ISASecure®

The Case for ISA/IEC 62443 Security Level 2 as a Minimum for COTS Components

February 2024

www.ISASecure.org

Table of Contents

0 Introduction 4

0.1 Purpose 4

0.2 Scope 5

0.3 Background 5

1 FR 1 - Identification and authentication control 8

2 FR 2 - Use control 10

3 FR 3 - System integrity 12

4 FR 4 - Data confidentiality 16

5 FR 5 - Restricted data flow 17

6 FR 6 - Timely response to events 18

7 FR 7 - Resource availability 19

8 FR 8 - Summary 20

8.1 Individual user identification, authentication and accountability 20

8.2 Software process and device identification, authentication and accountability 21

8.3 Authenticity checks 21

8.4 Physical access protection 22

9 Security capability level conformance 22

10 Product supplier benefits and implementation 22

10.1 Benefits 22

10.2 Implementation 23

Annex A 23

The Case for ISA/IEC 62443 Security Level 2 as a Minimum for COTS Components

Executive Summary

The purpose of this paper is to recommend that industrial control system components using the widely accepted security standard ISA/IEC 62443-4-2, target conformance to a minimum of security level 2 (SL2), as defined in that standard. The analysis presented here makes the case that SL2 capabilities are necessary for adequate security in this domain, even though the standard also defines a security level 1 (SL1) with fewer requirements. This paper has been developed by the ISA Security Compliance Institute (ISCI), an organization that represents asset owners, product suppliers and certification bodies. ISCI created the ISASecure certification program, an international commercial-off-the-shelf (COTS) product cybersecurity certification program based on the ISA/IEC 62443 standard. The intended audience for this paper is asset owners, product suppliers, system integrators and others in the industrial control system community who provide advice or determine security requirements for off-the-shelf products or for individual control system installations.

The reason for this recommendation is that the definition for SL1 prescribes capabilities to protect components from coincidental or casual access, misuse or manipulation of the component. In particular, SL1 capabilities do not address intentional attacks. SL2 adds additional security capabilities generally recognized to help mitigate well known attack scenarios.

Today, an increasing number of intentional attacks are being detected that target industrial automation and control systems, indicating the need for such additional mitigations. For example, the SL2 criteria strengthen the security capabilities of components by requiring that a component:

- Uniquely distinguish between individual human or non-human users interacting with the component, increasing the ability to trace the source for user activity that may constitute an attack
- Authenticate itself to an overall system into which it has been integrated, raising the level of trust between the system and component
- Provide the ability to tailor human role definitions to reflect site operations, limiting unnecessary insider access
- Close inactive communication sessions that remain open as potential attack vectors

- Verify the source of communications to the component, limiting sources for network attacks
- Protect test interfaces from use as potential attack vectors
- Increase assurance that code in execution, including mobile code, updates and upgrades came from a trusted source and has not been subject to tampering.

This paper provides a review of the additional security functionality that industrial automation and control system (IACS) components designed and certified to meet ISA/IEC 62443-4-2 SL2 capabilities must exhibit. This includes review of how those additional capabilities increase the security resiliency of the component, as well as the security of any system into which the component is integrated.

Secure interfaces between industrial control system (ICS) components and on-premises and cloud systems provide many benefits including increased productivity and more effective preventative maintenance. These systems are based on IT technologies that commonly support many of the above security capabilities. Securing such interfaces requires interoperable security approaches, which may not always be achievable using SL1 components. For example, a control system may have the capability to authenticate communicating devices, but using this capability requires those communicating devices to interoperate, using an authentication method supported by the system.

0 Introduction

0.1 Purpose

The purpose of this paper is to recommend that industrial control system components using the widely accepted security standard ISA/IEC 62443-4-2, target conformance to a minimum of SL2, as defined in that standard.

In support of this recommendation, the paper[1] provides a review of the additional security functionality that IACS components designed and certified to meet ISA/IEC 62443-4-2 SL2 capabilities must exhibit. This includes a review of how those additional capabilities increase the security resiliency of the component, as well as the security of any system into which the component is integrated, beyond baseline SL1 capabilities.

ISA/IEC 62443-4-2 SL1 capabilities have been instrumental in raising the bar from a lack of embedded security capabilities to the standardized minimum expected embedded security capabilities in IACS components today. However, SL1 capabilities are often generic and not intended to protect against intentional violations but rather address casual violations, as explicitly stated in the standard.

A drawback of some SL1 baseline capabilities is that their definition is generic, such that they can be implemented in many different and possibly outdated ways, affecting the interoperability of components although designed and certified for SL1.

1 This document is an interpretation of the ISA/IEC 62443 standard to facilitate understanding and application of the standard. It is not a product of the ISA99 committee that develops the standard, and as such may not represent the views of the committee.

SL2 capabilities not only raise the protection level by providing additional security functionality, but also enhance SL1 capabilities, narrowing down disparities and increasing security resiliency. More importantly, SL2 introduces security capabilities common in today's IT environments but less common in operational technology (OT) environments. Enabling those capabilities requires developing and maturing the right competencies for asset owners, system integrator service providers and product supplier organizations.

0.2 Scope

The review starts with a background overview of security capability levels and how security levels are defined.

This paper concentrates on reviewing the incremental SL2 capabilities above SL1 baseline capabilities to highlight their differences and advantages. Thus, the scope of this review includes both SL2 additional base requirements and SL2 requirement enhancements in the ISA/IEC 62443-4-2 standard as described in the background section. Review of baseline SL1 capabilities or of the underlying secure development lifecycle practices described in ISA/IEC 62443-4-1 that ISA/IEC 62443-4-2 requires for all security levels, is not in the scope of this paper.

The paper makes the case that SL2 capabilities are necessary to protect an IACS. A discussion of the conditions under which SL3 or SL4 capabilities would also be recommended is not in scope for this paper.

The following description of additional security capabilities and enhancements is organized by Foundational Requirement sets in sections 1 to 7. Section 8 provides a summary with examples of risks that can be mitigated using SL2 components; section 9 provides some of the advantages to product suppliers who design and maintain SL2 components, and section 10 provides a summary and discussion of how asset owners can be assured that the components they procure meet SL2 security requirements.

