

EMB3D for IEC 62443-3-2 Risk Assessment

MITRE EMB3D™ Threat Model as a structured input to IEC 62443-3-2 Cybersecurity Risk Assessment

Evaluation Guide for IACS Practitioners

Revision 1.0

Product: Evaluation Guide
Project name: EMB3D / IEC 62443-3-2 Integration
Customer: —
Project no.: —
Status: Final

Role	Name	Org. Unit
Author/Responsible		
Verification/Review		
Verification/Review		
Approval		

Template Change History

Version	Date	Author	Change description
1.0	21.04.2026	Markus Steinmetz	Document created from source material

Table of Contents

1 Purpose and audience	3
2 What is IEC 62443-3-2?	3
2.1 The zone and conduit model	3
2.2 The ZCR 5.x detailed risk assessment workflow	3
3 What is MITRE EMB3D™?	4
3.1 The three-layer architecture	4
3.1.1 Device properties (PID-xx)	4
3.1.2 Threats (TID-xxx)	5
3.1.3 Mitigations (MID-xxx)	5
3.2 The EMB3D workflow	5
4 Mapping EMB3D to ZCR 5.x	6
4.1 Steps with strong fit	6
ZCR 5.1 – Identify threats	6
ZCR 5.2 – Identify vulnerabilities	7
ZCR 5.8 – Evaluate existing countermeasures	7
ZCR 5.12 – Identify additional countermeasures	7
4.2 Steps with partial fit	7
ZCR 5.3 – Consequence and impact	7
ZCR 5.9 – Re-evaluate likelihood and impact	8
4.3 Steps with no direct contribution	8
5 Limitations and gaps	8
5.1 Scope mismatch: device vs. system	8
5.2 No consequence methodology	8
5.3 No likelihood quantification	8
5.4 Device-only mitigations	8
5.5 No OT protocol-specific threat depth	9
6 Recommended integration workflow	9
7 Conclusion	10
8 References	10

1 Purpose and audience

Who is this document for?

This guide is written for two audiences at once. Beginners in industrial cybersecurity will find plain-language explanations of each concept before the technical detail is introduced. Experts can skip the grey background boxes (marked "For beginners") and go straight to the mapping analysis.

This document evaluates whether and how the MITRE EMB3D™ Threat Model (version 2.0, April 2025) can be used as a structured input to the IEC 62443-3-2:2020 cybersecurity risk assessment process for Industrial Automation and Control Systems (IACS). It traces each of the 13 sub-steps of the detailed risk assessment workflow (ZCR 5.1 through ZCR 5.13) and assesses the degree to which EMB3D provides usable data for each step.

The evaluation is intended for asset owners, system integrators, cybersecurity assessors, and product security engineers working in process industries, critical infrastructure, and manufacturing.

2 What is IEC 62443-3-2?

For beginners: What problem does this standard solve?

Industrial control systems — the systems that run power plants, water treatment facilities, chemical plants, and factories — face cyber threats that can cause physical damage, environmental harm, or endanger human lives. IEC 62443 is a family of international standards that provides a structured approach to securing these systems. Part 3-2 specifically addresses how to assess the cybersecurity risk of a particular system and determine what security measures are needed.

IEC 62443-3-2:2020, Security risk assessment for system design, defines the methodology for performing cybersecurity risk assessments at the system level. It is part of the broader IEC 62443 standard series for IACS security.

2.1 The zone and conduit model

IEC 62443-3-2 organises an IACS into zones (logical or physical groupings of assets that share common security requirements) and conduits (the communication channels that connect zones). The risk assessment is performed per zone and per conduit.

2.2 The ZCR 5.x detailed risk assessment workflow

When an initial risk assessment indicates that risk exceeds the organisation's tolerable threshold (ZCR 4.1), the standard requires a detailed assessment following a 13-step workflow, designated ZCR 5.1 through ZCR 5.13. This workflow is the focus of this document. The steps, in sequence, are:

- **ZCR 5.1 – Identify threats:** Develop a comprehensive list of threats that could affect assets in the zone or conduit.
- **ZCR 5.2 – Identify vulnerabilities:** Analyse the zone or conduit to identify known vulnerabilities associated with its assets and access points.
- **ZCR 5.3 – Determine consequence and impact:** Evaluate each threat scenario for worst-case impact on safety, environment, finances, and operations.
- **ZCR 5.4 – Determine unmitigated likelihood:** Estimate the likelihood of each threat materialising, without considering existing countermeasures.

