ISA GLOBAL CYBERSECURITY ALLIANCE

ISASecure®

March 2025

Comparison of ISA/IEC 62443-4-1 and NIST SP 800-218, Secure Software Development Framework

www.isagca.org
www.isasecure.org

1. Summary

This document offers guidance for organizations having established a development process based on the ISA/IEC 62443-4-1[1] standard, *Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements*, to check conformance with the National Institute of Standards and Technology (NIST) SP 800-218[2], Secure Software Development Framework (SSDF).

NIST SP 800-218 addresses the tasks an organization undertakes to ensure the development of well-secured software. It describes a set of fundamental, sound practices for secure software development called the Secure Software Development Framework (SSDF). SSDF focuses on the following secure software development recommendations:

- Ensure that people, processes and technology are prepared to perform secure software development.
- Protect all components of the software from tampering and unauthorized access.
- Produce well-secured software with minimal security vulnerabilities.
- Identify residual vulnerabilities and respond appropriately to address those vulnerabilities and prevent similar ones from occurring in the future.

ISA/IEC 62443-4-1 addresses secure development practices to be applied for a specific product. It specifies process requirements for the secure development of products used in industrial automation and control systems. It defines a secure development lifecycle (SDL) for the purpose of developing and maintaining secure products. This lifecycle includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life.

ISA/IEC 62443-4-1 establishes a comprehensive set of requirements, as opposed to SSDF, which provides light guidance. The scope of these two documents differs in that one can evaluate a single product for conformance to ISA/IEC 62443-4-1 but cannot determine conformance to SSDF by evaluating a single product. However, it is possible to determine if a product was developed by an organization that conforms to SSDF. Likewise, it is possible to determine by examination of several products, whether an organization has implemented the practices of ISA/IEC 62443-4-1. As an example, maintaining a secure component library falls under the scope of SSDF but not of ISA/IEC 62443-4-1. Conformance to this practice is not determined by reviewing a single product.

The comparison of the tasks recommended by SSDF and the practices required by ISA/IEC 62443-4-1 highlights the following commonalities and differences.

Fuller Coverage of SSDF

There is a large overlap between tasks recommended by SSDF and practices required by ISA/IEC 62443-4-1. Of the 42 tasks outlined in SSDF, 36 are fully covered by one or several requirements of

[1] See https://www.isa.org/products/ansi-isa-62443-4-1-2018-security-for-industrial-au.
[2] See https://csrc.nist.gov/pubs/sp/800/218/final.

ISA/IEC 62443-4-1 (see clause 2). Tasks recommended by SSDF are often detailed in several requirements of ISA/IEC 62443-4-1.

Partial Coverage of SSDF

The focus of SSDF on software development practices explains the fact that four of 42 tasks of SSDF are partially covered by ISA/IEC 62443-4-1 (see clause 3). These tasks are not explicitly required by ISA/IEC 62443-4-1 but are implicitly recommended in the rationale and supplemental guidance section of the requirements.

Tasks of SSDF Not Addressed by ISA/IEC 62443-4-1

Two tasks recommended by SSDF are not covered by practices required by ISA/IEC 62443-4-1 (see clause 4). The official commitment of upper management and the creation of a library of well-secured software components are not relevant to the development practices of a single product.

Requirements of ISA/IEC 62443-4-1 Not Addressed by SSDF

The tasks recommended by SSDF are limited to the development phases, as opposed to the scope of ISA/IEC 62443-4-1, which covers the whole lifecycle of a product. Eleven practices required by ISA/IEC 62443-4-1 are relevant for the proper use of the product once it is commercialized (see clause 5). In particular, ISA/IEC 62443-4-1 requests providing updates and guidelines to help users securely integrate and operate the product in an overall system.

2. Tasks of SSDF Fully Covered by ISA/IEC 62443 4-1

Task of SSDF	Full Coverage by ISA/IEC 62443-4-1
PO.1.1: Identify and document all security requirements for the organization's software development infrastructures and processes and maintain the requirements over time.	SM-1 - Development process SM-7 - Development environment security SM-9 - Security requirements for externally provided components SM-12 - Process verification SM-13 - Continuous improvement
PO.1.2: Identify and document all security requirements for organization-developed software to meet and maintain the requirements over time.	SM-12 - Process verification SM-13 - Continuous improvement SR-3 - Product security requirements SR-4 - Product security requirements content SR-5 - Security requirements review SD-4 - Secure design best practices