0.3 Background

The ISA/IEC 62443-4-2 standard defines the technical cybersecurity capability requirements for IACS components. The standard is titled "Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components."

The standard defines IACS components as embedded devices, network devices, host devices and software applications. The technical security requirements define cybersecurity capabilities to be included in the four types of components. The requirements are organized by the seven foundational requirements of the ISA/IEC 62443 series. Most security requirements apply to all components, so they are designated component requirements or CRs. When requirements are specific to a component type, they are designated as EDR for embedded devices, HDR for host devices, NDR for network devices and SAR for software applications.

The standard organizes the requirements by security capability level. The security capability level is defined as security levels 1 through 4. The four security levels address an increasing level of risk of a cybersecurity incident based on the abilities of a cybersecurity attacker, where:

- SL1 prescribes capabilities to protect components from coincidental or casual access, misuse or manipulation of the component.
- SL2 prescribes capabilities to protect components from intentional cybersecurity attacks by an attacker with low resources, generic skills and low motivation.
- SL3 prescribes capabilities to protect components from intentional cybersecurity attacks by an attacker with moderate resources, industrial control system-specific skills and moderate motivation.
- SL4 prescribes capabilities to protect components against attackers with extended resources and high motivation.

The standard has two types of requirements: the base requirement and requirement enhancements. Requirement enhancements strengthen the base requirements and are required in addition to the base requirement. A requirement enhancement will never be a stand-alone requirement but will always be an enhancement to a base requirement.

Figure 1 shows the relationship between security levels, base requirements and requirement enhancements. Notice that the security levels are compounded. As the security level increases, the number of security requirements increases by adding requirements to the previous security levels. This increase will be in the form of additional base requirements and requirement enhancements to base requirements required by lower security levels. SL1 establishes the set of baseline requirements required for all security levels. SL2 adds both base requirements and requirement enhancements; SL3 adds additional base requirements and requirement enhancements, as does SL4.

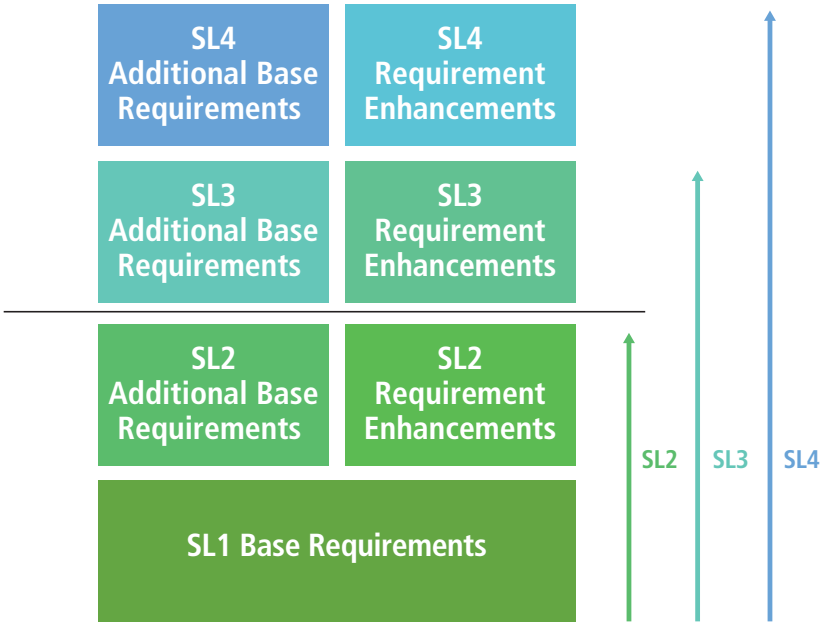

Figure 1 - Security Levels Structure

A common question that asset owners and product suppliers frequently have relates to the incremental effort required, in terms of number of requirements to meet SL2 capabilities. Figure 2 illustrates the number of requirements required for each of the security levels. There are 50 requirements associated with SL1, the baseline security level. As the security level is increased to SL2, Figure 2 shows an addition of 22 new base requirements and 21 requirement enhancements to the SL1 baseline requirements. Those interested in the distribution of requirements based on Foundational Requirement areas, please refer to Figure 10 in Annex A.

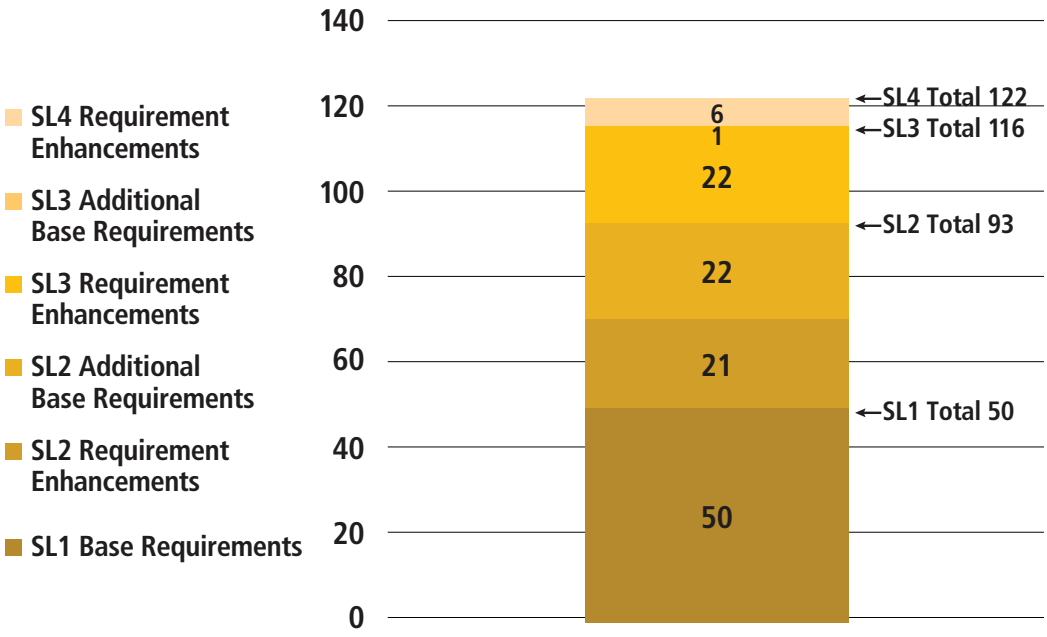

Figure 2 - Distribution of the number of requirements by Security Level

1 FR 1 - Identification and authentication control

The purpose of the identification and authentication control foundational requirement is to identify and authenticate all users (humans, software processes and devices), prior to allowing them access to the system or assets. As shown in Figure 3, there are ten baseline requirements at SL1. SL2 adds two requirement enhancements and four new base requirements.

