National Security Agency
Cybersecurity Technical Report

Operational Technology Assurance Partnership: Smart Controller Security within National Security Systems

APR 2025

U/OO/145018-25
PP-25-1731
Version 1.0

Notices and History

Document Change History

Date	Version	Description
APR 2025	1.0	Initial publication

Disclaimer of Warranties and Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Publication Information

Author(s)

National Security Agency (NSA)
Cybersecurity Directorate

Contact Information

Cybersecurity Report Feedback: CybersecurityReports@nsa.gov
Defense Industrial Base Inquiries and Cybersecurity Services: DIB_Defense@cyber.nsa.gov
Media Inquiries / Press Desk: NSA Media Relations: 443-634-0721, MediaRelations@nsa.gov

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats, and to develop and issue cybersecurity specifications and mitigations for National Security Systems, Department of Defense information systems, and the Defense Industrial Base. This information may be shared broadly to reach all appropriate stakeholders.

Executive Summary

Ongoing operational technology (OT) dependence on information technology (IT) and integrated communications and networking increasingly puts OT at risk. The risk is especially concerning for mission critical OT within National Security Systems (NSS) in that it could disrupt critical missions, endanger public safety, and cause significant financial loss. To mitigate the risk, OT systems must meet robust security policies and technical security requirements. By assessing NSS OT against rigorous criteria at the system and component levels, NSS can have assurance that their OT has fewer security gaps and less risk to critical missions.

In support of improving the security of NSS, NSA (National Security Agency) conducted a study on how to fortify NSS OT systems with rigorous technical security requirements focused specifically on smart controllers. Smart controllers are intelligent OT embedded devices with enhanced capabilities, such as advanced processing power, integrated communication features, and edge computing abilities that are normally associated with network devices. NSA used qualitative research methods, data mapping, and comparative analysis to identify gaps between relevant National Institute of Standards and Technology (NIST) security controls and International Society of Automation (ISA) requirements. The Cybersecurity Technical Report captures the results of the study, including the problem description, security objectives, analysis, findings, and new requirements for NSS smart controllers.

The study helps to shape the development of the Operational Technology Assurance Partnership (OTAP), a pilot cybersecurity conformance testing program for NSS OT, and supports the update of recommendations to ISA 62443-4-2 to improve OT component security standards. Although the emphasis of the study and its planned outcomes are tailored to NSS OT cybersecurity, public and private sector infrastructure owners and operators can also improve the cybersecurity of their infrastructures by using OT smart controllers that meet the additional Component Requirements and associated Requirement Enhancements criteria developed in the study.

Contents

Figures

Tables

1. Introduction

1.1. Background

In July 1990, National Security Directive (NSD) 42 designated the Director of the National Security Agency (NSA) as the National Manager for National Security Telecommunications and Information Systems Security (national security systems or NSS). In the fulfillment of assigned responsibilities, the National Manager reviews and approves standards, techniques, systems, and equipment related to the security of NSS.

In addition to the National Manager, the Committee on National Security Systems (CNSS) was established by Executive Order 13231 in October 2001 for the purpose of protecting NSS through the development of operating policies, procedures, guidelines, directives, instructions, and standards. On 27 March 2014, CNSS published CNSS Instruction (CNSSI) 1253, which provides guidance on the security categorization of NSS and the selection of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security controls (also referred to as countermeasures and hereafter referred to as NIST countermeasures). In April 2024, the National Manager published Binding Operational Directive (BOD) 2024-001: Operational Technology Security Implementation, Reporting, and Inventory Requirements, which established the minimum NIST countermeasures baseline as moderate-moderate-moderate (M-M-M) impact for OT systems that qualify as NSS.

1.2. Problem Statement

The USG lacks a formalized process for the cybersecurity testing of NSS OT components, specifically smart controllers, to ensure conformance with the M-M-M NIST countermeasures baseline.

1.3. Purpose

The purpose of the study is to develop the set of requirements that align to the M-M-M NIST countermeasures for NSS OT smart controllers. These requirements will help shape the development of the Operational Technology Assurance Partnership (OTAP), a pilot NSS OT cybersecurity conformance testing program, and will support the

updating of the International Society of Automation (ISA) 62443-4-2 to improve OT component security standards.

1.4. Overview

NSA used qualitative research methods, data mapping, and comparative analysis. The process began with a mapping of the M-M-M NIST countermeasures to corresponding ISA-62443-4-2 Component Requirements (CRs) and associated Requirement Enhancements (REs), Embedded Device Requirements (EDRs), and Network Device Requirements (NDRs) that applied to embedded devices up to Security Level (SL) 3 (hereafter referred to as SL-3). Once mapped, NSA conducted a comparative analysis of NIST countermeasures and ISA-62443-4-2 CR, RE, EDR, and NDR language to validate ISA-62443-4-2 requirements' conformity to their corresponding NIST countermeasures.

1.5. Scope

NSA focused on the mapping of NIST SP 800-53 Rev. 5 moderate-moderate-moderate (M-M-M) countermeasures to the ISA 62443-4-2 requirements for OT components, the identification of ISA-62443-4-2 cybersecurity gaps, and the development of recommendations for a future set of NSS requirements for OT smart controllers.

ISA-62443-4-2 provides the cybersecurity technical requirements for the components that make up industrial automation and control systems (IACS), specifically the embedded devices, network components, host components, and software applications. ISA-62443-4-2 also outlines four security levels (SLs) based on a cyber-actor's means, resources, skills, and motivations, with SL-1 representing the least risk of exploitation and SL-4 the greatest.

CNSSI 1253 explicitly defines security and privacy baselines of NIST countermeasures for NSS, and NIST SP 800-82 defines security baselines specifically for OT. National Manager BOD 2024-001: Operational Technology Security Implementation, Reporting, and Inventory Requirements draws from these documents to establish the minimum baseline of countermeasures, for all OT systems designated as NSS, as M-M-M.

These published standards and requirements documents served as the parameters for comparative analysis for the study.

Additionally, NSA primarily concentrated on smart controllers, which are intelligent OT embedded devices with enhanced capabilities, such as advanced processing power, integrated communication features, and edge computing abilities that are normally associated with network devices. NSA examined ISA-62443-4-2 CRs, EDRs, NDRs, and associated REs to create a list of essential security requirements for smart controllers.

1.6. Findings

NSA determined that 74 ISA-62443-4-2 SL-1 through SL-3 requirements were relevant to the NSS OT smart controller M-M-M NIST countermeasures baseline and that 13 M-M-M NIST countermeasures were not adequately addressed in the ISA-62443-4-2 requirements. NSA resolved the gaps by developing one new CR and five new REs, in accordance with the threat analysis in Section 2, the security objectives defined in Section 3, and NIST countermeasure requirements, as well as using research of existing industry component security capabilities and practices. The new requirements are written to align with the verbiage and format of existing ISA requirements and are provided in Section 5 of the report.

NSA is using the results to inform the development of a formalized NSS OT component cybersecurity testing process. Additionally, NSA will submit the newly identified CR and REs to the ISA standards committees for consideration and potential inclusion in future ISA-62443-4-2 updates. While NSA focused exclusively on smart controllers, future iterations will use the same process to explore other OT component categories.

2. Security Problem Description

The convergence and connectivity of IT and OT have introduced significant cybersecurity challenges for OT environments. Traditionally isolated from external networks, OT systems are increasingly connected to IT networks, exposing them to cyber threats. While beneficial for operational efficiency and data analytics, the integration has expanded the attack surface and increased the risk of cyber incidents that could disrupt critical missions, endanger public safety, and cause significant financial loss.

The increased risk is of particular concern to NSS OT systems, which are potentially high-value targets for hacking groups and nation-state adversaries.

Improving the overall security posture of NSS OT systems requires robust security policies and procedures at an organizational level and implementing technical security features at the system and component levels, including embedded OT devices, specifically smart controllers.

