ONEKEY.COM

TACKLING SOFTWARE SUPPLY CHAIN RISKS WITH IEC 62443 AND SBOM

ONEKEY

WHITEPAPER

SUMMARY

Tackling Software Supply Chain Risks with IEC 62443 and automated Software-Bill-of-Materials (SBOM)

Reading time: Approximate reading time: 15 min.

This whitepaper targets security teams of industrial automation and control systems (IACS) asset owners and product suppliers.

Components used in an IACS Environment must meet elevated security requirements while preserving essential functions and services. The IEC 62443 standard series provides with part 4-1 a comprehensive framework for product suppliers to build a secure product development lifecycle. While the defense in depth approach implied by this framework can mitigate the impact of vulnerabilities, some vulnerabilities must still be fixed through the product life cycle.

SBOMs help to increase the visibility of the entire supply chain and strengthen the security posture of IACS suppliers and operators by allowing a risk-based patching strategy when new vulnerabilities emerge. The whitepaper discusses how the IEC 62443-4-x proposes to mitigate these risks and how the software development process needs to mature to encompass these mitigating controls. Finally, to reduce time to market, cost and resources due to manual overhead, a high level of automation is required when generating SBOMs and performing security analysis to manage security related issues in compliance with IEC 62443-4-1.

ATTACKS ON IACS ARE ON THE RISE

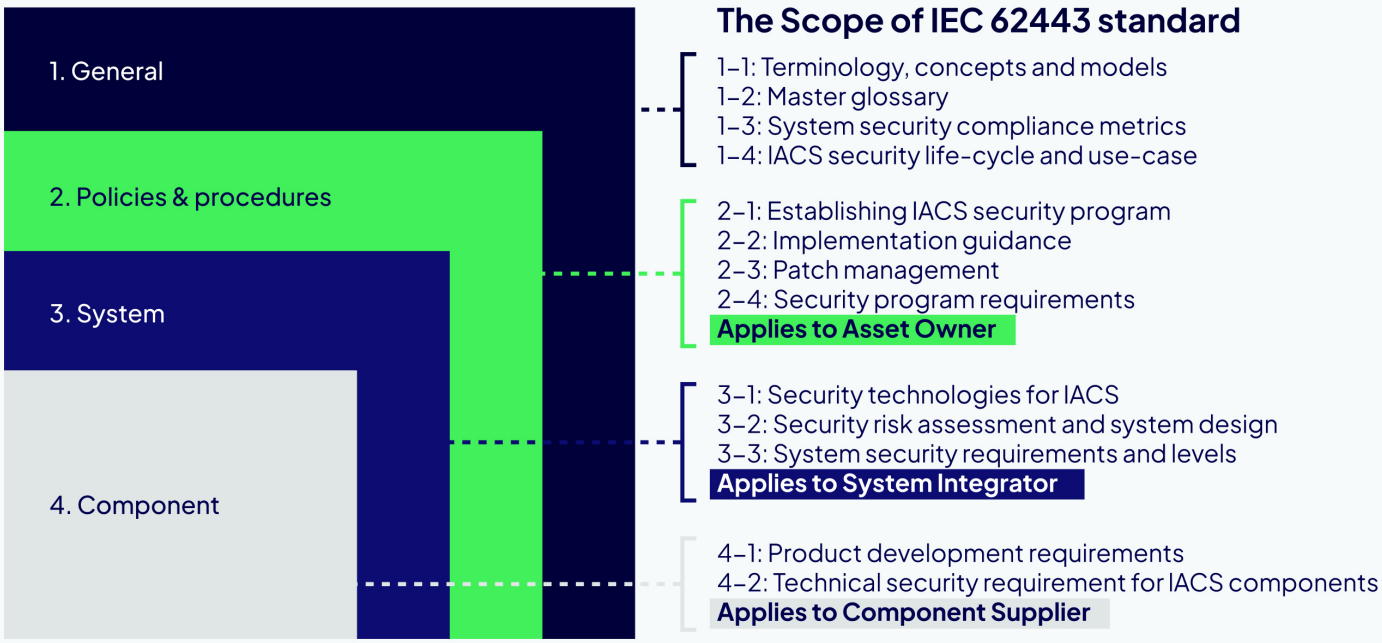
Cyber-attacks on industrial automation and control systems (IACS) are on the rise.1 In the past, IT and IoT systems were predominantly targeted by cyber criminals. But the same threats, such as ransom- ware attacks and devices being joined into massive botnets, increasingly affect IACS and OT too. The reason for this is simple - before IACS got smart and connected, they were mostly operated in air-gapped environments, not connected to the Internet and mostly not even connected to local corporate networks.