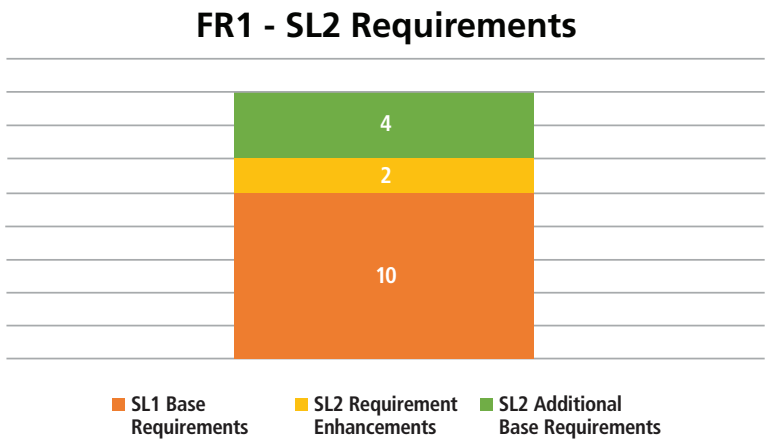

Figure 3 - Number of SL2 Requirements in FR 1

The requirements added for SL2 capability are shown in the table below. Requirement enhancements, shown in the first column, are to enhance the capabilities already present for SL1. SL2 then further requires additional base requirements, shown in the second column.

SL2 Requirement Enhancements (RE)	SL2 Additional Base Requirements
CR 1.1 RE 1 Unique human user identification and authentication	CR 1.2 Software process and device identification and authentication
NDR 1.6 RE 1 Unique identification and authentication of wireless users and devices	CR 1.8 Usage of public key infrastructure certificates
	CR 1.9 Strength of public key-based authentication
	CR 1.14 Strength of symmetric key-based authentication

CR 1.1 RE 1 Unique human user identification and authentication: This requirement enhancement can be a little confusing since the SL1 base requirement can be read to imply that a unique identification and authentication is needed for each human user; it states that human user identification and authentication is required to support segregation of duties and least privilege. It is important to note that the base requirement is silent on the need for

individual human user identification to support the segregation of duties and least privilege; thus, the base requirement can be met with the implementation of accounts that are assigned to roles and all personnel assigned to that role would share that same account. Therefore, a component that contains SL1 capabilities might not support identification and authentication of individual users, and as a result, any system with components with SL1-only capabilities might not be able to meet the requirement for non-repudiation since individual users may not be identifiable at the device level.

CR 1.2 Software process and device identification and authentication: This capability allows the component to identify and authenticate with the system into which the component is integrated. Without this capability in the component, the system ends up explicitly trusting all components, making it much easier for attackers to impersonate components without the system being aware of that impersonation. Typically, components will satisfy this requirement by having signed certificates installed by the product supplier at the time of manufacture. The product supplier then provides a public version of the signing key to certificate authorities, which can then be used to validate that the device is authentic by validating the signed certificate installed into the component. There is a second approach for authenticating components by installing a symmetric key into the component at the time of commissioning the component into the system. The second approach provides a means for authenticating the component with the system, but the component's authenticity is left to the commissioning steps before installing the symmetric key into the component. While this second approach meets the requirement, the first approach both meets the requirement and adds proof that the component is an authentic component that the product supplier manufactured. There are other ways to meet this requirement, but the two discussed here are the most popular.

NDR 1.6 RE 1 Unique identification and authentication of wireless users and devices: The requirement enhancement states that the network device shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication. This requirement enhancement is similar to CR 1.1 RE 1 with the addition of uniquely identifying all users engaged in wireless communication. This implies that the base NDR 1.6 requirement for SL1 may allow users to have a shared account.

CR 1.8 Usage of public key infrastructure certificates, CR 1.9 Strength of public key-based authentication and CR 1.14 Strength of symmetric key-based authentication: These requirements are necessary companions to the CR 1.2 requirement, which requires components and software processes to identify themselves and authenticate with the system using them. For components that use product supplier-installed and signed certificates to identify with the system, the requirements for using public key infrastructure certificates and the strength of public key-based authentication are necessary to assure that the device is authentic and can authenticate with the system. The requirement for strength of symmetric key-based authentication is necessary for components that use symmetric keys for authentication.

2 FR 2 - Use control

The purpose of the use control foundational requirement is to enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the component and monitor the use of these privileges. As shown in Figure 4 there are twelve SL1 baseline requirements. SL2 adds seven requirement enhancements and four new base requirements.

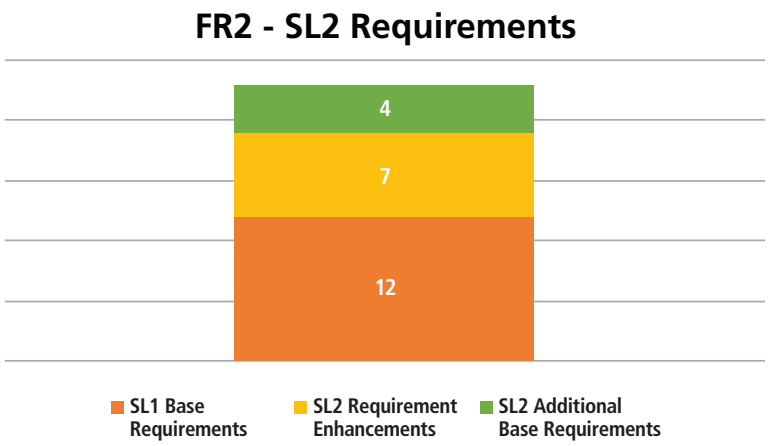

Figure 4 - Number of SL2 Requirements in FR 2

The requirements added for SL2 capability are shown in the table below.

