverage of cited harmonised standards; an IEC 62443 certificate alone is not automatic CRA conformity. [13,14]

NIS2 addresses risk management and incident reporting for entities within its scope. Asset-owner and service-provider practices can contribute, but applicability and national implementation need separate assessment. Map the obligations to reuse evidence without treating the standard as a substitute for law. [15]

13 PREPARING THE NEXT ENGINEERING STEP

Define a project that can be delivered

The most useful starting point is a real product or installation and a clear decision to be made.

An automation company does not need to begin by rewriting every process. It needs to understand where its current delivery creates security responsibilities, whether those responsibilities are assigned, and what evidence is missing. A focused assessment should leave the engineering team with decisions it can implement and management with a credible view of scope and effort.

PRAETORIO can support scope definition, system and product risk analysis, security requirements,

architecture review, development-process improvement and verification planning. The engagement should be tailored to the role performed and the intended customer evidence. Where independent certification is required, agree the assessment route early and keep consulting support distinct from the independent certification decision.

Prepare these inputs for the first discussion

Input	Why it matters
Product or system boundary	Identifies the models, versions, functions and interfaces included in the work.
Customer request and target outcome	Separates procurement expectations from a specific conformance or certification scope.
Architecture and operating context	Exposes remote access, external dependencies, safety functions and existing protection.
Current engineering and support evidence	Shows what can be reused and where implementation or evidence is missing.
Delivery constraints	Makes release dates, maintenance windows, test availability and supplier dependencies visible.

Define the outputs before beginning

A practical first work package can produce an agreed scope, a responsibility map, a prioritised gap register and an implementation plan with evidence milestones. Product teams may then focus on the secure development lifecycle and component capabilities; integration teams on risk, architecture and commissioning; service teams on maintaining the agreed security conditions. The

work packages should connect through common requirements and change control.

The aim is a security commitment that engineering can deliver and customers can understand: a defined object, explicit operating conditions, verified protection and a supported lifecycle. That is the basis for a technically credible IEC 62443 discussion.

Discuss your product or system with PRAETORIO at praetorio.com.

TECHNICAL REFERENCES

Sources and publication basis

Selected primary sources and standard editions used in this paper. Publication references and official descriptions checked on 24 September 2026.

[1] [IEC TS 62443-1-1:2009](#). Terminology, concepts and models.

[2] [IEC 62443-2-1:2024](#). Security program requirements for IACS asset owners.

[3] [IEC 62443-2-4:2023](#). Security program requirements for IACS service providers.

[4] [IEC 62443-3-2:2020](#). Security risk assessment for system design.

[5] [IEC 62443-3-3:2013](#). System security requirements and security levels; listed copy includes the 2014 corrigendum.

[6] [IEC 62443-4-1:2018](#). Secure product development lifecycle requirements.

[7] [IEC 62443-4-2:2019](#). Technical security requirements for IACS components; also consult COR1:2022.

[8] [IEC TR 62443-2-3:2015](#). Patch management in the IACS environment.

[9] [IEC PAS 62443-2-2:2025](#). IACS security protection scheme guidance.

[10] [Mandiant, 14 December 2017](#). Attackers deploy TRITON and cause operational disruption to critical infrastructure.

[11] [Hydro, 19 March 2019](#). Hydro subject to cyber attack.

[12] [ESET, 12 April 2022](#). Industroyer2: Industroyer reloaded.

[13] [European Commission](#). Cyber Resilience Act summary.

[14] [European Commission](#). Cyber Resilience Act standardisation.

[15] [European Commission](#). NIS2 Directive: securing network and information systems.

Scope of this publication

Technical explanations draw on the IEC 62443 source summaries supplied for this publication and the official publication information above. Detailed project conformance must be checked against the complete applicable normative texts, corrigenda and assessment rules. The packaging line, requirements, tests and diagrams are original illustrative examples. No client engagement, achieved security level or certification is implied.

Independent PRAETORIO publication. © 2026 PRAETORIO. Product and organisation names belong to their respective owners.