- **ZCR 5.5 – Determine unmitigated risk:** Combine impact and likelihood to determine unmitigated risk using the organisation’s risk matrix.
- **ZCR 5.6 – Determine SL-T:** Establish the target security level for the zone or conduit.
- **ZCR 5.7 – Compare unmitigated risk with tolerable risk:** Decide whether to accept, transfer, or mitigate.
- **ZCR 5.8 – Identify and evaluate existing countermeasures:** Document what security controls are already in place and assess their effectiveness.
- **ZCR 5.9 – Re-evaluate likelihood and impact:** Recalculate likelihood and impact considering existing countermeasures.
- **ZCR 5.10 – Determine residual risk:** Combine mitigated likelihood and impact to determine residual risk.
- **ZCR 5.11 – Compare residual risk with tolerable risk:** Determine whether residual risk is acceptable.
- **ZCR 5.12 – Identify additional countermeasures:** If residual risk exceeds tolerance, identify additional technical or procedural controls.
- **ZCR 5.13 – Document and communicate results:** Create the formal risk assessment report.

Key insight

Notice that ZCR 5.1 and 5.2 are parallel inputs, not sequential steps. Threats and vulnerabilities are identified independently and then combined: vulnerabilities feed into the likelihood assessment (ZCR 5.4), while threat scenarios feed into the consequence assessment (ZCR 5.3). This distinction matters when mapping external tools like EMB3D.

3 What is MITRE EMB3D™?

For beginners: What is a threat model?

A threat model is a structured catalogue of things that could go wrong with a system, organised so that engineers can systematically check whether their system is protected. Think of it as a checklist of known attack methods, organised by the type of device being assessed.

EMB3D is a publicly available, community-driven knowledge base maintained by MITRE, focused specifically on cyber threats to embedded devices — the controllers, sensors, actuators, gateways, and edge computing hardware found throughout industrial environments. Version 2.0 was released in April 2025 and includes a STIX/JSON data export for programmatic integration.

3.1 The three-layer architecture

EMB3D is structured around three interlinked concepts:

3.1.1 Device properties (PID-xx)

Properties describe the hardware and software characteristics of a device. They are organised into four categories: Hardware (e.g., PID-11 “Device includes a microprocessor”), System Software (e.g., PID-21 “Device includes a bootloader”), Application Software (e.g., PID-33 “Device includes interactive services”), and Networking (e.g., PID-41 “Device exposes remote network services”). Properties are hierarchical: PID-41 contains sub-properties like PID-411 (services that handle sensitive data) and PID-4111 (lacking message authentication).

For beginners: What does “property” mean here?

A property is a technical characteristic of your device. For example, if your PLC has an Ethernet port running a web server for configuration, that corresponds to property PID-311 (“Device includes web/HTTP applications”). By identifying which properties your device has, you can look up which threats apply to it.

3.1.2 Threats (TID-xxx)

Each threat describes how an attacker can exploit a device feature to achieve a specific malicious objective. There are approximately 80 threats in v2.0, organised into the same four categories as the properties. Each threat entry includes a description of the attack, the device properties that enable it, references to MITRE ATT&CK techniques and CWE weakness classes, known CVEs where applicable, and a threat maturity classification (observed in the wild, proof-of-concept demonstrated, or theoretical).

Example: TID-310 “Remotely Accessible Unauthenticated Services” describes how an attacker who connects to an exposed network service without authentication can access confidential data or modify device configuration. It maps to PID-331 (unauthenticated services) and PID-41 (remote network services), references ATT&CK technique T0855, and cites CWE-285 (Improper Authorization).

3.1.3 Mitigations (MID-xxx)

Each threat has associated mitigations — technical mechanisms that device vendors should implement to prevent or reduce the risk. Mitigations are tiered into three maturity levels:

- **Foundational:** Basic security hygiene measures expected in any device (e.g., MID-011 “Authenticated firmware updates”).
- **Intermediate:** More advanced controls that require deliberate engineering effort (e.g., MID-022 “Secure boot chain”).
- **Leading:** State-of-the-art protections suitable for high-assurance environments (e.g., MID-062 “Runtime integrity verification”).

3.2 The EMB3D workflow

The intended usage workflow is: (1) characterise your device’s properties using the Properties Mapper, (2) look up the threats mapped to those properties, and (3) for each applicable threat, determine whether the associated mitigations are implemented. This is a device-level assessment — a critical distinction that shapes how EMB3D integrates with IEC 62443-3-2, which operates at the system/zone/conduit level.