Interconnection of IACS increases, so must their Cyber-Resilience

To control IACS components or make changes to their configuration, an engineer would need to physically interact with the machine. With increased digitalization, this is changing rapidly. IACS environments are connected to internal networks and the Internet to feed data into other business processes and to allow for remote configuration and management.

While improved connectivity generally increases productivity and eases administration of IACS environments, those advances go hand in hand with an increased cyber-risk posture: the threat landscape is changing. It is no longer feasible to solely rely on security controls provided by the environment and the perimeter.

As such, the same security principles that apply to IT systems must be adapted to the industrial world. Defense in depth, security by design, and zero trust must be applied to increase resilience of IACS to cyber-attacks while preserving essential functions and services. While traditional IT security mainly deals with confidentiality of data a IACS security solution must protect the integrity and availability of physical assets essential to the controlled process.

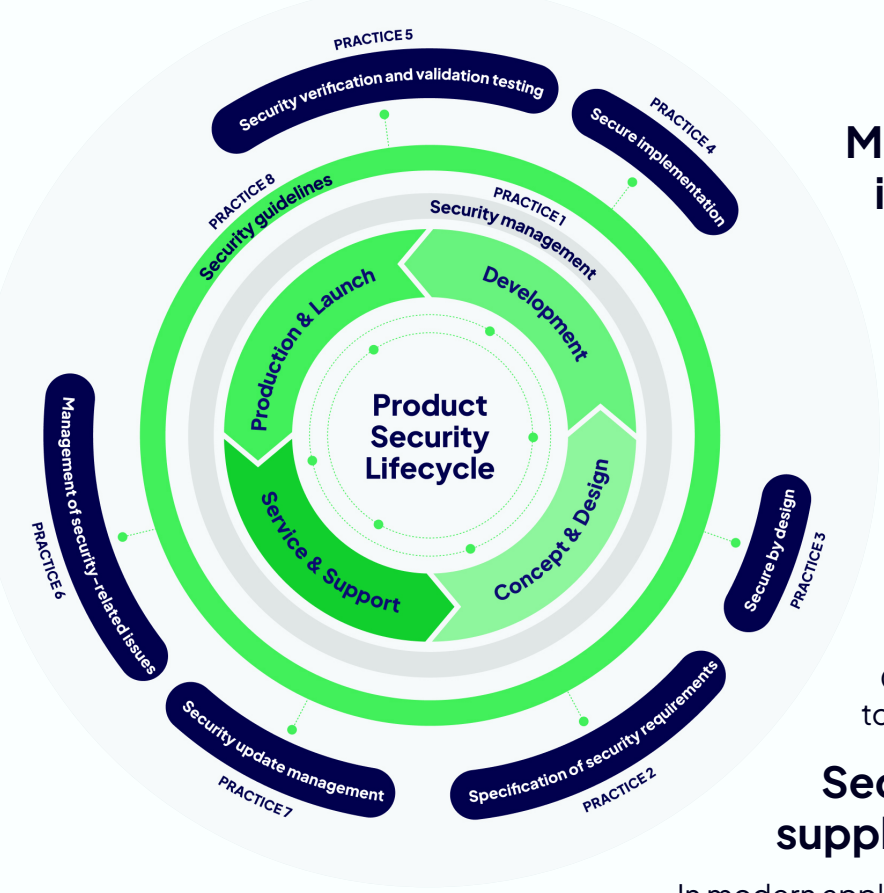


PRODUCT SECURITY LIFECYCLE FOR INDUSTRIAL AUTOMATION & CONTROL SYSTEMS

IEC 62443 provides guidance to create Cyber-Resilient IACS

This increased risk-posture results in elevated security requirements by asset owner and operators of IACS. To support the increased security demand with IACS, the International Electrotechnical Commission (IEC) worked on a series of standards that address cybersecurity for operational technology in automation and control systems since 2009: the IEC 62443.As shown in Figure 1 (Scope of the IEC 62443)., IEC 62443 consists of 13 parts – targeting all roles of complex industrial environments: asset owner, system integrator, and product supplier (the vendors of IACS components which can be embedded devices, network components, and host devices). At the core of all parts is to supportdefense-in-depth strategies as well as security by design principles for industrial environments. By adhering to defense-in-depth, reliance on network and perimeter security is insufficient. The de- vices themselves need to withstand cyber-attacks.