SL2 Requirement Enhancements (RE)	SL2 Additional Base Requirements
CR 2.1 RE 1 Authorization enforcement for all users (humans, software processes and devices)	CR 2.6 Remote session termination
CR 2.1 RE 2 Permission mapping to roles	EDR 2.13 Use of physical diagnostic and test interfaces
SAR 2.4 RE 1 Mobile code authenticity check	HDR 2.13 Use of physical diagnostic and test interfaces
EDR 2.4 RE 1 Mobile code authenticity check	NDR 2.13 Use of physical diagnostic and test interfaces
HDR 2.4 RE 1 Mobile code authenticity check	
NDR 2.4 RE 1 Mobile code authenticity check	
CR 2.11 RE 1 Time synchronization	

CR 2.6 Remote session termination: This requirement states that if a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time of inactivity, manually by a local authority or manually by the user (human, software process or device) who initiated the session. Since this is an SL2 requirement, SL1 components that support remote sessions may leave those sessions open indefinitely, leaving the component vulnerable to malicious activity through the open remote session. SL2 components provide the capability for remote sessions to be terminated due to inactivity, making the component less vulnerable to abuse through remote sessions.

EDR 2.13, HDR 2.13 and NDR 2.13 Use of physical diagnostic and test interfaces: These requirements apply when the embedded device, host device or network device is embodied in physical hardware. These interfaces are usually used during the manufacturing and testing of the device and remain in place in deployed devices. A Joint Test Action Group (JTAG) interface is one example of this type of interface. These requirements require that devices protect against unauthorized use of the physical factory diagnostic and test interface(s). SL1 devices are not required to meet this requirement. Although exploitation of this interface usually requires physical access, this physical access could be obtained anywhere in the supply chain between the manufacture and the deployment of the device, resulting in possible exploitation of the device.

CR 2.1 RE 1 Authorization enforcement for all users (humans, software processes and devices): This is the first of two SL2 requirement enhancements to SL1 CR 2.1, requiring components to provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege. This requirement enhancement requires that, in addition to human users, all software processes and devices identified and authenticated are subject to authorization enforcement of any actions. For software processes and devices to be subjected to authorization enforcement, they must be identified and authenticated with the system. For that to occur, those software processes and devices will have to meet the CR 1.2 requirement, which is also an SL2 capability requirement. If any software processes or components in the system do not conform to SL2 or higher, then there will be no authorization enforcement for those software processes and devices. This could leave a system vulnerable to unauthorized actions by unauthorized software processes or devices.

CR 2.1 RE 2 Permission mapping to roles: This is the second requirement enhancement to the CR 2.1 SL1 baseline required to meet SL2 capability. There is a note to this requirement enhancement stating that the requirement enhancement should apply to software processes and devices as well as human users. Components that do not have this capability may have preconfigured and unchangeable permissions for roles. Components that meet this requirement will have a separately defined role for mapping permissions to roles accessing and using the component. Thus, SL1 components may be unable to support asset owner-defined permissions for asset owner-defined roles.

SAR 2.4 RE1, EDR 2.4 RE 1, HDR 2.4 RE 1 and NDR 2.4 RE 1 Mobile code authenticity check: These four requirement enhancements add to the SL1 baseline CR 2.4 requirement that software applications, embedded devices, host devices and network devices must provide the capability to enforce a

security policy that allows the component to control the execution of mobile code based on the results of an authenticity check before the code is executed. Meeting this requirement assures that any executed mobile code is determined to be authentic code from the supplier that created it. SL1 components are not required to provide this authenticity check which might allow the execution of mobile code that might have been tampered with from the time of creation by the supplier until the time of execution on the system. This requirement depends on other SL2 requirements related to public key infrastructure (PKI) certificates and the certificate chain associated with them.

CR 2.11 RE 1 Time synchronization: This final requirement enhancement adds to the CR 2.11 SL1 baseline requirement that components must provide the capability to create timestamps that are synchronized with a system-wide time source. Without this capability in the components, the timestamps will be local to each component and could be significantly different. This makes individual component logs less useful for forensics purposes.

3 FR 3 - System integrity

The purpose of the system integrity foundational requirement is to ensure the integrity of the component to protect against unauthorized manipulation or modification. As shown in Figure 5, there are sixteen baseline security requirements at SL1. SL2 adds nine requirement enhancements and eleven new base requirements. The system integrity foundational requirement area has the most additional requirements for SL2 capability.

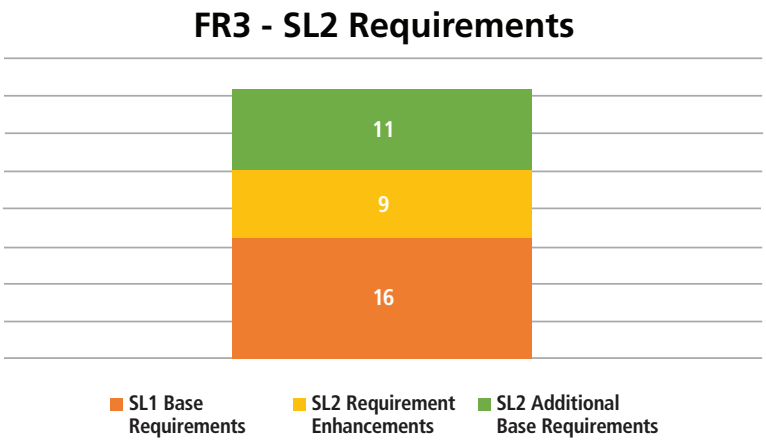

Figure 5 - Number of SL2 Requirements in FR 3

The requirements added for SL2 capability are shown in the table below.