4 Mapping EMB3D to ZCR 5.x

The following table provides a summary of how each EMB3D element (Properties, Threats, Mitigations) maps to each ZCR 5.x sub-step. The detailed rationale for each rating follows in sections 4.1 through 4.3.

Table 1: Mapping

ZCR	Step name	Fit	EMB3D contribution
5.1	Identify threats	Strong	Threats (TID) mapped via device Properties (PID) provide a systematic device-level threat register.
5.2	Identify vulnerabilities	Strong	CWE/CVE cross-references per threat; property-based attack surface enumeration.
5.3	Consequence and impact	Partial	Threat effects describe device-level impact only; process/safety consequences require PHA/HAZOP.
5.4	Unmitigated likelihood	None	EMB3D threat maturity (observed/PoC/theoretical) is qualitative; no calibrated likelihood scale.
5.5	Unmitigated risk	None	Risk matrix application is organisation-specific; no EMB3D contribution.
5.6	Determine SL-T	None	SL-T assignment is an asset-owner decision outside EMB3D's scope.
5.7	Compare with tolerable risk	None	Tolerable risk thresholds are organisation-specific.
5.8	Evaluate countermeasures	Strong	Mitigations (MID) with Foundational/Intermediate/Leading tiering serve as a checklist.
5.9	Re-evaluate likelihood	Partial	Mitigation presence informs qualitative likelihood reduction but not quantitative re-rating.
5.10	Residual risk	None	Requires organisation-specific risk matrix calculation.
5.11	Compare residual risk	None	Requires tolerable risk threshold comparison.
5.12	Additional countermeasures	Strong	Mitigation catalogue with maturity tiering provides an ordered selection guide.
5.13	Document results	None	Documentation is a process step; EMB3D provides citable references (TID/MID identifiers).

4.1 Steps with strong fit

ZCR 5.1 – Identify threats

IEC 62443-3-2 requires that a comprehensive list of threats be developed for each zone and conduit, including the threat source, its capability, possible threat vectors, and the affected assets. EMB3D's property-to-threat mapping directly supports this: the assessor characterises each embedded device type within the zone using PID properties, and the database enumerates the applicable threats.

Each EMB3D threat entry includes ATT&CK technique references that describe threat source capabilities and vectors, which satisfy the informational requirements of ZCR 5.1. The structured TID identifiers also provide traceability for documentation purposes.

Practical example

A zone contains a PLC with Ethernet connectivity (PID-41), a web-based configuration interface (PID-311), and default credentials on the web server (PID-332). The Properties Mapper will enumerate TID-310 (Unauthenticated Services), TID-311 (Default Credentials), TID-319 (Cross-Site Scripting), and several other threats. This gives the assessment team a structured starting point for the threat register.

ZCR 5.2 – Identify vulnerabilities

IEC 62443-3-2 requires identifying known vulnerabilities associated with assets in the zone, including access points. The supplemental guidance explicitly references ICS-CERT, product suppliers, and vulnerability databases as sources.

EMB3D contributes in two ways. First, each threat entry references CWE weakness classes and, where applicable, specific CVEs — these are direct vulnerability identifiers. Second, the property-based approach identifies classes of vulnerability exposure (e.g., a device with PID-271 “firmware not cryptographically verified” is inherently vulnerable to TID-211 “Unauthenticated Firmware Installation”) that CVE databases may not capture for bespoke OT devices without registered advisories.

ZCR 5.8 – Evaluate existing countermeasures

IEC 62443-3-2 requires identifying and evaluating existing countermeasures to determine their effectiveness at reducing likelihood or impact. The supplemental guidance notes that IEC 62443-3-3 provides guidance on countermeasure types and assigns capability security levels (SL-C).

EMB3D’s mitigations serve as a device-level checklist: for each applicable threat, the assessor can verify whether the associated mitigations are implemented in the device. The three-tier maturity classification (Foundational, Intermediate, Leading) provides an ordinal measure of countermeasure sophistication that aligns conceptually with the SL-C approach in IEC 62443-3-3. A device implementing only Foundational mitigations offers a lower degree of protection than one implementing Leading mitigations.