Parts IEC 62443-4-1 and IEC 62443-4-2 address security requirements for devices. While IEC 62443-4-2 focuses on product security itself, IEC 62443-4-1 defines requirements towards the product development life- cycle processes. This assures, that a secure product is not a result of lucky circumstances, but repeatable, transparent, and measurable with adequate security controls in place.



Mitigating supply-chain risks is one core requirement of IEC 62443

Figure 2 demonstrates the 8 practices for product development processes defined in IEC 62443-4-1.

The practices pose requirements to all phases of a product development lifecycle to support and assure defense in depth and secure by design during development but also to have all processes in place to manage security related issues through the products lifecycle. One core requirement of IEC 62443-4-1 is to manage supply-chain risk.

Security controls must cover supply-chain too

In modern applications, 80%-90% of the code base is made up of third-party software components – open source as well as proprietary.

These range from crypto-libraries being used to secure sensitive information to closed-source SDKs to control third-party hardware modules included in the IACS. As a majority of the code base is not under direct control of the vendor, a significant share of an IACS' risk and exposure is inherited from third-party software components.

Third-party risks remain hidden

Risks included: Lack of visibility: While direct dependencies and inclusions of third- party components are often known, the supply chain rarely ends there. Third-party components commonly rely on further dependencies, which in turn have dependencies as well. Making the entire supply-chain transparent is even more challenging when the source code of affected components is not available.

Third-party software may increase the thread level

Increase the thread level: Development practices as well as security measurements of vendors of third-party open source and commercial off-the-shelf (COTS) software components are rarely vetted. This results in scenarios where a significant part of the final product does not comply with the vendors' security requirements, which lowers the security posture of the entire IACS environment.

Attackers increasingly focus on supply-chain

Supply chain attacks: Supply chains have moved into the focus of cyber criminals as a lucrative entry-point into their target's infrastructure. Threat actors have started to actively plant backdoors in open-source components and to spread malware via open-source repositories.The severity of supply chain risks justifies rigorous mitigation efforts. The IEC 62443-4-1 acknowledges these challenges and discusses supply- chain risk from different angles in 3 of the 8 practices.

Define security requirement & addressse-curity issues

Practice 1 – security management (SM) contains security requirements for externally provided component (SM-9) and to assess and address security related issues (SM-11). A process must be established to identify third- party providers and assess the associated risks of third-party components taking their role in the product's secure design and defense in depth strategy into account. Additionally, it must be assured that all security-related issues – including such issues that are inherited by third-party dependencies – are addressed prior release.

Test 3rd-party software for vulnerabilieties

Practice 5 – securityverificationand validation testing (SVV) includes requirements for vulnerability testing (SVV-3). Vulnerability testing is required for the entire product including any third-party dependencies. As such, as part of this requirement, also third-party code needs to be tested for known vulnerabilities and configuration issues.

Manage emerging threats

Practice 6 – management of security-related issues (DM) defines requirements for receiving notifications (DM-1), reviewing (DM-2) and assessing security-related issues (DM-3). This includes monitoring of third-party components, which are integrated into the IACS, for security related events to allow for timely impact assessment and remediation.

Integrate automated SBOM into process-es automate SBOM generation & link to known vulnerabilities

The following section delves deeper into those aspects of supply-chain risk and how binary software composition analysis can significantly contribute to automating mitigating controls demanded by IEC 62443-4-1, while reducing manual efforts associated with achieving those requirements at the same time.

Supply chain risk	IEC 62443-4-1 Practice	ONEKEY automation support
Lack of visibility	SM-9: Security requirements for externally provided components	Automated SBOM build & export to CycloneDX /SPDX
Increase the thread level	Sm-11: Assessing and addressing security-related issues	Automated quality gate build-pipeline integration on automated security tests
Vulnerable components	SVV-3: Vulnerability testing	Automated CVE mapping Automated SCA Automated config review Automated compile flag check
Supply-chain attacks	DM-1, DM-2, DM-3 Receiving notifications, reviewing, and assessing security issues	Automated security alerts

Software composition analysis (SCA) describes the automated process of determining the software components (open source and COTS), which are included in a final product. The result of a SCA is a SBOM. As it cannot be assured that source code is available for all software components provided by third parties along the supply-chain, SCA can often only rely on compiled binary representations of a software component.

