CYBELLUM

Complying with IEC62443

A Product Security Perspective

IEC 62443 is a comprehensive framework of standards developed for securing Industrial Automation and Control Systems (IACS). It provides a structured approach to cybersecurity, spanning from risk assessment to system design, implementation, and maintenance across various industry sectors. The standard is divided into several parts, each addressing different aspects of cybersecurity within industrial facilities.

For product security professionals, two sections stand out as being most important. The first is IEC 62443-4-1, which deals with the full product security lifecycle considerations during the development phase. The second is IEC 62443-4-2 which specifies security requirements for embedded components.

Section 4-2 requires that teams meet a minimum security level while striving to bring greater maturity to their processes.

Read below to better understand this IEC 62443 with regards to product security and where your adherence stands.

Sections Relevant to Product Security

While 62443 works with a wide variety of security measures, when it comes to product security three sections are critical for adherence.

They are sections 4-1, 4-2, and 3-3.

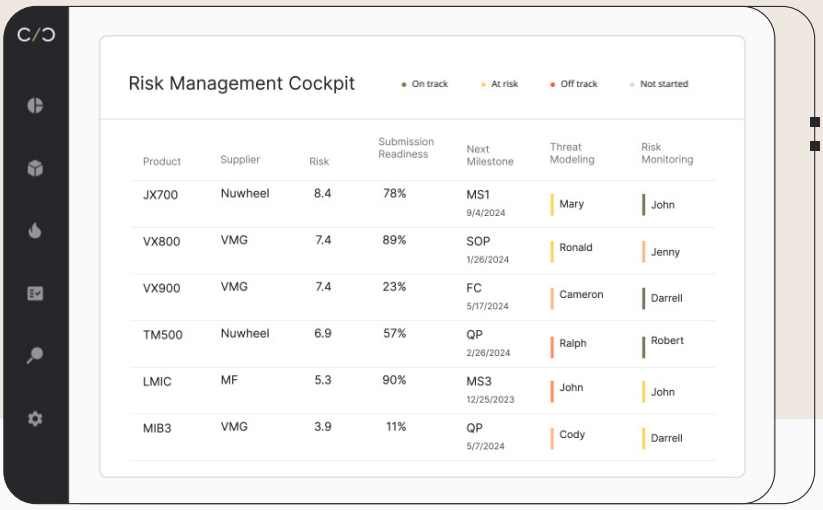
1. **IEC 62443-4-1** describes the requirements for the security development lifecycle (SDL) of control systems and component products. One of the key processes in the product SDL is threat modeling which is a systematic process to identify data flows, trust boundaries, attack vectors, and potential threats to the control system. The security issues identified in the threat model must be addressed in the final release of the product and the threat model itself must be periodically updated during the product's lifecycle.

2. **IEC 62443-4-2** covers technical security requirements for IACS components- and describes the requirements for IACS Components based on the security level. Components include embedded devices, host devices, network devices, and software applications. The principal audience includes suppliers of component products that are used in control systems.

3. **IEC 62443-3-3** further defines the Security Level in terms of the means, resources, skills, and motivation of the threat actor, as shown in the table. It is used as a means to discriminate between requirement enhancements for systems (Part 3-3) and Components (Part 4-2).

Source: Quick Start Guide: An Overview of ISA/IEC 62443 Standards

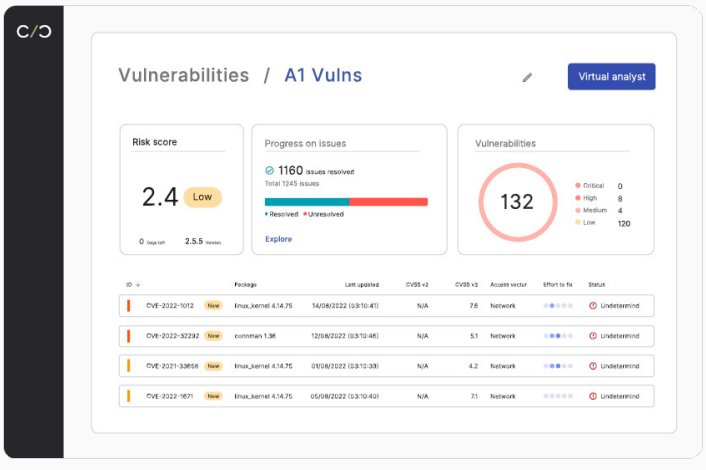
The Product Security Platform allows teams to understand the full status of their operations