ZCR 5.12 – Identify additional countermeasures

When residual risk exceeds tolerable levels, the assessor must identify additional countermeasures. EMB3D’s mitigation catalogue provides a structured selection guide: the assessor can look up which mitigations exist for the unmitigated threat, determine which tier is currently implemented (or absent), and select the next tier up. This provides an escalation path that is otherwise difficult to construct from generic IEC 62443-3-3 system requirements alone, because EMB3D’s mitigations are specific to the device’s technical architecture.

4.2 Steps with partial fit**ZCR 5.3 – Consequence and impact**

EMB3D threat descriptions include the device-level effect of a successful attack (e.g., “access confidential data”, “modify device configuration”, “install malicious firmware”). This provides the starting point of the causal chain that leads to a consequence.

However, IEC 62443-3-2 requires consequence assessment in terms of business and safety impact: personnel safety, financial loss, environmental damage, business interruption. The translation from “attacker modifies PLC logic” to “loss of containment causing chemical release” requires process hazard analysis (PHA/HAZOP), Layers of Protection Analysis (LOPA), or the methodology described in ISA-TR84.00.09. EMB3D provides the “what can go wrong at the device”; the “so what for the plant” must come from process safety expertise.

For beginners: Why can't a device threat model tell you about plant-level consequences?

Because the same device compromise can have very different consequences depending on what the device controls. A PLC running a packaging line and a PLC controlling a high-pressure reactor vessel may have identical cybersecurity properties and face the same EMB3D threats — but the consequences of a successful attack are vastly different. The consequence assessment must consider the physical process, not just the device.

ZCR 5.9 – Re-evaluate likelihood and impact

EMB3D mitigations help reason qualitatively about likelihood reduction: a device that implements MID-034 (input validation) is less likely to be compromised via TID-319 (XSS) than one without it. However, formal re-evaluation requires organisation-specific likelihood scales, and the assessment must also account for compensating controls outside the device (network segmentation, monitoring, procedural controls) that EMB3D does not address.

4.3 Steps with no direct contribution

ZCR 5.4 (unmitigated likelihood), ZCR 5.5 (unmitigated risk), ZCR 5.6 (SL-T), ZCR 5.7 (risk comparison), ZCR 5.10 (residual risk), ZCR 5.11 (residual risk comparison), and ZCR 5.13 (documentation) are methodology-level steps that depend entirely on the asset owner's risk management framework, corporate risk matrix, and regulatory context. EMB3D provides no data for these steps — nor is it designed to. These steps require site-specific, organisation-specific judgement.

Note that ZCR 5.13 (documentation) benefits indirectly from EMB3D's structured identifiers: TID and MID codes provide citable, traceable references for the risk assessment report.

5 Limitations and gaps**5.1 Scope mismatch: device vs. system**

The most fundamental limitation is the scope mismatch between EMB3D (device-level) and IEC 62443-3-2 (system/zone/conduit-level). Threats that arise from the interaction between devices — such as DCS configuration logic manipulating SIS through shared conduits, BPCS/SIS coordination vulnerabilities, or application-layer logic gaps — are outside EMB3D's scope. These inter-device, inter-zone threats are among the most consequential for process safety and are precisely where IEC 62443 coverage itself has known gaps (e.g., the lack of explicit coverage for Layer 3 application logic between BPCS and SIS).

5.2 No consequence methodology

EMB3D cannot replace HAZOP, PHA, LOPA, or ISA-TR84.00.09 for determining process safety consequences. The ZCR 5.3 → 5.5 chain requires consequence assessment in business and safety terms that are fundamentally outside a device-level threat model.

5.3 No likelihood quantification

EMB3D's threat maturity classification (observed / proof-of-concept / theoretical) provides a qualitative sense of how proven a threat is, but it is not calibrated to the likelihood scales that IEC 62443-3-2 Annex B recommends (e.g., probability ranges such as "Likely: 50–90%" or frequency-based scales). The maturity information is useful background context but cannot substitute for a formal likelihood assessment.

5.4 Device-only mitigations

EMB3D mitigations are technical controls implemented within the device itself. Process security measures (policies, procedures, training, maintenance programmes) as defined in IEC 62443-2-1 and IEC 62443-2-4 are outside scope. For many IACS environments — especially those with legacy devices that cannot be upgraded — compensating controls at the operational level are often the only practical risk reduction measure. EMB3D provides no guidance on these.