Understanding the threats and vulnerabilities facing OT systems and devices is critical when designing policies, procedures, and technical security features.

2.1. Threats to OT Systems and Devices

Threats to OT systems and devices can mimic or mirror threats to IT systems. Legacy OT systems are more vulnerable to attack primarily for two reasons: (1) lack of security by default and (2) integrating these systems into an IT infrastructure with its own vulnerabilities.

In 2024, MITRE published the EMB3D Framework white paper to address security considerations for embedded devices, which states, “The security of our Nation’s critical infrastructure depends on embedded devices that frequently lack adequate countermeasures or have not undergone sufficient testing for vulnerabilities.” To further reinforce the observation, according to the ICS Advisory Project Dashboard as of December 2024, the Cybersecurity and Infrastructure Security Agency (CISA) has released over 3,000 ICS alerts since 2011 with a Medium or higher Common Vulnerability Scoring System (CVSS) severity score.**Error! Reference source not found.**

To determine which threats are commonplace across embedded systems, organizations should consider the most recent trends in the OT industry across various OT Original Equipment Manufacturers (OEMs). This can be accomplished by analyzing the Common Vulnerabilities and Exposures (CVE) from the NIST-managed National Vulnerability Database.

2.1.1. Assumptions and Considerations

The report makes several assumptions or considerations regarding OT devices. The following assumptions or considerations provide an understanding as to why embedded smart controller devices within the OT environment are highly susceptible to exploitation:

- Developed and expanded upon from the 1960s through the 2000s, developers designed many legacy OT systems to be isolated or air-gapped, with no intention of connecting to IT networks. Once they became part of an interconnected IT infrastructure, attackers could then choose from a variety of attack paths without physically interacting with the system or its embedded devices or setting foot on-site. These attack paths include inadequately protected routers, servers, and workstations that have network access to embedded devices, such as Programmable Logic Controllers (PLCs).
- Legacy OT systems rely on clear text communications through insecure protocols and have little to no encryption out of the box. A clear text data stream discovered with a protocol analyzer, such as Wireshark, can reveal a variety of information about the target. The information includes OEM names, system parameters, transport protocols, and many other data points that enable attackers to identify known vulnerabilities.
- Many legacy OT systems lack input validation, which makes it possible to execute arbitrary code on the target system. For example, a text input field on a human-machine interface (HMI) communicating with a PLC designed to receive a specific input would be able to receive malicious code to corrupt the system. The malicious code may lead to memory corruption, buffer overflows, and directory traversals, potentially opening the door to an organization’s critical data and trade secrets.
- Many legacy OT systems are designed with hard-coded credentials, which allow ease of authentication and elevation of access privileges. For example, a hard-

coded username and password is easy to obtain through OEM documentation, and an attacker can use the knowledge of an OEM's product to gain privileged access to the OT environment.

- In some cases, organizations use routable public-facing Internet Protocol (IP) addresses instead of private IP addresses. The configuration increases the risk of external attacks since these public IP addresses are accessible from anywhere worldwide. Some organizations use these addresses for external remote monitoring, while others incorrectly use them in air-gapped networks, allowing a potential attack path if the air gap is ever compromised.
- The growing reliance on global supply chains creates increased risk in supply chain security as some OEM devices may contain components that include hidden backdoors or other intentional vulnerabilities that adversaries can exploit to infiltrate target systems.

2.1.2. Known Attack Techniques

The MITRE ATT&CK Framework for Industrial Control Systems (ICS) recognizes 94 adversary techniques applied across 12 different tactics categories. These tactics and techniques range from gaining unauthorized access via supply chain compromise to establishing persistence by exploiting hardcoded credentials. MITRE developed the framework by analyzing real-world incidents, including those involving Advanced Persistent Threats (APTs), to reflect the tactics and techniques commonly used in OT/ICS environments.

Once an adversary gains access and establishes persistence, they can accomplish any number of malicious objectives. For example, as described in the MITRE ATT&CK Framework for ICS Matrix (2024), Stuxnet was deployed in November 2008, yet it was not discovered until approximately two years later, in 2010. It used zero-day vulnerabilities, rootkits, and network infection routines, which are just a few of the techniques showcased in the ATT&CK for ICS framework.

Additionally, the MITRE EMB3D Framework places 79 threats into one of four categories: hardware, system software, application software, and networking. Examples of each include:

- Hardware: side channel, firmware, and memory attacks

- System software: bootloader, root of trust data exfiltration, and authentication bypass attacks
- Application software: directory/path traversal, cross-site scripting (XSS), cross-site request forgery (CSR) session hijacking, hard-coded credentials exploitation
- Networking: undocumented protocols/commands and cryptographic attacks.

2.1.3. Common Vulnerability Analysis

During the study, NSA analyzed CVE data from the National Vulnerability Database website and focused on eight OEMs that supply products typically found in OT environments. NSA reviewed all recent CVEs (2023-2024) from these vendors to identify the associated threat. The analysis concluded that the top seven OT threats are:

1. Buffer overflow – 11 total CVEs
2. Memory corruption – 10 total CVEs
3. Input validation – 10 total CVEs
4. Cross-site scripting – 7 total CVEs
5. Directory, or path, traversal – 7 total CVEs
6. SQL injection – 5 total CVEs
7. Cross-site request forgery – 4 total CVEs

Common impacts from these threats include code execution, privilege escalation, denial of service, and information leaks. Table 1 reflects the results of the CVE analysis.

Table 1: CVE Survey of Common OT OEMs and Listed Threat Categories

Threat Categories	Vendors								Totals
	A	B	C	D	E	F	G	H	
Buffer Overflow	2	1	2	2	1	1	1	1	**11**
Memory Corruption	2	0	2	2	1	1	1	1	**10**
Input Validation	2	2	2	2	0	1	0	1	**10**
Cross-Site Scripting	1	1	0	1	0	1	1	2	**7**
Directory/Path Traversal	2	0	1	1	1	1	0	1	**7**
SQL Injection	2	0	0	0	0	0	2	1	**5**
Cross-Site Request Forgery	1	1	0	1	0	0	0	1	**4**

An attack proof-of-concept academic study by Sapir et al. (2022) substantiates the aforementioned CVE analysis and findings. In the study, a notional “EVIL PLC” ransomware attack was developed and conducted against PLCs from seven OEMs. The successful execution of the attack revealed that vulnerabilities in the PLCs and engineering workstations could be exploited and used as an attack vector by weaponizing PLCs through the use of malicious code. Attackers performed buffer overflows, path traversal, spoofing techniques, denial of service, remote/arbitrary code execution, and overwrite engineering software by using compromised PLCs.

Protecting OT devices against these aforementioned threats is vital to ensuring the availability and integrity of OT devices, systems, and associated services. This is of particular importance in the context of NSS, safety, and other mission-critical functions. Potential consequences of OT cybersecurity compromises, per NIST SP 800-82, are:

- Impact on national security (e.g., facilitate an act of terrorism)
- Lost or reduced production at one or multiple sites simultaneously
- Injury or death of employees
- Injury or death of persons in the community
- Damage to equipment
- Release, diversion, or theft of hazardous materials
- Environmental damage
- Violation of regulatory requirements
- Product contamination
- Criminal or civil legal liabilities
- Loss of proprietary or confidential information
- Loss of reputation or public trust

2.2. Organizational Security Policy

Organizational security policies are rules and procedures that address security needs at various levels, including organizational, operational, system, and component levels. These policies are the primary means for an organization to implement many NIST countermeasures, such as access control, audit and accountability, configuration management, identification and authentication, media protection, system and communications protection, and system and information integrity for OT systems.

While compliance with these policies establishes the rules for many countermeasures, the component-level devices must have the technical capabilities to support these rules. For example, if an organization's policy specifies a minimum password length of 12 characters, any component that only supports passwords up to 8 characters would violate the policy and create a security risk. Many of the ISA-62443-4-2 technical requirements, along with additional recommended NSS requirements, define the minimum capabilities of components. It is then up to the organizational security policy to determine how extensively these capabilities are implemented within the OT system.