SL2 Requirement Enhancements (RE)	SL2 Additional Base Requirements
CR 3.1 RE 1 Communication authentication	CR 3.8 Session integrity
HDR 3.2 RE 1 Report version of code protection	CR 3.9 Protection of audit information
CR 3.4 RE 1 Authenticity of software and information	EDR 3.11 Physical tamper resistance and detection
EDR 3.10 RE 1 Update authenticity and integrity	HDR 3.11 Physical tamper resistance and detection
HDR 3.10 RE 1 Update authenticity and integrity	NDR 3.11 Physical tamper resistance and detection
NDR 3.10 RE 1 Update authenticity and integrity	EDR 3.12 Provisioning product supplier roots of trust
EDR 3.14 RE 1 Authenticity of the boot process	HDR 3.12 Provisioning product supplier roots of trust
HDR 3.14 RE 1 Authenticity of the boot process	NDR 3.12 Provisioning product supplier roots of trust
NDR 3.14 RE 1 Authenticity of the boot process	EDR 3.13 Provisioning asset owner roots of trust
	HDR 3.13 Provisioning asset owner roots of trust
	NDR 3.13 Provisioning asset owner roots of trust

CR 3.1 RE 1 Communication authentication: This is a requirement enhancement to the CR 3.1 communication integrity SL1 base requirement. The base requirement requires that components provide the capability to protect the integrity of transmitted information. The requirement enhancement added at SL2 requires that components provide the capability to verify the authenticity of received information during communication. The best means for verifying the authenticity of communications is to require that components communicating with each other first need to authenticate with each other and negotiate how they will securely communicate as part of the identification and authentication process. Without this authentication between components, well-known network-based attacks such as man-in-the-middle attacks are possible. SL2 components provide an additional layer of authentication that helps mitigate these types of attacks.

HDR 3.2 RE 1 Report version of code protection: All SL1 components are required to provide protection from malicious code. When the component is a host device, this requirement enhancement requires that host devices provide the capability to automatically report the software and file versions of the malicious code protection in use (as part of the overall logging function). Thus, an SL2 host device allows for system-level monitoring of the version of malicious code protection on that device and may also allow for centralized management of that protection. Without this capability the version of code protection has to be manually checked on all host devices, delaying the ability to quickly deploy more up to date code protection across large systems.

CR 3.4 RE 1 Authenticity of software and information: All components have a requirement to either provide the capability to perform or support *integrity checks* on software, configuration and other information; or to be integrated into a system that can perform or support integrity checks as defined in CR 3.4 for SL1. RE 1 for SL2 adds the requirement enhancement that components must also provide either the capability to perform or support *authenticity checks* on software, configuration and other information; or to be integrated into a system that can perform or support *authenticity checks*. *Authenticity checks* provide an extra layer of security beyond the *integrity checks* on software. This additional layer is typically implemented by digitally signing the software, making it much harder for a malicious attacker to modify the software by injecting malicious code into it. Without the digital signature of the software, it is much simpler for a malicious agent or user to modify the software between the time of manufacture and time of use, recalculate the *integrity check* value and replace that value in the software and place where that *integrity check* value is posted. Digitally signing is done using a private key at the time of manufacture and a public key at the time of the *authenticity check*. To provide the security of the digitally signed software, the private key used by the product supplier must be protected from compromise. This also includes the root key that might be used to sign the public/private key pair that is part of the digital signing and verification process. Product supplier protection of their private root key and signing key is validated through the certification process of the product supplier's security development lifecycle for conformance to ISA/IEC 62443-4-1, which is required for any component to be certified for conformance to ISA/IEC 62443-4-2. Without this assurance that product suppliers are appropriately protecting their signature keys, there can be no real authenticity checks of software or devices.

EDR 3.10 RE 1, HDR 3.10 RE 1 and NDR 3.10 RE 1 Update authenticity and integrity: Components need to be periodically updated or upgraded. Examples of updates include corrections of security vulnerabilities, corrections of software anomalies and software bugs, while upgrades primarily modify features and functions. There is a set of SL1 base requirements, EDR 3.10 for embedded devices, HDR 3.10 for host devices and NDR 3.10 for network devices to support updates and upgrades. These three SL2 requirement enhancements require that components must validate the authenticity and integrity of any software update or upgrade prior to installation. This means that although SL1 components must have the capability to be updated and upgraded, they may not check to see if the update or upgrade is authentic and has not been tampered with prior to installation. This may leave SL1 components vulnerable to malicious updates or upgrades.

EDR 3.12, HDR 3.12 and NDR 3.12 Provisioning product supplier roots of trust: The keys that are used to validate the authenticity of software and devices, which use certificates to meet the identification and authentication requirement, are validated using product supplier public keys that can be validated to a root of trust. Since many control system components cannot communicate with the internet to perform this validation, those roots of trust must be installed into the components, which is the purpose of these SL2 base requirements. These three SL2 additional requirements require that components must provide the capability to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data used as one or more "roots of trust" at the time of manufacture of the device. All the SL2 requirements which require authenticity checks will depend on the root of trust from the product supplier being part of the component.

EDR 3.13, HDR 3.13 and NDR 3.13 Provisioning asset owner roots of trust: This is a companion requirement to that for the *product supplier* root of trust, applicable to asset owner roots of trust. Where asset owner keys may be used in a deployed system, this requirement is necessary to assure that those asset owner keys are authentic. This requirement is slightly different from that for the product supplier root of trust. *Asset owner* roots of trust need to be installed into the component as part of the component's deployment into the asset owner system. At the same time, *product supplier* roots of trust would typically be installed into the component at manufacture. *Asset owner* keys might be used to meet the requirement for authentic communications in the system using asset owner-generated keys.

EDR 3.14 RE 1, HDR 3.14 RE 1 and NDR 3.14 RE 1 Authenticity of the boot process: The SL1 baseline requirements of these SL2 requirement enhancements require components to provide the capability to *verify the integrity* of the firmware, software and configuration data needed for the component's boot prior to use. These SL2 requirement enhancements require components to in addition provide the capability to *verify the authenticity* of the boot firmware, software and configuration data prior to booting up the component. This authenticity check is also dependent on the product supplier roots of trust installed into the component. Components that meet both the SL1 baseline requirement and the SL2 requirement enhancement can be considered trusted components in the environment in which they are operating. Trusted in this context means that the component is determined to be authentic. Authentic means the device and software have not been modified from the time of manufacture to the time of use and there is a very high level of assurance that the manufacture of the device and the software was done by the product supplier.

CR 3.8 Session integrity: This SL2 additional base requirement requires that components provide mechanisms to protect the integrity of communications sessions. The primary purpose of this requirement is to protect against communication attacks on the network, such as network replay attacks and session hijacking attacks. To do this, the requirement states that the mechanisms to protect the integrity of communication sessions include: the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions), the capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated; and the capability to generate unique session identifiers

with commonly accepted sources of randomness. Systems that include SL1 components may not be protected from easy-to-perform network attacks against the communications with those components.