5.5 No OT protocol-specific threat depth

While EMB3D's Networking category (TID-4xx) covers generic network threats (unauthenticated messages, unencrypted communications, protocol side channels), it does not provide deep, protocol-specific threat analysis for industrial protocols such as Modbus/TCP, OPC UA, PROFINET, EtherNet/IP, or IEC 61850 MMS. Protocol-specific vulnerability databases and vendor advisories remain necessary supplements.

6 Recommended integration workflow

Based on the analysis above, EMB3D is best used as a structured input to ZCR 5.1, 5.2, 5.8, and 5.12 within a broader IEC 62443-3-2 risk assessment. The following workflow describes how to integrate it practically.

- **Characterise devices per zone.** For each zone and conduit, inventory the embedded device types and use the EMB3D Properties Mapper to identify the applicable PID properties per device. This step enriches the asset inventory required by ZCR 2.
- **Generate the device-level threat register.** Map the identified properties to EMB3D threats (TID). This produces the device-specific component of the threat register for ZCR 5.1. Supplement with zone-level and inter-device threats from other sources (PHA/HAZOP, ATT&CK for ICS, ISA-TR84.00.09 PSCAI methodology).
- **Extract vulnerability indicators.** Collect the CWE and CVE references from each applicable TID entry for ZCR 5.2. Cross-reference with ICS-CERT advisories and vendor vulnerability disclosures for the specific device models in the zone.
- **Assess consequences independently.** Use the device-level threat effects from EMB3D as the starting point of the causal chain but determine the process-level consequences and business impact (ZCR 5.3) using PHA/HAZOP, LOPA, and process safety engineering judgement.
- **Apply the organisation's risk methodology.** Use the organisation's risk matrix, likelihood scales, and tolerable risk thresholds for ZCR 5.4 through 5.7. These are entirely outside EMB3D's scope.
- **Evaluate countermeasures against EMB3D mitigations.** For each applicable TID, check whether the associated MID mitigations are implemented in the device (ZCR 5.8). Record the implemented mitigation tier (Foundational, Intermediate, Leading) as part of the countermeasure effectiveness assessment. Cross-reference with IEC 62443-3-3 SR/RE mappings for SL-C evaluation.
- **Select additional countermeasures from the mitigation catalogue.** Where residual risk exceeds tolerance (ZCR 5.12), use the EMB3D mitigation catalogue to identify the next tier of device-level controls. Supplement with system-level countermeasures from IEC 62443-3-3 and process-level measures from IEC 62443-2-1/2-4.

Tool integration opportunity

EMB3D v2.0 provides STIX/JSON exports. This enables programmatic workflows: import a zone's device inventory, map properties automatically, generate an initial threat register and pre-populate the ZCR 5.1/5.2 outputs. This reduces manual effort and improves consistency, particularly for large IACS installations with many device types.

7 Conclusion

EMB3D is a valuable, freely available complement to IEC 62443-3-2 risk assessment — but it is not a replacement for the standard's full methodology. Its primary contribution is providing a systematic, property-driven threat enumeration at the embedded device level that the standard's zone/conduit model benefits from but does not itself prescribe.

The framework addresses four of the thirteen ZCR 5.x sub-steps with strong, direct support (5.1, 5.2, 5.8, 5.12), contributes partially to two more (5.3, 5.9), and has no role in the remaining seven steps that depend on organisation-specific risk management decisions. The scope gap between device-level and system-level analysis is structural, not a deficiency — it means EMB3D must be used alongside, not instead of, process-level threat assessment tools (PHA/HAZOP, ISA-TR84.00.09) and system-level security requirements (IEC 62443-3-3, IEC 62443-2-1).

For organisations beginning to integrate EMB3D into their cybersecurity risk assessment practice, the recommended approach is to start with new assessments of zones containing modern embedded devices (where property characterisation is straightforward) and expand to legacy device environments as experience is gained. The STIX/JSON export capability in v2.0 makes automated workflow integration feasible for the first time.

8 References

- [1] IEC 62443-3-2:2020, Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design.
- [2] IEC 62443-3-3:2013, Security for industrial automation and control systems – Part 3-3: System security requirements and security levels.
- [3] IEC 62443-2-1:2024, Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners.
- [4] IEC 62443-4-2:2019, Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components.
- [5] MITRE EMB3D™ Threat Model, Version 2.0, April 2025. Available at: <https://emb3d.mitre.org/>
- [6] ISA-TR84.00.09-2024, Cybersecurity Related to the Safety Lifecycle.
- [7] IEC 61511 (all parts), Functional safety – Safety instrumented systems for the process industry sector.

End of document