3. Security Objectives

In the National Information Assurance Partnership's (NIAP) community, security objectives are established for specific IT devices, commonly referred to as Targets of Evaluation (TOEs), that are to be tested and certified through the NIAP evaluation process. NIAP defines a TOE as an IT product or group of IT products configured as an IT System and associated documentation subject to a security evaluation under the Common Criteria (CC). Similarly, the study used parts of the NIAP process to evaluate the security of NSS OT smart controllers. As such, the TOE for the study, for which security objectives are being established, is an NSS OT smart controller.

3.1. Security Objectives for NSS OT Smart Controllers

The security objectives for NSS OT smart controllers have been organized along the seven ISA-62443-4-2 Foundational Requirements (FRs) and conform to M-M-M NIST countermeasures to address the security threats described in Section 2. The following sections provide the ISA-62443-4-2 SL-3 protection descriptions associated with each FR in italicized font. Additionally, the new NSS CR and REs required to meet M-M-M NIST countermeasure gaps not addressed by the existing ISA-62443-4-2 requirements are listed as a bullet under each appropriate FR.

3.1.1. Foundational Requirements:

3.1.1.1. Identification and Authentication Control

NSS OT smart controllers *must identify and authenticate all users (humans, software processes, and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation*.

No additional NSS requirements or enhancements were developed for the FR.

3.1.1.2. Use Control

NSS OT smart controllers *must restrict the use of the IACS according to specified privileges to protect against circumvention by entities using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation*.

New NSS requirement and enhancements:

- Disabling of Wireless Capabilities
- Disabling of SSID Broadcast
- Use of Pattern-Hiding Displays
- Restricted Use of Removable Media Devices

3.1.1.3. System Integrity

NSS OT smart controllers *must protect the integrity of the IACS against manipulation by someone using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation.*

No additional NSS requirements or enhancements were developed for the FR.

3.1.1.4. Data Confidentiality

NSS OT smart controllers *must prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation.*

New NSS requirement enhancements:

- Use of Encryption to Protect Confidentiality
- Use of Approved Cryptographic Security Measures

3.1.1.5. Restricted Data Flow

NSS OT smart controllers *must prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation.*

No additional NSS requirements or enhancements were developed for the FR.

3.1.1.6. Timely Response to Events

NSS OT smart controllers *must monitor the operation of the components of the IACS, and respond to incidents when discovered, by actively collecting and pushing forensic evidence to the proper authorities.*

No additional NSS requirements or enhancements were developed for the FR.

3.1.1.7. Resource Availability

NSS OT smart controllers *must ensure that the component operates reliably under normal, abnormal, and extreme production conditions and prevents denial-of-service situations by entities using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation.*

No additional NSS requirements or enhancements were developed for the FR.

3.2. Security Objectives for the Operational Environment

While the study is focused on the mapping of M-M-M NIST countermeasures to component-level requirements that NSS OT smart controllers must be designed, developed, and tested to, the security of the operational environment must not be overlooked. Security failures within the operational environment can nullify organic NSS OT component countermeasures. Therefore, the following six security objectives for the operational environment have been developed:

3.2.1. Physical Protection

The operational environment must provide physical security commensurate with the value of the NSS OT smart controller and the data it contains. Platforms that operate within access-controlled environments are expected to receive a considerable degree of protection within these environments.

3.2.2. Supply Chain

Processes must be implemented by suppliers, manufacturers, and OEMs to ensure that NSS OT smart controller hardware and firmware are not compromised between the time of manufacturing and delivery to its operational site.

3.2.3. Trusted Administrators

Security Administrators must be vetted and trusted to follow and apply all guidance documentation appropriately. The administrator must not be careless or willfully negligent and must administer the platform in compliance with enterprise security policies.

3.2.4. Secure Administrator Credentials

The administrator credentials used to access NSS OT smart controllers must be protected on all platforms on which they reside.

3.2.5. Updates

Firmware and software must be tested and updated regularly by an administrator or integrator for all NSS OT components, including embedded, host, and network devices. This is especially important when product updates are released in response to known vulnerabilities.

3.2.6. Security Monitoring and Assurance

For NSS OT smart controllers, the Security Administrator must ensure that the availability and audit functionality of every device is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components.

4. Analysis, Findings, and New Requirements Development

In April 2024, the National Manager for NSS released BOD 2024-001 which defines the minimum-security categorization and applicable countermeasure baseline as M-M-M for all OT systems designated as NSS. NIST SP 800-53 Rev. 5 defines the complete list of cybersecurity countermeasures, while NIST 800-82 Rev. 3 and CNSSI 1253 identify the 470 countermeasures required for the M-M-M baseline.

When considering the overall security of OT systems designated as NSS, each component of these systems must be able to perform a certain level of security functions. ISA established a set of cybersecurity technical requirements for these OT elements in ISA-62443-4-2. Relevant requirements are identified as CRs, EDRs, NDRs, and underlying REs. NSA analyzed all requirements associated with SL-1 through SL-3.

The analysis mapped the existing ISA-62443-4-2 requirements relevant to NSS OT smart controllers to the M-M-M countermeasure baseline, which led to the identifying requirement gaps. NSA developed recommendations for new requirements to address these gaps and used the results of the analysis to recommend a set of designated ISA-62443-4-2 requirements and new NSS requirements as the baseline requirements for smart controllers within OT NSS.

4.1. Methodology

The first step of the effort was to analyze all 470 M-M-M NIST countermeasures to determine their relevance to OT smart controllers. During the process, NSA determined that many countermeasures were organizational or policy-based controls (i.e. AC-1 Access Control Policy and Procedures and all AT countermeasures), and others were determined to be system level countermeasures that are technically infeasible for smart controllers (for example PE-14 Environmental Controls and SI-2(2) Flaw Remediation | Automated Flaw Remediation Status). After analysis, NSA identified 154 countermeasures as relevant.

NSA mapped the existing ISA-62443-4-2 requirements to the relevant NIST countermeasures. NSA determined that requirements mapped directly to one or more countermeasures are essential for meeting the M-M-M baseline. The mapping resulted in one-to-one, one-to-many, or many-to-one requirements to countermeasure