CR 3.9 Protection of audit information: This SL2 additional base requirement requires that components provide the capability to protect audit information, audit logs and audit tools (if present) from unauthorized access, modification and deletion. This is a SL2 requirement meaning that components at SL1 may have audit logs, but those logs may not be protected per the requirement. This implies that systems using SL1 components may have unreliable security logs.

EDR 3.11, HDR 3.11 and NDR 3.11 Physical tamper resistance and detection: The SL2 additional base system integrity requirements require that components provide tamper resistance and detection mechanisms to protect against *unauthorized physical* access into the device. This capability protects the component from being *physically tampered* with between the time of manufacture and the time of installation and beyond. Components that do not meet these requirements, such as some SL1 devices, may be subject to physical tampering such as during the time when the device is in the supply chain.

4 FR 4 - Data confidentiality

The data confidentiality foundational requirement aims to ensure the confidentiality of information on communication channels and of data stored in repositories to protect against unauthorized disclosure.

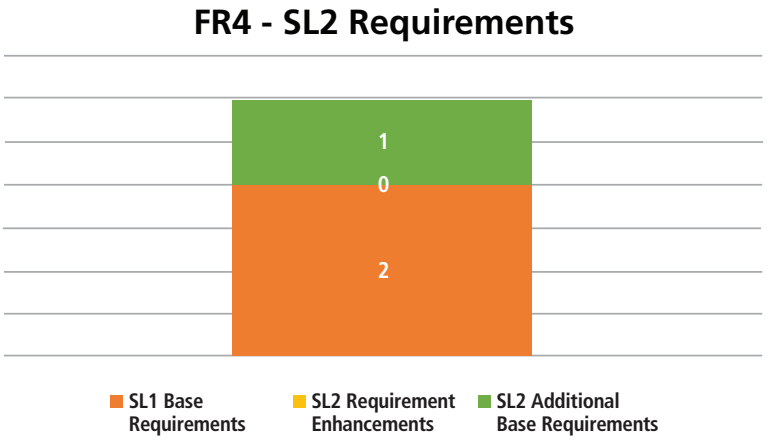

Figure 6 - Number of SL2 Requirements in FR 4

The requirements added for SL2 capability are shown in the table below.

SL2 Requirement Enhancements (RE)	SL2 Additional Base Requirements
	CR 4.2 Information persistence

CR 4.2 Information persistence: This is the only added SL2 requirement for FR 5 data confidentiality. This additional base requirement requires that components provide the capability to erase all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned. This implies that SL1 components might retain confidential information after being released from active service or decommissioned, and that information might be extracted from the component later, for example using the technique of "dumpster diving."

5 FR 5 - Restricted data flow

The purpose of the restricted data flow foundational requirement is to segment the control system via zones and conduits and limit the unnecessary flow of data.

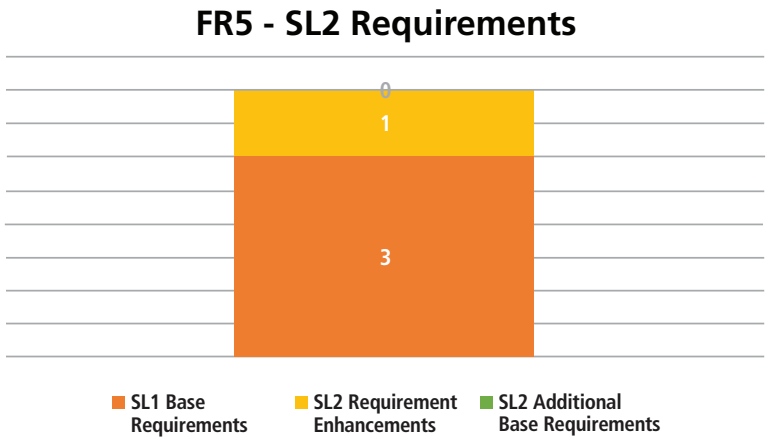

Figure 7 - Number of SL2 Requirements in FR 5

The requirements added for SL2 capability level 2 are shown in the table below.

SL2 Requirement Enhancements (RE)	SL2 Additional Base Requirements
NDR 5.2 RE 1 Deny all, permit by exception	

NDR 5.2 RE 1 Deny all, permit by exception: This is the only additional SL2 requirement for FR 5 restricted data flows and is intended for network device-type components. The SL1 base requirement NDR 5.2 requires that a network device at a zone boundary provides the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model. In addition, this SL2 requirement enhancement requires that network components provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception). This SL2 requirement enhancement requires stronger, less error-prone configuration capabilities for zone boundary protection devices such as firewalls.

6 FR 6 - Timely response to events

The purpose of the timely response to events foundational requirement is to respond to security violations by notifying the proper authorities, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.

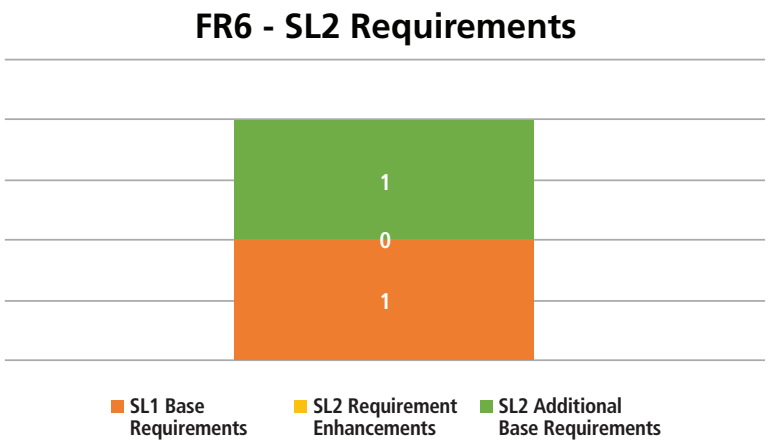

Figure 8 - Number of SL2 Requirements in FR 6

The requirements added for SL2 capability are shown in the table below.

