ChatGPT

Designing a repeatable IEC 62443-3-2 risk-assessment tool

Why IEC 62443-3-2 matters

IEC 62443-3-2 is the security risk assessment part of the IEC 62443 standard. It provides a structured method for analysing risk in industrial automation and control systems (IACS). The ISA Global Cybersecurity Alliance notes that the IEC 62443 process starts with **identification of the system under consideration (SuC), a high-level risk assessment, partitioning of the system into zones and conduits, a detailed risk assessment, and documenting cyber-security requirements** [1]. Risk is defined as the product of **consequence and likelihood** [2]; consequence covers safety, environmental and economic impacts, while likelihood reflects the combination of vulnerabilities and the probability that a threat has the skills and motivation to exploit them [3]. An initial assessment assumes likelihood = 1 (worst-case scenario) and is used to define security-level targets (SL-T) and identify high-risk zones [4], whereas a detailed assessment evaluates credible threat scenarios and residual risk [5].

Types of assessments to implement

Different types of assessments will deliver different value. The tool should allow the user to pick an assessment type and then collect the appropriate level of detail. Suggested assessment types are described below.

Assessment type	Purpose / when to use	Key characteristics
Initial (high-level) risk assessment	First stage of IEC 62443 risk analysis [4]. Used when scoping a project or screening multiple systems.	Define the system under consideration (SuC) and the boundaries, assume likelihood = 1, estimate worst-case impacts, identify zones and conduits, set **initial security-level targets** (SL-T). Requires minimal asset details.
Detailed risk assessment	When the initial assessment shows risk above tolerable limits [6]. Used for critical zones or after major changes.	Identify realistic threat scenarios, evaluate vulnerabilities and existing counter-measures, estimate likelihood and impact, refine SL-T for each zone or conduit, and document cyber-security requirements [7]. Requires detailed asset inventory, network diagrams and controls.
Vulnerability assessment	To identify current vulnerabilities and mis-configurations. Often performed in support of the detailed assessment.	Use automated scans or manual enumeration to collect OS versions, services and configurations [8]. Map discovered vulnerabilities to risk scenarios and feed them into the detailed assessment.

Assessment type	Purpose / when to use	Key characteristics
Compliance/ maturity assessment	To determine how well an organisation's policies and controls align with the IEC 62443 foundational requirements (FR) and security requirements (SR).	Use checklists derived from IEC 62443-2-1, -2-4 and -3-3. Score each requirement (implemented, partially implemented, not implemented). Highlight gaps, recommend improvements and link them to risk-mitigation plans.

Key features of a repeatable tool

1 – Structured workflow reflecting IEC 62443-3-2

Use the **Zonal Cyber Risk (ZCR) stages** described in IEC 62443-3-2 as the backbone of the workflow [9]:

1. **Identify the System under Consideration (ZCR 1)** – collect asset inventory, architecture diagrams and data flow diagrams; record access points [10]. Provide import capabilities for spreadsheets or integration with asset-discovery tools.
2. **Initial risk assessment (ZCR 2)** – let the user select or estimate impact categories (safety, environmental, financial etc.) and use a configurable risk matrix to calculate worst-case risk [11]. For each zone or asset, calculate risk = impact × likelihood (likelihood = 1 in this stage). Allow custom impact scales to reflect organisational risk tolerance.
3. **Zone and conduit partitioning (ZCR 3)** – help the user group assets into logical zones and define conduits. Enforce rules, such as grouping safety-related assets separately and putting temporary or wireless devices in separate zones [12]. Visual tools (drag-and-drop diagrams) can make this process intuitive.
4. **Compare initial risk to tolerable risk (ZCR 4)** – compare calculated risks against the organisation's risk matrix. If initial risk is less than or equal to the tolerable risk, record a justification; otherwise proceed to the detailed assessment [6].
5. **Detailed risk assessment (ZCR 5)** – capture realistic threat scenarios, vulnerabilities and existing controls [7]. Incorporate vulnerability-assessment data. Calculate likelihood based on threat capability, vulnerability severity and control effectiveness. Compute residual risk and adjust the security-level target (SL-T) for each zone/conduit.
6. **Document cybersecurity requirements (ZCR 6)** – convert SL-Ts into actionable requirements. Each requirement should be measurable and aligned with the organisation's policies and regulatory obligations [13].
7. **Approval (ZCR 7)** – include a formal approval workflow where asset owners review and sign off the risk assessment [14].

2 – Data model and storage

A repeatable tool needs to capture the raw assessment data as structured records. Suggested design considerations:

- **Assessment entity**: stores meta-data (assessment type, SuC name, date, assessor, status), references to assets, zones, conduits and risk scenarios.
- **Asset inventory**: contains asset identifiers, descriptions, location, operating system, firmware versions, network interfaces, existing controls and links to vulnerability findings [8].

- **Zone and conduit definitions**: each zone record contains associated assets, security-level target and justification; each conduit record contains connected zones and type (wired, wireless, remote access).
- **Risk scenarios**: for each scenario, record threat description, vulnerability exploited, potential consequence categories, impact rating, likelihood estimate, risk score and recommended mitigation.
- **Controls and counter-measures**: maintain a library of typical controls (firewalls, network segmentation, role-based access, patch management etc.) with references to IEC 62443 security requirements.