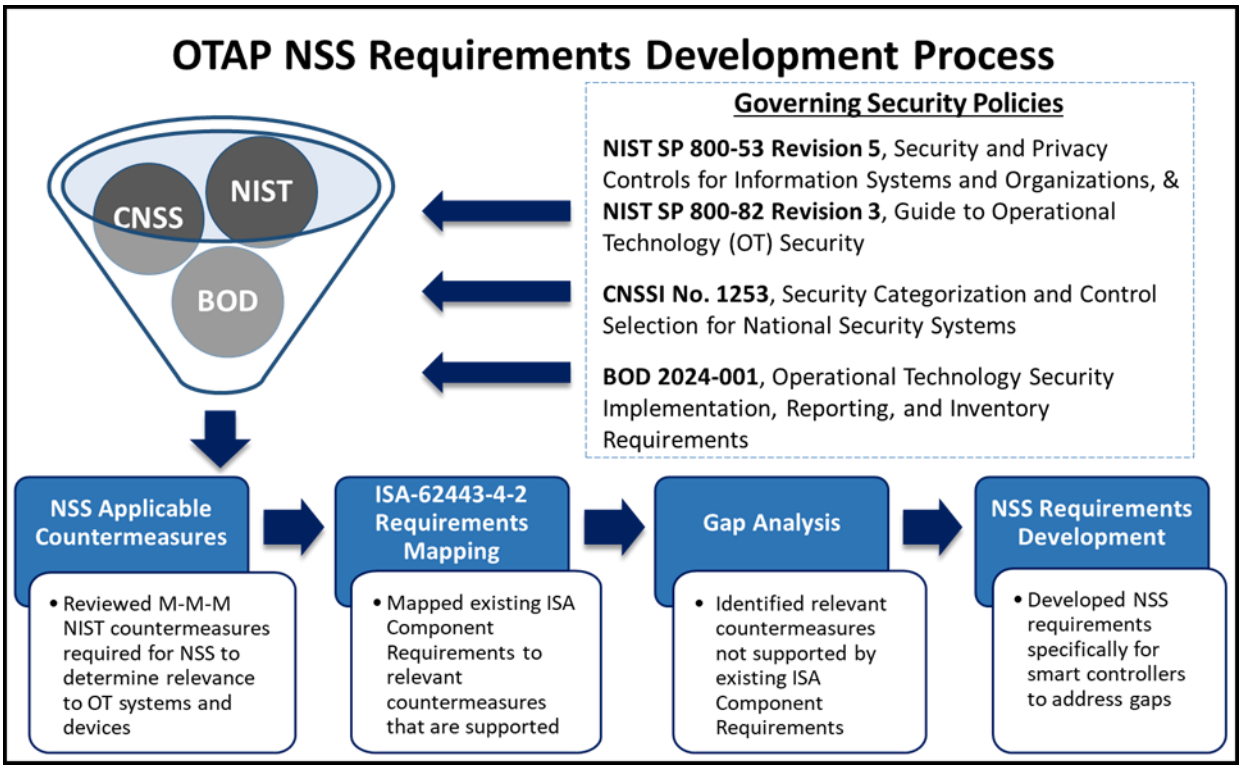
relationships. For example, CR 1.10 Authenticator Feedback was mapped solely to IA-6 Authenticator Feedback, whereas CR 1.5 Authenticator Management mapped to both IA-5 Authenticator Management and IA-5(6) Protection of Authenticators.

Next, NSA determined whether each NIST countermeasure was satisfied by the mapped CRs, EDRs, NDRs, and REs. Satisfied indicates that a smart controller that meets the applicable requirement(s) can fully support an OT system at the M-M-M baseline. For example, when examining the requirements for secure boot, the NIST countermeasures SI-7(9) and SI-7(10) align with EDRs 3.12 and 3.14. These requirements discuss the roots of trust and integrity for the boot process and fully satisfy the associated countermeasures.

Any countermeasure that was not fully satisfied by existing requirements was identified as a gap that may prevent an OT NSS smart controller from achieving the M-M-M baseline. For each gap, NSA developed a new recommended NSS CR or NSS RE.

An overview of the process is illustrated below in Figure 1.

Figure 1: OTAP NSS Requirements Development Process



The identification of relevant ISA-62443-4-2 requirements and the development of new NSS CRs and REs were informed and developed based on insights gained from the threat analysis in Section 2 and the security objectives in Section 3.

4.2. Overview of Findings

In the study, NSA determined 74 ISA-62443-4-2 requirements were relevant to NSS OT smart controllers and the M-M-M NIST countermeasures baseline, and that 13 M-M-M NIST countermeasures were not adequately addressed by the 74 requirements. To resolve these gaps, NSA recommended new requirements, including one new NSS CR and five new NSS Res according to the threat analysis in Section 2, the security objectives defined in Section 3, and NIST countermeasure requirements. The recommended requirements partially resulted from researching existing industry component security capabilities and practices. The new recommended requirements and rationale are provided in Section 5 of the study.

Appendix D of the document contains a complete list of the relevant CRs, EDRs, NDRs, and REs mapped to M-M-M NIST countermeasures, and Appendix E is the complete list of M-M-M NIST countermeasures mapped to the requirements. The 13 M-M-M NIST countermeasures identified as gaps are listed in Table 2 and the new recommended NSS requirements are listed in Table 3.

Table 2: NIST SP 800-53 Rev. 5 Countermeasure Gaps

M-M-M NIST SP 800-53 Rev. 5 Countermeasure Gaps	
ID	**TITLE**
AC-11(1)	Device Lock | Pattern-Hiding Displays
AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption
AC-18	Wireless Access
AC-18(1)	Wireless Access | Authentication and Encryption
AC-18(3)	Wireless Access | Disable Wireless Networking
AC-20(2)	Use of External Systems | Portable Storage Devices – Restricted Use
MP-7	Media Use
SC-8	Transmission Confidentiality and Integrity
SC-8(1)	Transmission Confidentiality and Integrity |Cryptographic Protection
SC-13	Cryptographic Protection
SC-28	Protection of Information At Rest
SC-28(1)	Protection of Information At Rest | Cryptographic Protection
SC-41	Port and I/O Device Access

Table 3: NSS CR and RE Additions with Mapped Countermeasures

Required OT NSS CR and RE Additions to ISA-62443-4-2		NIST SP 800-53 Rev. 5 Countermeasures
CR 2.2 NSS RE(1)	Disabling of Wireless Capabilities	AC-18(3)
		AC-20(2)
CR 2.2 NSS RE(2)	Disabling of SSID Broadcast	AC-18
CR 2.5 NSS RE(1)	Use of Pattern-Hiding Displays	AC-11(1)
CR2 NSS CR(1)	Restricted Use of Removable Media Devices	MP-7
		SC-41
CR 4.1 NSS RE(1)	Use of Cryptography to Protect Confidentiality	AC-17(2)
		AC-18(1)
		SC-8
		SC-8(1)
		SC-28
		SC-28(1)
CR 4.3 NSS RE(1)	Use of Approved Cryptographic Security Measures	AC-18(1)
		SC-13
		SC-28(1)

5. Requirements for National Security Systems (NSS) OT Smart Controllers

The study determined that NSS OT smart controllers must conform to 74 ISA-62443-4-2 SL-1 through SL-3 requirements and the 6 newly developed NSS smart controller requirements in order to meet the M-M-M NIST countermeasure baseline. All relevant ISA-62443-4-2 requirements with their mapped M-M-M NIST countermeasures are listed in Appendix D of the study.

5.1. New NSS Smart Controller Requirements

The newly developed NSS OT smart controller requirements defined in sections 5.2 through 5.3 of the study are organized along the ISA-62443 FR, CR, and associated RE categorization and numbering identifications. Additionally, all new recommended NSS OT smart controller requirements are listed in table format in Appendix F.

5.2. FR 2 – Use Control

5.2.1. CR 2.2 — Wireless Use Control

5.2.1.1. NSS Requirement Enhancement (1) – Disabling of Wireless Capabilities

If a component has wireless capabilities, it must:

a) have the capability to physically disable the wireless interfaces via a switch or other means, and
b) be disabled by default within the operating system or application settings.

Rationale and Supplemental Guidance

Within the OT environment, the increasing use of wireless networking places OT implementations at greater risk from adversaries who are in relatively close physical proximity but do not have direct physical access to the equipment. Having wireless access to sensors and final elements allows for direct manipulation of the physical processes within the OT environment, which could potentially render the OT system inoperable. Examples of potential attacks include: Unauthorized client accesses, Denial of Service (DoS) attacks, Man-in-the-Middle attacks, side-channel attacks (through dual-homed connections), IP spoofing, and hijacking.

Organizations that manage NSS OT/ICS networks may choose to disable the wireless interfaces within components to reduce these risks.

Note: These organizations may prefer to utilize components that do not have built in wireless capabilities.

Mapped Countermeasures: AC-18(3) and AC-20(2)

5.2.1.2. NSS Requirement Enhancement (2) – Disabling of SSID Broadcast

If a smart controller has the capability to be a wireless access point, it must have the SSID broadcast disabled by default.

Rationale and Supplemental Guidance

When SSID broadcast is enabled, the SSID, or network name, is continuously advertised by the wireless access point (AP). This makes the network easily detectable by nearby devices, including those of potential attackers. Disabling SSID broadcasts hides the network from casual scanning, reducing the visibility to unauthorized users who may attempt to gain access.