SL2 Requirement Enhancements (RE)	SL2 Additional Base Requirements
	CR 6.2 Continuous monitoring

CR 6.2 Continuous monitoring: This SL2 additional base requirement requires that components provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner. This implies that SL1 components may not have this capability, meaning that security breaches may not be reported in a timely manner. This places a burden on the system to provide this capability by some other means or accept that SL1 components provide an additional risk to the system.

7 FR 7 - Resource availability

The purpose of the resource availability foundational requirement is to ensure the availability of components against the degradation or denial of essential services. As illustrated in Figure 9, there are six baseline security requirements for SL1. SL2 adds two requirement enhancements and one new base requirement to the SL1 baseline.

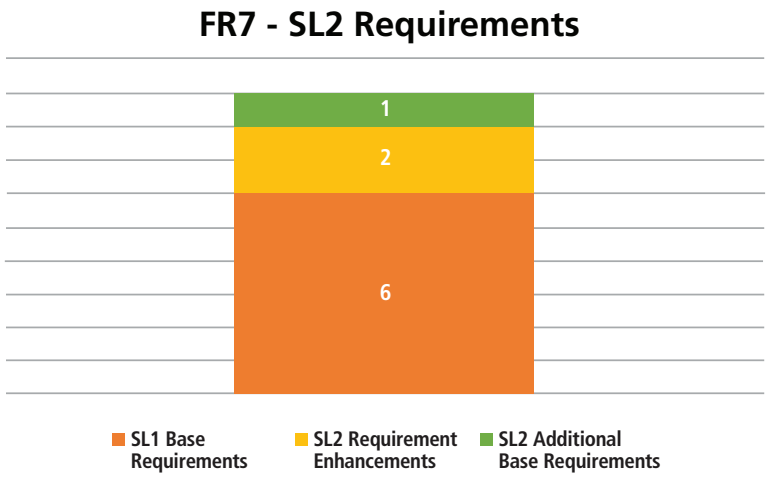

Figure 9 - Number of SL2 Requirements in FR 7

The requirements added for SL2 capability are shown in the table below.

SL2 Requirement Enhancements (RE)	SL2 Additional Base Requirements
CR 7.1 RE 1 Manage communication load from component	CR 7.8 Control system component inventory
CR 7.3 RE 1 Backup integrity verification	

CR 7.1 RE 1 Manage communication load from component: This is an SL2 requirement enhancement to the denial-of-service protection SL1 baseline requirement CR 7.1, which requires that components provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS (denial of service) event. The SL1 baseline requirement assures that components maintain essential services in the event of a DoS on the network or one aimed at the component. This SL2 requirement enhancement requires that components provide the capability to mitigate the effects of information and/or message flooding types of DoS events. SL1 components can maintain essential functions within the component, but all other functions might fail. SL2 components should be able to maintain additional non-essential functions, which may include outbound communications, during a DoS event.

CR 7.3 RE 1 Backup integrity verification: This is an SL2 requirement enhancement to the SL1 control system backup requirement CR 7.3. This SL2

requirement enhancement requires that components *validate the integrity* of backed-up information prior to the initiation of a restore of that information. This capability provides a layer of protection to ensure that the information being restored is the information that was backed up. SL1 components might restore other information than the information that was backed up, causing both a system integrity issue and possibly causing the restored component to fail or behave maliciously.

CR 7.8 Control system component inventory: This SL2 additional base requirement requires that components provide the capability to support a control system component inventory. This additional requirement allows the end user to gather a control system component inventory without walking the installed system to inventory the components manually. Accurate and up-to-date inventory information is a necessary basis for cybersecurity management.

8 FR 8 - Summary

The ISA/IEC 62443-4-2 standard defines a cybersecurity attack as an unauthorized attempt to compromise the confidentiality, integrity or availability of an IACS. In most cases, attackers of industrial control systems will want to target the integrity or availability of the system. Availability attacks can be in the form of denial-of-service attacks toward components in the system. Integrity attacks can take on several forms, such as modification of data as it traverses the network between components of the system, modification of the configuration of components of the system and modification of the component itself by modifying the hardware, firmware or software of the component.

Components with SL2 capabilities add additional layers of defense to protect against these attacks. In many cases, multiple SL2 capabilities work together to provide a defense in depth approach in protecting components and the systems in which those components reside. This section will give several examples of SL2 capabilities that, when combined, add to the cybersecurity resiliency of components and systems.

8.1 Individual user identification, authentication and accountability

CR 1.1 requirement enhancement 1 adds the security capability to uniquely identify and authenticate individual users. CR 2.1 requirement enhancement 1 adds authorization enforcement for all users, CR 2.1 requirement enhancement 2 adds permission mapping to roles, and CR 3.9 adds the protection of audit information. The combination of these requirements together increases a component's resiliency to attacks by authorized users who may try to perform actions they are not authorized to perform. The audit logs will log unauthorized actions and the strengthening of the audit log protection by CR 3.9 assures that the log is protected from unauthorized access or modification. This increases the accountability for users' actions towards a component in the system.

8.2 Software process and device identification, authentication and accountability

The addition of CR 1.2 as a SL2 capability can potentially add significant protection to systems that only integrate SL2 components into the system. SL2 components are required to identify themselves and authenticate to other components with which they wish to communicate. Therefore, if a system is composed of only SL2 components, every component in the system is known and has been authenticated. This significantly reduces the risk of unknown components being inserted into a system.

An additional strength of SL2 components communicating with other SL2 components is that those components also meet the CR 3.1 requirement enhancement 1 communication authentication capability. This results in the components knowing the identity of the source of the communications between the components. This is a significant defense against common network attacks such as man-in-the-middle and replay attacks.

8.3 Authenticity checks

Eleven of the SL2 capability requirements are related to authenticity checks. Four of these authenticity checks are related to mobile code (EDR, HDR, NDR and SAR 2.4 RE 1), one is related to software applications (CR 3.4 RE 1), three are related to updates and upgrades (EDR, HDR and NDR 3.10 RE 1), and the remaining three are related to the boot code of components (EDR, HDR and NDR 3.14 RE 1). These checks are intended to validate that the mobile code, software applications, updates and upgrades and boot code have not been modified since the product supplier created them and that the code is verified to have come from the product supplier. This check is usually performed by validating the digital signature attached to the code by the product supplier at production time. In most cases, this digital signing of the code includes the signing of an integrity value for the code, which also provides assurance that the code has not been modified since the product supplier produced it.