Task of SSDF	Full Coverage by ISA/IEC 62443-4-1
PO.1.3: Communicate requirements to all third parties who will provide commercial software components to the organization for reuse by the organization's own software. [Formerly PW.3.1]	SM-9 - Security requirements for externally provided components SM-10 - Custom-developed components from third-party suppliers
PO.2.1: Create new roles and alter responsibilities for existing roles as needed to encompass all parts of the SDLC. Periodically review and maintain the defined roles and responsibilities, updating them as needed.	SM-2 - Identification of responsibilities
PO.2.2: Provide role-based training for all personnel with responsibilities that contribute to secure development. Periodically review personnel proficiency and role-based training, and update the training as needed.	SM-4 - Security expertise
PO.3.1: Specify which tools or tool types must or should be included in each toolchain to mitigate identified risks, as well as how the toolchain components are to be integrated with each other.	SM-12 - Process verification SI-2 - Secure coding standards SVV-3 - Vulnerability testing SVV-4 - Penetration testing
PO.3.3: Configure tools to generate artifacts of their support of secure software development practices as defined by the organization.	SM-12 - Process verification SI-2 - Secure coding standards SVV-3 - Vulnerability testing
PO.4.1: Define criteria for software security checks and track throughout the SDLC.	SI-1 - Security implementation review SI-2 - Secure coding standards SVV-3 - Vulnerability testing
PO.4.2: Implement processes, mechanisms, etc. to gather and safeguard the necessary information in support of the criteria.	SI-1 - Security implementation review SVV-1 - Security requirements testing SVV-2 - Threat mitigation testing SVV-3 - Vulnerability testing SVV-4 - Penetration testing

Task of SSDF	Full Coverage by ISA/IEC 62443-4-1
PO.5.1: Separate and protect each environment involved in software development.	SM-7 - Development environment security SVV-5 - Independence of testers
PS.1.1: Store all forms of code – including source code, executable code, and configuration-as-code – based on the principle of least privilege so that only authorized personnel, tools, services, etc. have access.	SM-6 - File integrity SM-7 - Development environment security SM-8 - Controls for private keys
PS.2.1: Make software integrity verification information available to software acquirers.	SM-6 - File integrity SM-8 - Controls for private keys
PS.3.1: Securely archive the necessary files and supporting data (*e.g.*, integrity verification information, provenance data) to be retained for each software release.	SM-6 - File integrity SM-7 - Development environment security
PS.3.2: Collect, safeguard, maintain, and share provenance data for all components of each software release (*e.g.*, in a software bill of materials [SBOM]).	SM-9 - Security requirements for externally provided components SM-10 - Custom-developed components from third-party suppliers
PW.1.1: Use forms of risk modeling – such as threat modeling, attack modeling, or attack surface mapping – to help assess the security risk for the software.	SM-4 - Security expertise SM-11 - Assessing and addressing security-related issues SR-1 - Product security context SR-2 - Threat model SD-1 - Secure design principles
PW.1.2: Track and maintain the software's security requirements, risks, and design decisions.	SM-11 - Assessing and addressing security-related issues SR-3 - Product security requirements SR-4 - Product security requirements content SR-5 - Security requirements review SD-1 - Secure design principles
PW.1.3: Where appropriate, build in support for using standardized security features and services (e.g., enabling software to integrate	SD-1 - Secure design principles SD-4 - Secure design best practices

Task of SSDF	Full Coverage by ISA/IEC 62443-4-1
with existing log management, identity management, access control, and vulnerability management systems) instead of creating proprietary implementations of security features and services. [Formerly PW.4.3]	SI-2 - Secure coding standards
PW.2.1: Have 1) a qualified person (or people) who were not involved with the design and/or 2) automated processes instantiated in the toolchain review the software design to confirm and enforce that it meets all of the security requirements and satisfactorily addresses the identified risk information.	SM-2 - Identification of responsibilities SM-11 - Assessing and addressing security-related issues SR-2 - Threat model SR-5 - Security requirements review SD-3 - Security design review SD-4 - Secure design best practices SI-2 - Secure coding standards
PW.4.1: Acquire and maintain well-secured software components (*e.g.*, software libraries, modules, middleware, frameworks) from commercial, open-source, and other third-party developers for use by the organization's software.	SM-9 - Security requirements for externally provided components SM-10 - Custom-developed components from third-party suppliers
PW.4.4: Verify that acquired commercial, open-source, and all other third-party software components comply with the requirements, as defined by the organization, throughout their life cycles.	SM-9 - Security requirements for externally provided components SM-10 - Custom-developed components from third-party suppliers SI-1 - Security implementation review DM-1 - Receiving notifications of security-related issues
PW.5.1: Follow all secure coding practices that are appropriate to the development languages and environment to meet the organization's requirements.	SI-1 - Security implementation review SI-2 - Secure coding standards
PW.6.1: Use compiler, interpreter, and build tools that offer features to improve executable security.	SI-1 - Security implementation review SI-2 - Secure coding standards