Mapped Countermeasure: AC-18

5.2.2. CR 2.5 – Session Lock

5.2.2.1. NSS Requirement Enhancement (1) – Use of Pattern-Hiding Displays

When a session lock is initiated, smart controllers with a connected display must have the capability to use configurable pattern-hiding display screens, such as a blank screen, solid colors, clock, or other selectable screen.

Rationale and Supplemental Guidance

Utilizing pattern-hiding displays conceals sensitive information previously visible on the display screen before the session lock. This reduces the risk of information disclosure to unauthorized individuals within close proximity of the components.

Users should be able to configure the pattern hiding display to continuously show information and maintain functionality that is determined to be non-sensitive, critical to the operations, or safety instrumented system information and life safety controls.

Mapped Countermeasure: AC-11(1)

5.2.3. NSS Component Requirement (1) – Restricted Use of Removable Media Devices

Smart Controllers must provide the capability to restrict the use of unauthorized removable media devices that may connect directly to the smart controller.

Rationale and Supplemental Guidance

Removable media device types that should be restricted include, but are not limited to, USB devices, laptops, flash drives, SD cards, external hard drives, and other portable storage devices.

These media devices may serve as an entry point for malware into OT networks that bypasses traditional network security. Malicious software can be intentionally or inadvertently transferred onto these devices from external sources and then brought into secure network environments, compromising critical systems. Malicious software (e.g., malware, viruses, ransomware) specifically designed to target industrial systems can exploit vulnerabilities in OT systems. Once introduced, malware can spread rapidly across networks, causing operational disruptions, data breaches, or physical damage.

By restricting the use of removable media devices, organizations can significantly reduce the attack surface and enhance the security posture of their OT networks.

Note: The restriction may be accomplished by logically shutting down available connection ports or physically disabling them.

Mapped Countermeasures: MP-7 and SC-41

5.3. FR 4 – Data Confidentiality

5.3.1. CR 4.1 – Information Confidentiality

5.3.1.1. NSS Requirement Enhancement (1) – Use of Cryptography to Protect Confidentiality

Smart controllers must support the capability to encrypt information in transit over all enabled and active external interfaces, as well as information at rest.

Note: ISA's use of the phrases "information in transit" and "information at rest" is synonymous with the NIST phrases "data in transit" and "data at rest". While the requirement reflects the ISA language, the intent is the same as the aligned NIST countermeasure.

Rationale and Supplemental Guidance

Protecting information in transit involves encrypting data as it moves from one location to another over any external interface, including both traditional wired networks and wireless communication channels. This includes all protocols, such as routable protocols (e.g., TCP/IP), serial communication (e.g., Modbus RTU), and both internal and external interfaces used for control and monitoring systems. Each level of the network should be safeguarded to ensure confidentiality and integrity, whether it is the data traveling across local network boundaries, between control systems, or externally over remote access links. Encryption must extend to these varying transmission methods, whether the data is passing through physical cables or wireless signals, and includes data sent between industrial equipment or to remote devices.

Protecting information at rest involves encrypting data that is stored on physical media, such as hard drives, databases, or any other storage devices, awaiting retrieval or use. This type of data is not actively being transferred but must still be protected from unauthorized access.

The implementation of security architecture and encryption technologies must not degrade the operational performance of the end devices within the OT enclave. Exemptions for the requirement are permitted if the encrypted information at rest would greatly impact processing times. Examples of this are the operating system files and other files needed for the boot process.

Encryption technologies must meet CR 4.3 NSS RE (1) requirements.

Mapped Countermeasures: AC-17(2), AC-18(1), SC-8, SC-8(1), SC-28, and SC-28(1)

5.3.2. CR 4.3 – Use of Cryptography

5.3.2.1. NSS Requirement Enhancement (1) – Use of Approved Cryptographic Security Measures

Smart Controllers must utilize NSA-approved cryptographic security mechanisms.

Rationale and Supplemental Guidance

Cryptography is fundamental to securing critical infrastructure systems that support the mission-critical services essential for the operation of NSS. By leveraging approved cryptographic algorithms listed in the Commercial National Security Algorithm (CNSA) suite (see CNSS Policy 15) and Federal Information Processing Standards (FIPS) 140-2 or newer, these systems are fortified against advanced and evolving cyber threats. These cryptographic frameworks provide robust protection for data both in transit and at rest, mitigating the risks of unauthorized access, tampering, and data breaches.

To maintain long-term resilience, cryptographic agility is crucial. This means the ability to adapt and migrate to stronger cryptographic algorithms and protocols as they evolve over time, ensuring the systems remain secure against future threats. Additionally, utilizing secure OT communication protocols further reinforces the integrity and security of critical infrastructure systems, ensuring that all data exchanges and remote operations are safeguarded.

Note: Deprecated algorithms, such as SSL, 3DES, and SSH 1.0, should be avoided. These outdated algorithms have known vulnerabilities that can be exploited by cyber adversaries, posing significant risks to both the integrity of systems and national security.

Mapped Countermeasures: AC-18(1), SC-13, SC-28(1)

6. Conclusion

6.1. Study Summary

The growing dependence on IT technologies within OT systems and networks and the advancing capabilities of cyber adversaries have introduced significant cybersecurity risks to OT environments. The increased risk is of particular concern to mission-critical NSS OT systems, which are potentially high-value targets for hacking groups and nation-state adversaries. Thus, improving the overall security posture of NSS OT systems is of the utmost importance. The improvement requires robust security policies and procedures at an organizational level and the implementation of technical security features at the system and component levels, which includes OT smart controllers. Therefore, these OT systems and devices must be developed and tested against a robust set of technical requirements designed to meet these security needs, especially given the criticality of embedded devices in the operation and assurance of mission-critical national security functions.

The purpose of the study was to develop the set of requirements that align to the M-M-M NIST countermeasures for NSS OT smart controllers. The study concluded that the design, development, and testing of OT smart controllers using the ISA-62443-4-2 SL-1 through SL-3 requirements alone would not sufficiently satisfy the CNSSI 1253 M-M-M baseline of NIST SP 800-53 Rev. 5 countermeasures. However, with the addition of one new NSS CR and five new NSS REs, focused on smart controllers and specifically tailored to address the identified countermeasures gaps, the cybersecurity conformance testing to the mandated M-M-M security baseline can be achieved.

6.2. Way Forward

The results of the study may be used to inform the development of a formalized NSS OT cybersecurity conformance testing process similar to ISASecure's Component Security Assurance (CSA) and Industrial Internet of Things (IIoT) Component Security Assurance (ICSA) certifications. Additionally, the newly developed NSS CR and NSS REs may be submitted to the ISA standards committees for consideration and potential inclusion in future ISA-62443-4-2 updates for broad adoption by NSS OT and others.

While the study recommends smart controller requirements that address the gaps that exist between ISA and NIST, further analysis suggests the importance of addressing

secure by default requirements, as identified in the January 2025 Cybersecurity and Infrastructure Security (CISA) Secure by Demand joint guide on selecting products for OT environments, as well as the need to protect critical functions and data within smart controllers to ensure process integrity through the isolation of functions. Requirements addressing these two additional areas of concern may be developed by future OTAP efforts, and included in the future NSS OT cybersecurity requirements and conformance testing process.

Although the emphasis of the study and its planned outcomes have been specific to the cybersecurity of NSS OT systems, public and private sector infrastructure owners and operators can also improve the cybersecurity of their respective infrastructures through the employment of OT smart controllers that meet the additional requirements identified through the study.

Appendix A: Terms and Definitions

Terms and definitions have been derived from ISA-62443-4-2 unless otherwise noted with a derivative source provided.

Attack

Unauthorized attempt to compromise the confidentiality, integrity, or availability of an IACS that derives from an intelligent threat.

Note 1: For example, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Note 2: There are different commonly recognized classes of attack

- An "active attack" attempts to alter system resources or affect their operation.
- A "passive attack" attempts to learn or use information from the system but does not affect system resources.
- An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider"), for example, an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.
- An "outside attack" is initiated from outside the perimeter by an unauthorized or illegitimate user of the system (including an insider attack from outside the security perimeter). Potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

Authentication

The verification of the claimed identity of an entity.