Because these authenticity checks will, in most cases, rely on digital signatures, these digital signatures will be validated using public keys provided by the producer of the code. These public keys need to be installed into the devices so that authenticity checks can be made at the boot-up time of the component to meet the component's boot authenticity and integrity requirements. This need is met with the three requirements for provisioning product supplier roots of trust (EDR, HDR and NDR 3.12).

These authenticity checks can result in a remarkably high level of trust that the components, which have SL2 capability, can be trusted to be authentic and execute code that has not been modified from the time the component was created until it is placed into use. The authenticity and integrity of updates and upgrades installed into the component allow it to retain that trust throughout its installed lifecycle in a system.

8.4 Physical access protection

Six of the SL2 capability requirements protect components from physical access, which might be used to perform unauthorized modifications to a component. The first three additional requirements protect against unauthorized use of physical diagnostic and test interfaces that may exist on a component (EDR, HDR and NDR 2.13). If left unprotected, these interfaces could allow for unauthorized modification of the configuration or the software that resides within the component.

The next three requirements add physical tamper resistance and detection to components (EDR, HDR and NDR 3.11). Without these requirements, implemented components may be open to unauthorized modification of the component's hardware, such as substituting or adding components to the physical hardware.

This summary does not include all the additional SL2 capabilities described in this paper but gives examples of how SL2 capabilities work together to improve the resiliency of SL2 components and help to protect the systems using SL2 components. SL1 components can protect from casual or coincidental compromise of the component but contribute little protection from intentional compromise. With more focus today on the security of industrial control systems, and with data indicating that these systems are becoming targets, asset owners should strongly consider requiring SL2 components to be installed in their systems.

9 Security capability level conformance

How do asset owners know that the components they are installing into the system meet the requirements of SL2? They have three choices:

1. Trust the product supplier statement that their products are designed to meet the requirements of ISA/IEC 62443-4-2 SL2
2. Build an assessment organization with the responsibility of testing all of the components from all of their product suppliers for conformance to the ISA/IEC 62443-4-2 SL2 requirements
3. Only procure components certified by an independent conformance body and specify that the components must be certified conformant to ISA/IEC 62443-4-2 SL2

10 Product supplier benefits and implementation

10.1 Benefits

Other papers and presentations have addressed the marketplace advantages to product suppliers for certifying their products. There are a few other significant advantages to product suppliers for designing and certifying their products to meet the requirements of ISA/IEC 62443-4-2 SL2.

The primary advantage is that their products will maintain their authenticity. The authenticity checks make it quite easy to detect unauthorized changes to the component's firmware and/or software. The additional SL2 capabilities that

strengthen the capability to protect the component from unauthorized changes through stronger access control requirements and physical access control requirements increase the level of difficulty in making unauthorized changes as well.

One final benefit of authenticity checks required in SL2 capable components is that it becomes exceedingly difficult to clone the component, reducing the possibility of counterfeit components being created.

10.2 Implementation

Product suppliers may ask how much design effort is required to upgrade their components from SL1 to SL2. The answer is not simple, considering the legacy SL1 component may be difficult to upgrade. New components, however, should be designed as SL2 as part of the design goals and requirements.

Many of the additional base requirements and requirement enhancements depend on the capability of the component to perform cryptographic functions and have secure storage for cryptographic keys. Almost all modern microprocessors have the capability built into them. With this capability in the component hardware, it is a matter of utilizing the capabilities in the firmware and software design of the component to meet the ISA/IEC 62443-4-2 requirements for SL2 as part of the design requirements.

If the component design does not utilize a modern microprocessor with cryptographic capabilities, then the design will need to include an external cryptographic engine, and many of those external devices also include secure storage for cryptographic keys. If the design does not include either a microprocessor with cryptographic capabilities or an external cryptographic engine, it will be very difficult to develop an SL2 component. If a product supplier is developing virtual components, it is critical that the virtual component be developed to execute in virtual containers that provide the necessary cryptographic capabilities.

Annex A

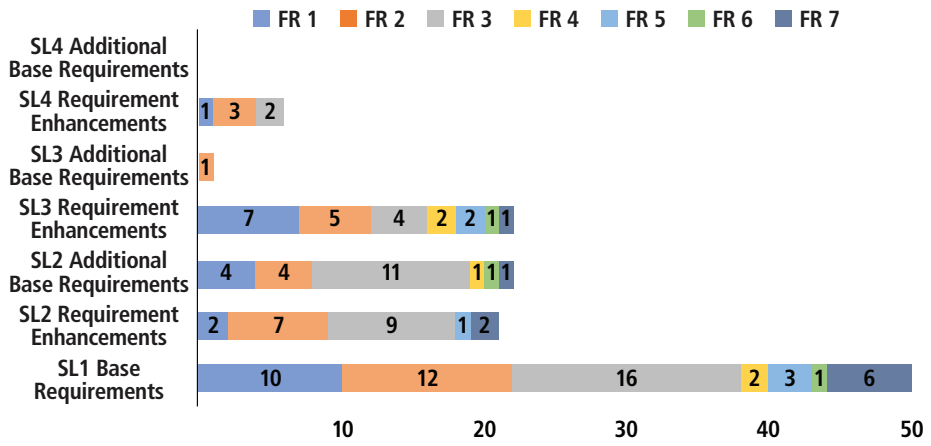

Figure 10 - Distribution of number of requirements by FR

Founded by the International Society of Automation (ISA), the ISASecure certification program certifies conformance to the ISA/IEC 62443 series of internationally adopted industrial security standards.

ISASecure assesses automation and control products and systems to ensure they are robust against network attacks, free from known vulnerabilities and meet the security capabilities defined in the ISA/IEC 62443 standards.

All ISASecure certifications are conducted by globally recognized ISO/IEC 17065 accredited certification bodies.

ISASecure®

International Society of Automation
3252 S. Miami Blvd., #102
Durham, NC 27703
+1 919 990 9222
aristaino@isa.org
www.ISASecure.org