SM-9: Security requirements for externally provided components

By including binary SCA as part of the process to identify and manage security risks associated with third-party components used within the product, the generation of an inventory of software components from third-party suppliers can be automated. This is achieved by deconstructing the binary firmware to assure that all software components, which will eventually be delivered to the users of IACS, can be identified. Static and dynamic methods can be utilized to build a SBOM by identifying software components, associated versions, as well as applied patches. Based on this information, known vulnerabilities, affecting those software components can be identified and further investigated.

SM-11: Assessing and addressing security-related issues

Implementing an automated security quality gate with binary SCA as part of the release process will assist the process of verifying that a product or product upgrade is not released until its secu- rity-related issues have been mitigated. To identify such issues as early as possible in the software development process, this security quality gate must be integrated into the build process. By automatically failing release pipelines if the identified security issues exceed previously accepted risk levels appropriated to the intended use-cases and security context, it can be assured that security- related issues originating from third-party software are addresses as early as possible.

SVV-3: Vulnerability testing

Performing binary SCA on all executable files to identify known vulnerabilities in the product's software components and libraries is explicitly mentioned as a requirement as part of vulnerability testing.

Additionally, extending SCA by automating analysis of system configuration to highlight misconfigured and insufficiently hardened services, and investigate compiler settings to avoid insecure configurations that foster vulnerabilities can significantly reduce manual efforts and provide a head-start on subsequent penetration tests.

DM-1, DM-2, DM-3: Receiving notifications, reviewing, and assessing security-related issues

Security is not just a one-off effort. It is a process and requires continuous maintenance. Regularly assessing the SBOM of a firmware for newly published vulnerabilities, pro-actively addresses this requirement and supports reviewing and assessing phases of security- related issues by validating applicability to the product and determining impact.

The table summarizes the supply chain risks, the requirements that IEC 62443-4-1 imposes on software development processes of IACS vendors to mitigate these risks, and how ONEKEY's automation for firmware security analysis supports complying with these requirements.

NO SHORTCUT TO IEC 62443 COMPLIANCE!

Stringent security practices as required by IEC 62443-4-1 add significant overhead to existing development life cycles.

Nevertheless, they are a necessity to address today's elevated security requirements and address the ever-increasing threat landscape. Unfortunately, there is - in general - no shortcut to implement IEC 62443 and related compliance.

There are various tools available to improve documentation, processes and cybersecurity. To simplify and support your IEC 62443 implementation, ONEKEY provides expert 's advice and offers consulting resources to support product suppliers.

Check out the key takeaways on the next page and learn how to substantially reduce your efforts during implementation and maintaining compliance with IEC 62443.

ONEKEY 360: CONSULTING AND AUTOMATION

In addition to reducing manual efforts by adding automate controls to processes required by IEC 62443-4-1, ONEKEY aids product suppliers in adopting IEC 62443-4-1 with gap analyses and implementation support.

ONEKEY also offers IEC 62443-4-1 compliant managed services to conduct security verification and validation testing, covering requirements of practice 5, and to manage security-related issues, as required by practice 6, supporting with validation, triage, and impact assessments of reported vulnerabilities.

ONEKEY's technical experts and security researchers are also available to identify gaps to a product's adherence to IEC 62443-4-2 and to conduct penetration tests and vulnerability assessments on IACS applications, embedded devices, network components, and host devices.

KEY TAKE AWAYS

- The goal of IEC 62443-4-1 is to create an environment and basic conditions for products to be developed securely.
- IEC 62443-4-2 on the other hand has concrete security requirements for ICAS devices with the possibility of a device certification.
- With attacks on IACS on the rise, the demand for cyber-
- resilient IACS is increasing. IEC 62443-4-1 provides the toolset to produce such cyber-resilient IACS components, especially from a supply-chain risk's perspective.
- To meet elevated security and compliance requirements and to tackle supply-chain risks, implementation of automated security and compliance controls, i.e. holistic binary software analysis, are required.
- With its automated security checks, the ONEKEY Product Security & Compliance Platform automatically uncovers violations of functional requirements of IEC 62443-4-2 such as strength of password-based authentication, strength of public key-based authentication, or use of unsecure cryptographic functions and many more.

ONEKEY
onekey.com
+49 211 1587 41 04
info@onekey.com

SecurITy made in Germany

V20250500IEN