Note: Authentication is usually a prerequisite to access resources in a control system.

Authenticator

Means used to confirm the identity of an entity.

Note: A password or token may be used as an authenticator.

Availability

Property of ensuring timely and reliable access to and use of control system information and functionality.

Buffer Overflow

A condition at an interface under which more input can be placed into a buffer or data holding area than the capacity allocated, overwriting other information. Adversaries exploit such a condition to crash a system or to insert specially crafted code that allows them to gain control of the system.

Source: NIST CSRC

Communication Channel

Specific logical or physical communication link between assets.

Note: A channel facilitates the establishment of a connection.

Compartmentalization

Use of any method or technology to separate multiple functions during execution, where separation limits their interactions to those intended.

Note: Examples of compartmentalization methods are containerization, virtual machines, hardware separation (by chip or board), enforced memory allocation, and software-based segmentation.

Component

Entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device.

Conduit

Logical grouping of communication channels, connecting two or more zones that share common security requirements.

Note: A conduit is allowed to traverse a zone as long as the zone does not impact the security of the channels contained within the conduit.

Confidentiality

Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

Note: When used in the context of an IACS, refers to protecting IACS data and information from unauthorized access.

Connection

Association established between two or more endpoints that supports the establishment of a session.

Control System

Hardware and software components of an IACS.

Countermeasure

Action, device, procedure or technique that reduces a threat, a vulnerability, or the consequences of an attack by minimizing the harm the attack can cause or by discovering and reporting it so that corrective action can be taken.

Note: The term "security control" is also used to describe the concept in some contexts. The term countermeasure has been chosen for the document to avoid confusion with the term "security control" in the context of "process control" and "control system."

Cross-site Request Forgery (CSRF)

An attack in which a subscriber currently authenticated to a relying party and connected through a secure session browses to an attacker's website, causing the subscriber to unknowingly invoke unwanted actions at the relying party. For example, if a bank website is vulnerable to a CSRF attack, it may be possible for a subscriber to unintentionally authorize a large money transfer, merely by viewing a malicious link in a webmail message while a connection to the bank is open in another browser window.

Source: NIST CSRC

Cross-site Scripting (XSS)

A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user-supplied data from requests or forms without sanitizing the data so that it is not executable.

Source: NIST CSRC

Device

Discrete physical asset that provides a set of capabilities.

Note 1: Examples include controllers, human-machine interfaces (HMI), PLCs, remote terminal units (RTUs), transmitters, actuators, valves, network switches, etc.

Note 2: A device may exhibit the characteristics of one or more of a host device, network device, software application, or embedded device.

Directory/Path Traversal

Aims to access files and directories that are stored outside the web root folder. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on the file system including application source code or configuration and critical system files.

Source: OWASP

Embedded Device

Special purpose device designed to directly monitor or control an industrial process.

Note 1: Typical attributes limited storage, limited number of exposed services, programmed through an external interface, embedded operating systems (OS) or firmware equivalent, real-time scheduler, may have an attached control panel, and may have a communications interface.

Note 2: Examples include PLCs, wired or wireless field sensor devices, wired or wireless field actuator devices, safety instrumented system (SIS) controllers, and distributed control system (DCS) controllers.

Environment

Surrounding objects, regions, or circumstances that may influence the behavior of the IACS and/or may be influenced by the IACS.

Event

Occurrence of or change to a particular set of circumstances.

Note: In an IACS, this may be an action taken by an individual (authorized or unauthorized), a change detected within the control system (normal or abnormal), or an automated response from the control system itself (normal or abnormal).

Foundational Requirement

Essential service, capability, feature, or activity that serves as a basis for derivation of detailed requirements.

Incident

Event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system.

Input Validation (Input Manipulation Attack)

Input Manipulation Attacks is an umbrella term, which includes Adversarial Attacks, a type of attack in which an attacker deliberately alters input data to mislead the model [device].

Source: OWASP

Note: Input validation covers SQL Injections, Directory/Path Traversal, Cross-site Scripting (XSS), and Cross-Site Request Forgery (CSRF) attacks.

Insider Threat

The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of organizational operations and assets, individuals, other organizations, and the Nation. The threat can include damage through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of organizational resources or capabilities.

Source: NIST CSRC

Integrity

Property of protecting the accuracy and completeness of assets.

Least Privilege

Basic principle that holds that users (humans, software processes, or devices) should be assigned the fewest privileges consistent with their assigned duties and functions.

Note: Least privilege is commonly implemented as a set of roles in an IACS.

Memory Corruption

Making use of freed or deleted memory, causing a program or system to crash.

Source: OWASP

Note: Buffer overflows (previously mentioned) can fit into this category.

Mobile Code

Program transferred between assets that can be executed without explicit installation by the recipient.

Note: Examples of mobile code include JavaScript, VBScript, Java applets, ActiveX controls, Flash animations, Shockwave movies, and Microsoft Office macros.

Network Device

Device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process.

Note: Typical attributes include embedded OS or firmware, no HMI, no real-time scheduler, and configuration through an external interface.

Remote Access

Access to a component by any user (human, software process, or device) communicating from outside the perimeter of the zone being addressed.

Note: the preceding definition is from ISA. NIST defines remote access as access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network.

Role

Set of connected behaviors, privileges and obligations that may be assigned to a user or group of users (humans, software processes or devices) of an IACS.

Note: The privileges to perform certain operations are assigned to specific roles.

Secure Boot (also known as Trusted Boot)

A system boot where aspects of the hardware and firmware are measured and compared against known good values to verify their integrity.

Security Control

Safeguards or countermeasures employed within a system or an organization to protect the confidentiality, integrity, and availability of the system and its information and to manage information security risk.

Note 1: Security Controls referenced throughout the document are derived from NIST SP 800-53 Rev. 5.

Note 2: Within the document, the term Countermeasures is used synonymously with the term Security Controls.

Security Level

Level corresponding to the required set of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit.

Session

Semi-permanent, stateful and interactive information interchange between two or more communicating components.

Note: Typically a session has clearly defined start and end processes.

Smart Controller

PLCs or ICS Controllers that have enhanced capabilities such as:

- advanced processing power to handle more complex operations and make real-time decisions
- integrated communication features to support various communication protocols, such as Ethernet, wireless, or IoT protocols, enabling them to interact with broader networks
- edge computing abilities that enable them to perform data processing at the device level (at the "edge") rather than relying solely on centralized systems

Source: NSA internally developed the definition based on industry and academic normative language.

Software Application

One or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian).

Note 1: Software applications typically execute on host devices or embedded devices.

Note 2: Dependencies are any software programs that are necessary for the software application to function, such as database packages, reporting tools, or any third-party or open-source software.

SQL Injection

Attacks that look for websites that pass insufficiently-processed user input to database back-ends.

Source: NIST CSRC

Threat

Set of circumstances and associated sequence of events with the potential to adversely affect operations (including mission, functions, image, or reputation), assets, control systems, or individuals via unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Trust

Confidence that an operation, data transaction source, network, or software process can be relied upon to behave as expected.

Note 1: Generally, an entity can be said to 'trust' a second entity when it (the first entity) assumes that the second entity will behave as the first entity expects.

Note 2: The trust may apply only for some specific functions.

Update

Incremental hardware or software change in order to address security vulnerabilities, bugs, reliability, or operability issues.

Zone

Collection of entities that represent partitioning of a system under consideration on the basis of their functional, logical, and physical (including location) relationship.

Note: A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.

Appendix B: Abbreviations and Acronyms

The following provides a complete list of abbreviated terms and acronyms used throughout the study.