Task of SSDF	Full Coverage by ISA/IEC 62443-4-1
PW.6.2: Determine which compiler, interpreter, and build tool features should be used and how each should be configured, then implement and use the approved configurations.	SI-1 - Security implementation review SI-2 - Secure coding standards
PW.7.1: Determine whether code review (a person looks directly at the code to find issues) and/or code analysis (tools are used to find issues in code, either in a fully automated way or in conjunction with a person) should be used, as defined by the organization.	SM-5 - Process scoping SI-1 - Security implementation review SVV-1 - Security requirements testing
PW.7.2: Perform the code review and/or code analysis based on the organization's secure coding standards, and record and triage all discovered issues and recommended remediations in the development team's workflow or issue tracking system.	SI-1 - Security implementation review SI-2 - Secure coding standards SVV-1 - Security requirements testing SVV-2 - Threat mitigation testing
PW.8.1: Determine whether executable code testing should be performed to find vulnerabilities not identified by previous reviews, analysis, or testing and, if so, which types of testing should be used.	SVV-1 - Security requirements testing SVV-2 - Threat mitigation testing SVV-3 - Vulnerability testing SVV-4 - Penetration testing SVV-5 - Independence of testers
PW.8.2: Scope the testing, design the tests, perform the testing, and document the results, including recording and triaging all discovered issues and recommended remediations in the development team's workflow or issue tracking system.	SM-5 - Process scoping SM-13 - Continuous improvement SI-1 - Security implementation review SVV-1 - Security requirements testing SVV-2 - Threat mitigation testing SVV-3 - Vulnerability testing SVV-4 - Penetration testing SVV-5 - Independence of testers

Task of SSDF	Full Coverage by ISA/IEC 62443-4-1
PW.9.1: Define a secure baseline by determining how to configure each setting that has an effect on security or a security-related setting so that the default settings are secure and do not weaken the security functions provided by the platform, network infrastructure, or services.	SD-1 - Secure design principles SD-4 - Secure design best practices SVV-1 - Security requirements testing SG-1 - Product defense-in-depth SG-3 - Security hardening guidelines
PW.9.2: Implement the default settings (or groups of default settings, if applicable), and document each setting for software administrators.	SG-3 - Security hardening guidelines SG-6 - Account management guidelines
RV.1.1: Gather information from software acquirers, users, and public sources on potential vulnerabilities in the software and third-party components that the software uses, and investigate all credible reports.	DM-1 - Receiving notifications of security-related issues DM-2 - Reviewing security-related issues DM-3 - Assessing security-related issues
RV.1.2: Review, analyze, and/or test the software's code to identify or confirm the presence of previously undetected vulnerabilities.	SI-1 - Security implementation review SVV-2 - Threat mitigation testing SVV-3 - Vulnerability testing SVV-4 - Penetration testing DM-1 - Receiving notifications of security-related issues DM-2 - Reviewing security-related issues
RV.1.3: Have a policy that addresses vulnerability disclosure and remediation, and implement the roles, responsibilities, and processes needed to support that policy.	DM-1 - Receiving notifications of security-related issues DM-2 - Reviewing security-related issues DM-3 - Assessing security-related issues DM-4 - Addressing security-related issues DM-5 - Disclosing security-related issues
RV.2.1: Analyze each vulnerability to gather sufficient information about risk to plan its remediation or other risk response.	SM-11 - Assessing and addressing security-related issues DM-2 - Reviewing security-related issues DM-3 - Assessing security-related issues

Task of SSDF	Full Coverage by ISA/IEC 62443-4-1
RV.2.2: Plan and implement risk responses for vulnerabilities.	SM-11 - Assessing and addressing security-related issues DM-4 - Addressing security-related issues
RV.3.1: Analyze identified vulnerabilities to determine their root causes.	DM-3 - Assessing security-related issues
RV.3.4: Review the SDLC process and update it if appropriate to prevent (or reduce the likelihood of) the root cause recurring in updates to the software or in new software that is created.	SM-13 - Continuous improvement DM-6 - Periodic review of security defect management practice

3. Tasks of SSDF Partially Covered by ISA/IEC 62443 4-1

Task of SSDF	Partial Coverage by ISA/IEC 62443-4-1
PO.3.2: Follow recommended security practices to deploy, operate, and maintain tools and toolchains.	SM-7 - Development environment security SI-2 - Secure coding standards

Rationale:
Although ISA/IEC 62443-4-1 recommends following best practices for all activities of SDL, it does not explicitly request to follow best practices for the deployments, operation and maintenance of tools.

Task of SSDF	Coverage by ISA/IEC 62443-4-1
PO.5.2: Secure and harden development endpoints (*i.e.*, endpoints for software designers, developers, testers, builders, etc.) to perform development-related tasks using a risk-based approach.	SM-6 - File integrity SM-7 - Development environment security

Rationale:
Although ISA/IEC 62443-4-1 requests protecting the development environment and the integrity of all product-related files, it does not explicitly request or recommend protecting the endpoints used in the SDL.