Store these records in a database (relational or document-oriented) to support querying, versioning and auditing. Use unique identifiers so assessments can be cloned and updated without overwriting previous versions. Include a **status** field (draft, approved, archived) and timestamps to support traceability.

3 – Configurability and templates

- **Risk matrix configuration**: organisations should be able to define the number of impact levels and likelihood categories and set threshold values for tolerable risk. The tool can provide default matrices for typical OT environments and allow modifications. ISA/IEC guidance emphasises that risk should be ranked using the company's own risk matrix [15].
- **Assessment templates**: provide default questionnaires for initial and detailed assessments. A template can pre-populate typical threat scenarios and vulnerabilities for common asset types (PLCs, HMIs, network switches) and save time for repeat assessments.
- **Compliance checklists**: include sections mapping the controls in IEC 62443-3-3 and -2-4 to the organisation's implementation. Use yes/no/partial fields with evidence links.

4 – Report generation and archiving

- Generate human-readable reports in PDF/Word summarising the assessment: scope, methodology, zone and conduit diagrams, risk matrix, risk scores, SL-Ts, mitigation recommendations and compliance gaps. Include an executive summary and technical details.
- Provide options to export the **raw assessment data** as JSON or CSV. This allows future re-use or integration with BI tools for trend analysis.
- Implement version control: each time an assessment is updated, store a new version while retaining previous versions. This supports auditing and comparison of risk over time.

5 – Re-use and continuous improvement

- **Clone and update**: allow users to duplicate an existing assessment, update asset lists or controls, and run the calculations again. Use difference reports to highlight changes in risk.
- **Trend dashboards**: show how risk scores evolve across assessments and identify zones where risk is consistently high.
- **Integration**: support data import from asset-management systems and vulnerability scanners. Provide an API for external tools to query assessments.

6 – Process considerations for getting the most from assessments

- **Cross-functional involvement** – risk is not solely a technical issue; it also affects operations and safety. Industrial-cyber experts note that effective assessments require collaboration between security and operations teams and an understanding of how physical processes function [16].

- **Site visits and data collection** – paper- or interview-based assessments provide high-level insight, but site visits and technical evaluations reveal “ground truth” and unknown single points of failure [17]. The tool should facilitate capturing observations and photos during site visits.
- **Focus on critical assets** – experts warn that cataloguing every asset and vulnerability can produce noise and overwhelm teams. Instead, begin by identifying mission-critical processes and the assets that enable them [18]. The tool should therefore support prioritization and filtering.
- **Consequence-driven analysis** – modern risk assessments are moving beyond abstract threat modeling toward consequences and resilience [19]. The tool’s risk scenarios should explicitly link threat actions to business impacts (throughput loss, safety disruption, environmental harm).
- **Incorporate evolving threats** – maintain an up-to-date threat library with references to MITRE ATT&CK for industrial control systems. Users should periodically review and update threat scenarios to reflect the changing landscape.

Summary

To build a repeatable IEC 62443 risk-assessment tool, base its workflow on the ZCR stages of IEC 62443-3-2: define the system under consideration, perform an initial worst-case assessment, partition the system into zones and conduits, conduct a detailed assessment when necessary, document requirements and obtain approval [20]. Different assessment types (initial, detailed, vulnerability and compliance assessments) allow the user to pick the level of detail and objectives. The tool should store structured data about assets, zones, risk scenarios and controls, allow configuration of risk matrices, generate reports and raw data exports, and support cloning assessments for later reuse. Incorporating site-visit data, focusing on consequence-driven analysis and critical assets, and aligning with organisational risk tolerances will help organisations derive the most value from their assessments [21].

---

[1] [2] [3] [15] [20] White Paper Excerpt: Leveraging ISA 62443-3-2 For IACS Risk Assessment and Risk Related Strategies
https://gca.isa.org/blog/white-paper-excerpt-leveraging-isa-62443-3-2-for-iacs-risk-assessment-and-risk-related-strategies

[4] Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2
https://gca.isa.org/blog/cybersecurity-risk-assessment-according-to-isa-iec-62443-3-2

[5] [6] [7] [9] [10] [11] [12] [13] [14] A Practical Guide to Risk Assessment in ICS/OT using IEC 62443–3.2 | by Sathish | Jul, 2025 | Medium
https://medium.com/@sathish95/a-practical-guide-to-risk-assessment-in-ics-ot-using-iec-62443-3-2-c3fb43471e67

[8] Practical Guide to Performing Risk Assessment as per IEC 62443-3-2 and NIST 800-30 – Hard Hat Security
https://hardhatsecurity.com/2024/05/15/practical-guide-to-performing-high-and-detailed-level-risk-assessment-as-per-iec-62443-3-2-and-nist-800-30/

[16] [17] [18] [19] [21] Industrial cyber risk assessment evolving into operational imperative with focus on consequence and resilience - Industrial Cyber
https://industrialcyber.co/features/industrial-cyber-risk-assessment-evolving-into-operational-imperative-with-focus-on-consequence-and-resilience/