ANSI	American National Standards Institute
AP	Access Point
APT	Advanced Persistent Threat
BOD	Binding Operational Directive
CISA	Cybersecurity and Infrastructure Security Agency
CNSA	Commercial National Security Algorithm
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CR	Component Requirement
CSA	Component Security Assurance
CSRF	Cross-Site Request Forgery
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DCS	Distributed Control System
DES	Data Encryption Standard
DoD	Department of Defense
DoS	Denial of Service
EDR	Embedded Device Requirement
FIPS	[US NIST] Federal Information Processing Standard
FR	Foundational Requirement
HMI	Human-Machine Interface
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IACS	Industrial Automation and Control System(s)
ICS	Industrial Control Systems
IP	Internet protocol
ISA	International Society of Automation
ISAGCA	ISA Global Security Alliance
ISA TR	ISA Technical Reports
IT	Information Technology
M-M-M	Moderate-Moderate-Moderate
MITRE	The MITRE Corporation
NIST	U.S. National Institute of Standards and Technology
NSA	National Security Agency
NSD	National Security Directive
NSS	National Security System
OEM	Original Equipment Manufacturer
OS	Operating System

OT	Operational Technology
OTAP	Operational Technology Assurance Partnership
OWASP	Open Web Application Security Project
PDF	Portable Document Format
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
RE	Requirement Enhancement
RTU	Remote Terminal Unit
SHA	Secure Hash Algorithm
SIS	Safety Instrumented System
SL	Security Level
SP	[US NIST] Special Publication
SQL	Structured Query Language
SSH	Secure Socket Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TOE	Target of Evaluation
TLS	Transport Layer Security
US	United States
USB	Universal Serial Bus
U.S.C.	United States Code
USG	United States Government
VBScript	Visual Basic Script
XSS	Cross-Site Scripting

Appendix C: References

USG Directives and Documents

BOD 2024-001, *Operational Technology Security Implementation, Reporting, and Inventory Requirements*

Commercial National Security Algorithm (CNSA) Suite 1.0, MFS U/00/814670-15

CNSSI 1253, *Security Categorization and Control Selection for National Security Systems*

CNSSP 15, *Use of Public Standards for Secure Information Sharing*

Executive Order 13231, *Critical Infrastructure Protection in the Information Age*

Executive Order 14028, *Improving the Nation's Cybersecurity*

FIPS 140-2, *Security Requirements for Cryptographic Modules*

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*

NIST Computer Security Resource Center (CSRC) Glossary

NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*

NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*

NIST SP 800-39 Revision 1, *Managing Information Security Risk: Organization, Mission, and Information System View*

NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*

NIST SP 800-53A Revision 5, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*

NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*

NIST SP 800-59, *Guideline for Identifying an Information System as a National Security System*

NIST SP 800-82 Revision 3, *Guide to Operational Technology (OT) Security*

NSD 42, *National Policy for the Security of National Security Telecommunications and Information Systems*

NSM-8, *Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems*

ISA and ISASecure Documents

ANSI/ISA-62443-3-3-2013 *Security for industrial automation and control systems Part 3-3: System Security Requirements and security levels*

ANSI/ISA-62443-4-2-2018 *Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components*

ISA/Global Cybersecurity Alliance Joint IIoT Study, *IIoT Component Certification Based on the 62443 Standard*

Academic and Industry Documents and Sites

CVE Details. (2024). *Security Scorecard.* Retrieved from https://www.cvedetails.com/

Hahn, A., Cyprus, J., (et al). (May 2024). The EMB3D Threat Model for Embedded Devices. *MITRE Corporation.* Retrieved from https://emb3d.mitre.org/assets/EMB3D_Paper_v2_2024-05-13.pdf

ICS Advisory Project Dashboard. (2024, December 10). Retrieved from https://www.icsadvisoryproject.com/

MITRE ATT&CK Framework for ICS Matrix. (2024). *MITRE Corporation.* Retrieved from https://attack.mitre.org/matrices/ics/

MITRE EMB3D Threat Model. (2024, May 13). Retrieved from https://emb3d.mitre.org/

Open Worldwide Application Security Project (OWASP). Definitions retrieved from https://owasp.org/

Sapir, M., Katz, U., Moshe, N., Brinzov, S., & Preminger, A. (2022). Evil PLC Attack: Weaponizing PLCS. *Team82, Claroty Research Team White Paper.* Retrieved from https://web-assets.claroty.com/resource-downloads/team82-evil-plc-attack-research-paper-1661285586.pdf

Appendix D: Smart Controller Requirements Mapped to M-M-M NIST Countermeasures

Note: Table blocks highlighted in "yellow" reflect new NSS Component Requirements (CRs) or Requirement Enhancements (REs).

ISA-62443-4-2 Component Security Requirements				Associated M-M-M NIST Countermeasures
FR 1	**Identification and Authentication Control**			
	CR 1.1	**Human User Identification and Authentication**		AC-2, AC-2(7), AC-3, AC-5, AC-6, AC-6(1), AC-6(2), AC-6(5), AC-6(10), AC-18(1), CM-11, IA-2, IA-2(12), IA-4, IA-4(4), IA-5, IA-8, RA-5(5), SC-2, SI-4(20)
		CR 1.1 RE(1)	Unique Identification and Authentication	AC-2, AC-5, AC-6, AC-6(1), AC-6(2), AC-6(5), AC-6(10), AC-18(1), IA-2(5), IA-2(12) IA-4(4), SC-2
		CR 1.1 RE(2)	Multifactor Authentication for all Interfaces	IA-2(1), IA-2(2), IA-2(12)
	CR 1.2	**Software Process and Device Identification and Authentication**		AC-3, AC-17(10), AC-19, CA-3(6), CM-7(5), CM-11, CM-14, IA-3, IA-4, IA-4(4), IA-5, IA-7, IA-8, IA-9, RA-5(5), SI-4(20)
		CR 1.2 RE(1)	Unique Identification and Authentication	IA-3, IA-4(4)
	CR 1.3	**Account Management**		AC-2, AC-3, IA-4, IA-4(4)
	CR 1.4	**Identifier Management**		IA-4, IA-4(4)
	CR 1.5	**Authenticator Management**		IA-5, IA-5(6)
	CR 1.7	**Strength of Password-Based Authentication**		IA-5(1)
	CR 1.8	**Public Key Infrastructure (PKI) Certificates**		IA-2, IA-5, IA-5(2), SC-17
	CR 1.9	**Strength of Public Key-Based Authentication**		IA-5(2)
	CR 1.10	**Authenticator Feedback**		IA-6
	CR 1.11	**Unsuccessful Login Attempts**		AC-7
	CR 1.12	**System Use Notification**		AC-8
	CR 1.14	**Strength of Symmetric Key-Based Authentication**		IA-5
FR 2	**Use Control**			
	CR 2.1	**Authorization Enforcement**		AC-2(7), AC-3, AC-3(4), AC-5, AC-6, AC-6(1), AC-6(2), AC-6(10), AC-17, AC-17(4), AC-17(10), AC-18(1), AC-18(4), AC-19, AU-12(3), CA-3(6), CM-5, CM-5(1), CM-7(5), CM-10, CM-11, IA-2, IA-3, SC-2
		CR 2.1 RE(1)	Authorization Enforcement for all Users	AC-3, AC-18(4), IA-2, IA-3
		CR 2.1 RE(2)	Permission Mapping to Roles	AC-2(7), AC-3, AC-18(4), IA-2, IA-3