Task of SSDF	Coverage by ISA/IEC 62443-4-1
RV.3.2: Analyze the root causes over time to identify patterns, such as a particular secure coding practice not being followed consistently.	SD-4 - Secure design best practices SI-2 - Secure coding standards DM-4 - Addressing security-related issues

Rationale:
Although 62443-4-1 recommends applying lessons learned, it does not explicitly request or recommend identifying patterns.

Task of SSDF	Coverage by ISA/IEC 62443-4-1
RV.3.3: Review the software for similar vulnerabilities to eradicate a class of vulnerabilities, and proactively fix them rather than waiting for external reports.	SI-1 - Security implementation review DM-3 - Assessing security-related issues DM-4 - Addressing security-related issues

Rationale:
Although 62443-4-1 recommends applying lessons learned, it does not explicitly request or recommend reviewing the product design for similar vulnerabilities.

4. Tasks of SSDF Not Covered by ISA/IEC 62443 4-1

Task of SSDF
PO.2.3: Obtain upper management or authorizing official commitment to secure development, and convey that commitment to all with development-related roles and responsibilities.

Rationale:
ISA/IEC 62443-4-1 does not request official commitment from management, as it is a prerequisite to execute the practices of a secure product development lifecycle.

Task of SSDF
PW.4.2: Create and maintain well-secured software components in-house following SDLC processes to meet common internal software development needs that cannot be better met by third-party software components.

Rationale:
Although it is a commonly accepted best practice to create a library of internally developed SW components, ISA/IEC 62443-4-1 does not explicitly request or recommend creating such a library, as it is about what should be done for a specific product.

5. Practices of ISA/IEC 62443 4-1 Not Requested by SSDF

SM-3	Identification of applicability
SD-2	Defense in depth design
SUM-1	Security update qualification
SUM-2	Security update documentation
SUM-3	Dependent component or operating system security update documentation
SUM-4	Security update delivery
SUM-5	Timely delivery of security patches
SG-2	Defense-in-depth measures expected in the environment
SG-4	Secure disposal guidelines
SG-5	Secure operation guidelines
SG-7	Documentation review

Rationale:
SSDF defines tasks for the secure development of software. The document does not consider the content and the scope of application of the software. Except for the security configuration, SSDF does not require to generate user documentation for integrating the software in an overall system.

The scope of ISA/IEC 62443-4-1 covers the practices for the development and support of a product used in an overall industrial automation and control system (IACS) and its contribution to a defense-in-depth strategy of the IACS. The requirements are based on the product's intended use and operational environment.

Furthermore, ISA/IEC 62443-4-1 requires supporting users of the product along the phases of the IACS. This includes providing guidelines for integrating and operating the product and providing updates and patches as necessary.

About

International Society of Automation

The International Society of Automation (ISA) is a non-profit professional association founded in 1945 to create a better world through automation. ISA's mission is to empower the global automation community through standards and knowledge sharing. ISA develops widely used global standards and conformity assessment programs; certifies professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its members and customers around the world.

ISA develops the ISA/IEC 62443 series[3], the world's leading consensus-based automation and control systems cybersecurity standards. Learn more at www.isa.org.

ISA GLOBAL CYBERSECURITY ALLIANCE

The ISA Global Cybersecurity Alliance (ISAGCA) is a collaborative forum to advance OT cybersecurity awareness, education, readiness, standardization and knowledge sharing.

ISAGCA is made up of 50+ member companies and industry groups, representing more than $1.5 trillion in aggregate revenue across more than 2,400 combined worldwide locations. Automation and cybersecurity provider members serve 31 different industries, underscoring the broad applicability of the ISA/IEC 62443 series of standards. Learn more at www.isagca.org.

ISASecure

Founded in 2007 by the International Society of Automation (ISA), the ISASecure program's mission is to provide the highest level of assurance possible for the cybersecurity of automation and control systems.

Founders and key supporters of ISASecure® include: BP, Chevron, ExxonMobil, Saudi Aramco, Shell, YPF, GSK, Honeywell, Johnson Controls, Schneider Electric, Trane, Yokogawa, Carrier, Siemens, YPF, Amazon Web Services, exida, TUV Rheinland, CSSC, FM Approvals, Synopsys, Trust CB, UL Solutions, SecurityGate, Interstates, BYHON, TUV SUD, ITRI and Bureau Veritas.

The program's ISASecure designation signifies to the marketplace that automation and control system products conform to industry-consensus cybersecurity standards. The ISASecure trademark provides confidence to users of ISASecure-certified products and systems and creates product differentiation for suppliers who conform to the ISASecure specifications. Learn more at www.isasecure.org.

[3] See www.isa.org/62443standards.