How Cybellum's Platform and Services Help Manufacturers Comply

62443-4-1 - Product Security Development Lifecycle Requirements

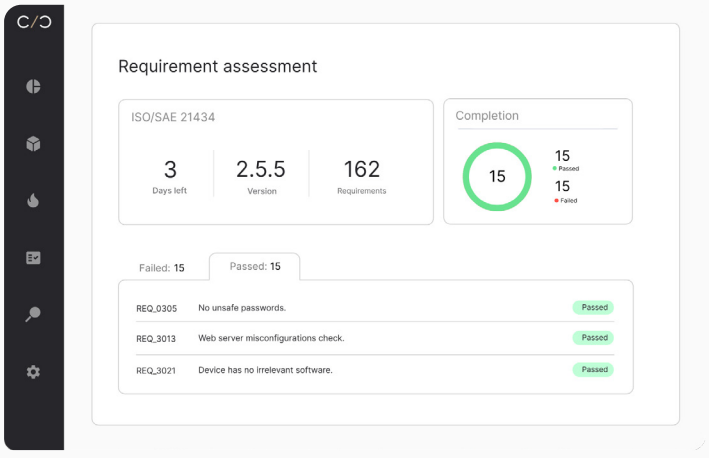
Part 4-1: This part defines how a secure product development process should look like.
It is divided into eight areas ("Practices"):

Item	Requirement	How Cybellum Helps
1	Management of development	**The Product Security Platform** allows for teams to mitigate and minimize risk in the earliest stages of development. These are done by considering all risks within a device via **SBOMs, vulnerability triaging** and management, identifying coding weaknesses and Zero Days, and version variations. This information is logged throughout the full product lifecycle, allowing security teams later in the development process and PSIRTs post-market, to better understand a product's history and maintain a high standard of security. In addition, the **Risk Management Cockpit** in the platform allows teams to track and measure the status of all their product security activities across product lines and lifecycle stages. Cybellum's **Synergy Services** also allow teams to advance their SBOM and PSIRT activities by managing SBOM validation and Incident Response on behalf of the manufacturer. 

Item	Requirement	How Cybellum Helps
2	Definition of security requirements	The Product Security Platform assists teams in validating requirements for various sections of IEC62443 in addition to 50+ built-in standards and regulation workflows. Teams can also implement custom policies to meet internal standards. Product security engineers can follow-up on security findings arising from these policies (such as OS hardening misconfigurations) with detailed fix instructions.

3	Security by design	Cybellums' Product Security Platform provides both engineering level and governance level capabilities to ensure that full product security is reached. This includes our System-of-Systems capability, which helps model complex multi-component products and assess them as a single device or down to the individual component.
		
		This is achieved:
		• During design and development:
		  • Ability to assess the security during the design stage using virtual SBOMs
		  • Create and manage SBOMs, and HBOMs at the product and component levels
		  • Identify and track vulnerabilities across product versions
		  • Analyze OS security hardening configurations against defined policies
		• During production / operational use:
		  • Incident response capabilities allow for continuous monitoring of new vulnerabilities, along with investigation and treatment capabilities for any detected threats that actually impact products

4	Secure implementation	The Product Security Platform can validate secure implementation in multiple ways: • Built-in policy assessments validating secure coding practices such as CERT-C and MISRA-C • Detection and management of coding weaknesses OS hardening requirement validation • Detecting and managing known vulnerabilities lurking in your product's code
5	Security verification and validation testing	Cybellum's platform tracks the treatment of vulnerabilities across software builds and continuous monitoring of vulnerabilities. This includes managing SBOMs and conducting security verification for each version during the development, testing, and production stages. A wide range of security aspects can be identified and managed - ranging from publicly disclosed vulnerabilities, OS misconfigurations, coding weaknesses, and even software licensing risks.

Item	Requirement	How Cybellum Helps
6	Management of security-related issues	The Product Security Platform has a built-in Risk Management Cockpit which allows teams to track and measure their products' cybersecurity and compliance and risks across multiple activities, from vulnerability management to SBOMs and Threat Modeling. Not only that, but a service called ProdSec BI allows teams to customize and build their own security risk management dashboards as well. In addition, the platform offers a streamlined approach to vulnerability management, enabling organizations to quickly identify, prioritize, and remediate vulnerabilities across their software portfolio. It provides automated discovery, real-time tracking, integrated workflow management, actionable guidance, and automated patch validation, empowering organizations to maintain a secure software supply chain. During post-production, the Product Security Platform checks for new vulnerabilities, enabling investigations into security issues.
7	Security update management	Secure software updates are supported in the Product Security Platform by analyzing, scanning, and triaging risks discovered within new software versions as they become available. This allows for product security teams to validate SBOMs and management vulnerabilities with fewer resources.
8	Security Guidelines	Provides detailed technical reports and supporting documentation to assist internal stakeholders and auditors in following a plan and understanding company practices. Such reports include SBOMs, HBOMs, product configuration information, and vulnerability assessments. Policies related to security guidelines (e.g. OS hardening, OWASP Top 10 risk, and others) are built-in to the platform, and custom ones can be created to enable automated validation of adherence. Reports presenting failed/passed guidelines are available as evidence of adherence to the organization's security guidelines. 

62443-4-2 - Product Security Development Lifecycle Requirements

Item	Requirement	How Cybellum Helps
1	CCSC 1 describes that components must take into account the general security characteristics of the system in which they are used.	Similar to the medical and automotive industries, industrial devices operate in unique environments, adapting and protecting against threats that can arise from the natural environment of a facility. The Product Security Platform helps by highlighting risk via CVSS, EPSS, and automated triaging based on device configuration so threats most relevant to the specific device and its environment can be prioritized and mitigated.
2	CCSC 2 specifies that the technical requirements that the component cannot meet itself can be met by compensating countermeasures at the system level (see IEC 62443-3-3). For this purpose, the countermeasures must be described in the documentation of the component.	Product configuration data, including evidence of system-level mitigations, can be added to VEX reports, enabling other product security professionals to recognize the mitigation steps that were implemented.
3	CCSC 3 requires that the "Least Privilege" principle is applied in the component.	The Product Security Platform's OS hardening capabilities are designed for: • Identify security-sensitive default settings around encryption, authentication, logging, interfaces, etc. • Confirm hardened values are set by default by security standards vs convenience. • Enumerate any default accounts, passwords, and SSH keys included in the system and verify these have been changed from common defaults and follow security best practices in terms of password strength and SSH key encryption.
4	CCSC 4 requires that the component is developed and supported by IEC 62443-4-1 compliant development processes.	Cybellum's full product lifecycle approach allows for detailed insight into a component's security posture from development through deployment and end of life, ensuring continuous compliance throughout all stages. (For more on complying with IEC 62443-4-1, see above.)

Security levels according to IEC 62443-3-3

Security Level	Definition	Means	Resources	Skills	Motivation
1	CCSC 1 describes that components must take into account the general security characteristics of the system in which they are used.	Simple	low	generic	low
2	Protection against international violation using simple means with low resources, generic skills, and low motivation	Simple	low	generic	low
3	Protection against international violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation	Sophisticated	moderate	IACS-specific	moderate
4	Protection against international violation using sophisticated means with extended resources, IACS-specific skills, and high motivation	Sophisticated	extended	IACS-specific	high

Part 3-3's security levels are critical for mapping and reporting in section 4-2

The three types of security levels are:

- Capability Security Levels (SL-C) indicate the inherent security a system or component offers without extra measures.
- Target Security Levels (SL-T) represent the aimed security level based on risk assessments and guide product selection and countermeasure design.
- Achieved Security Levels (SL-A) are the actual security levels attained post-implementation.

Complying with IEC62443 is critical to ensure the continued uptime of facilities across manufacturing, critical infrastructure, and various other sectors.In addition, without a proper level of security, organizations risk falling out of compliance and opening themselves to product security threats.

Where does your product security maturity stand?
Take our maturity test to identify capability gaps in complying with IEC 62443

About us

CYBELLUM IS WHERE TEAMS DO PRODUCT SECURITY.

Device manufacturers such as Jaguar Land Rover, Supermicro, Danaher, and Faurecia use Cybellum's Product Security Platform and services to manage cybersecurity risk and compliance across business units and lifecycle stages. From SBOM to Vulnerability Management, Compliance Validation, and Incident Response, teams ensure their connected products are fundamentally secure and compliant – and stay that way.

Download the State of Critical Infrastructure Security

Learn more about Product Security

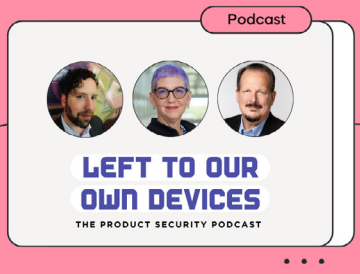
Blogs

Introduction to Medical Device Security Standards and Regulations

Rolling Regulations: Embrace Them, Don't Chase Them

Keeping the Software Supply Chain Accountable with SBOMs

Podcasts



Knowledge Base

Breaking down the FDA's 2023 Premarket Cybersecurity Requirements

Learn More →

Mastering TARA and Risk Management with itemis and Cybellum

Learn More →

SBOM for Connected Devices: Getting it Right

Learn More →

More about the Product Security Platform