ISA-62443-4-2 Component Security Requirements				Associated M-M-M NIST Countermeasures
	CR 2.2	**Wireless Use Control**		AC-18, AC-18(1), AC-18(4), AC-19, RA-5(4)
		CR 2.2 NSS RE(1)	Disabling of Wireless Capabilities	AC-18(3), AC-20(2)
		CR 2.2 NSS RE(2)	Disabling of SSID Broadcast	AC-18
	CR 2.5	**Session Lock-Initiation**		AC-11, AC-11(1), AC-12, AC-12(1), AC-12(2), IA-11
		CR 2.5 NSS RE(1)	Use of Pattern-Hiding Displays	AC-11(1)
	CR 2.6	**Remote Session Termination**		AC-12, AC-12(1), AC-12(2), AC-17(9), MA-4
	CR 2.7	**Concurrent Session Control**		AC-10
	CR 2.8	**Auditable Events**		AC-2(4), AC-2(12), AC-6(9), AC-17(1), AU-2, AU-3, AU-3(1), AU-7, AU-7(1), AU-8, AU-12, AU-12(1), CA-7(4), CM-5(1), CM-6, CM-11, MA-4(1), SI-4, SI-4(12), SI-4(22)
	CR 2.9	**Audit Storage Capacity**		AU-4, AU-5(1)
	CR 2.10	**Response to Audit Processing Failures**		AU-5
	CR 2.11	**Timestamps**		AU-3, AU-8, AU-12(1), SC-45
		CR 2.11 RE(1)	Time Synchronization	AU-3, AU-8, AU-12(1), SC-45
	CR 2.12	**Non-Repudiation**		AU-10
	CR 2 NSS CR(1)	**Restricted Use of Removable Media Devices**		MP-7, SC-41
FR 3	**System Integrity**			
	CR 3.1	**Communication Integrity**		CA-3(6), SC-8, SC-8(1), SC-47
		CR 3.1 RE(1)	Communication Authentication	SC-8
	CR 3.3	**Security Functionality Verification**		CM-6(1)
	CR 3.4	**Software and Information Integrity**		CM-6(1), CM-7(2), SI-7, SI-7(1), SI-7(7), SI-15
		CR 3.4 RE(1)	Authenticity of Software and Information	SI-3, SI-7(1)
	CR 3.5	**Input Validation**		SI-10, SI-10(6)
	CR 3.6	**Deterministic Output**		CP-12, SC-24
	CR 3.7	**Error Handling**		SI-11
	CR 3.8	**Session Integrity**		IA-2(8), SC-8, SC-23, SC-23(1)
	CR 3.9	**Protection of Audit Information**		AU-9, AU-9(4), AU-12(3)

ISA-62443-4-2 Component Security Requirements				Associated M-M-M NIST Countermeasures
FR 4	**Data Confidentiality**			
	CR 4.1	**Information Confidentiality**		AC-19(5), CP-9(8), SC-8, SC-8(1), SI-4(10), SR-12
		CR 4.1 NSS RE(1)	Use of Cryptography to Protect Confidentiality	AC-17(2), AC-18(1), SC-8, SC-8(1), SC-28, SC-28(1)
	CR 4.2	**Information Persistence**		MA-2, MA-3(3), MA-4(3), MP-6, SR-12
	CR 4.3	**Use of Cryptography**		AC-19(5), CP-9(8), SC-13, SC-28(1)
		CR 4.3 NSS RE(1)	Use of Approved Cryptographic Security Measures	AC-18(1), SC-13, SC-28(1)
FR 5	**Restricted Data Flow**			
	CR 5.1	**Network Segmentation**		AC-4, CA-9, SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(7), SC-7(8), SC-7(28)
FR 6	**Timely Response to Event**			
	CR 6.1	**Audit Log Accessibility**		AC-6(9), AU-6, AU-6(4), AU-7, AU-9(6), SI-4(5), SI-4(12), SI-4(20)
	CR 6.2	**Continuous Monitoring**		AC-2(12), AC-6(9), AC-17(1), AU-7, CA-7, CA-7(4), SI-4, SI-4(5), SI-4(12), SI-4(20), SI-7(7), SI-4(22), SI-4(10)
FR 7	**Resource Availability**			
	CR 7.1	**Denial of Service Protection**		SC-5
		CR 7.1 RE(1)	Manage Communication Load from Component	SC-5
	CR 7.2	**Resource Management**		CM-7(2)
	CR 7.3	**Control System Backup**		CM-2(3), CP-9, CP-9(1), CP-9(8)
		CR 7.3 RE(1)	Backup Integrity Verification	CM-2(3), CP-9(1)
	CR 7.4	**Control System Recovery and Reconstitution**		CM-2(3), CP-10, CP-10(2), SR-11(2)
	CR 7.6	**Network and Security Configuration Settings**		AC-18, CM-2(2), CM-6, CM-6(1), SR-11(2)
	CR 7.7	**Least Functionality**		AC-6, AC-6(1), AC-6(2), AC-6(5), CM-7, CM-7(1), CM-7(2), CM-7(5), SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(7), SC-7(8), SC-7(28)
	CR 7.8	**Control System Component Inventory**		CM-2(2), CM-8, CM-8(2), SR-11(2)
EDR	**Embedded Device Requirements (EDR)**			
	EDR 2.4	**Mobile Code**		SC-18, SI-7(1)
		EDR 2.4 RE(1)	Mobile Code Authenticity Check	SI-7
	EDR 2.13	**Use of Physical Diagnostic and Test Interfaces**		MA-2, MA-4, MA-4(1), SR-10, SR-11(2)
		EDR 2.13 RE(1)	Active Monitoring	SI-4

ISA-62443-4-2 Component Security Requirements				Associated M-M-M NIST Countermeasures
	EDR 3.2	**Protection from Malicious Code**		SI-3, SI-4, SI-10(6), SI-16
	EDR 3.10	**Support for Updates**		SI-2
		EDR 3.10 RE(1)	Update Authenticity and Integrity	SI-2, SI-7, SI-7(1)
	EDR 3.11	**Physical Tamper Resistance Guidance**		SI-4(5), SR-10
	EDR 3.12	**Provisioning Product Supplier Roots of Trust**		SR-4
	EDR 3.13	**Provisioning Asset Owner Roots of Trust**		SR-4
	EDR 3.14	**Integrity of the Boot Process**		SI-7(9), SI-7(10)
		EDR 3.14 RE(1)	Authenticity of the Boot Process	SI-7(9), SI-7(10)
NDR	**Network Device Requirements (NDR)**			
	NDR 1.6	**Wireless Access Management**		AC-18, AC-18(1), AC-18(4), AC-19
		NDR 1.6 RE(1)	Unique Identification and Authentication	AC-18
	NDR 1.13	**Access Via Untrusted Networks**		AC-3, AC-17, AC-17(1), AC-17(3), AC-17(4), SC-4, SC-7, SI-4, SI-4(4)
		NDR 1.13 RE(1)	Explicit Access Request Approval	AC-3, AC-17, AC-17(3), AC-17(4)
	NDR 5.2	**Zone Boundary Protection**		AC-3, AC-4, AC-17(3), CA-9, SC-4, SC-7, SC-7(3), SC-7(4), SC-7(5), SC-7(7), SC-7(8), SC-7(28)
		NDR 5.2 RE(1)	Deny All, Permit by Exception	AC-17(3), CA-9, SC-4, SC-7(5)
		NDR 5.2 RE(2)	Island Mode	AC-4, SC-4, SC-7
		NDR 5.2 RE(3)	Fail Close	SC-7(18)
	NDR 5.3	**General Purpose, Person-to-Person Communication Restrictions**		CA-9

Appendix E: M-M-M NIST Countermeasures Mapped to Smart Controller Requirements

Relevant M-M-M NIST Countermeasures		Associated ISA-62443-4-2 Requirements and Recommended NSS Requirements
ID	TITLE	
AC-2	Account Management	CR 1.1, CR 1.1 RE(1), CR 1.3
AC-2(4)	Account Management | Automated Audit Actions	CR 2.8
AC-2(7)	Account Management | Privileged User Accounts	CR 1.1, CR 2.1, CR 2.1 RE(2)
AC-2(12)	Account Management | Account Monitoring for Atypical Usage	CR 2.8, CR 6.2
AC-3	Access Enforcement	CR 1.1, CR 1.2, CR 1.3, CR 2.1, CR 2.1 RE(1), CR 2.1 RE(2), NDR 1.13, NDR 1.13 RE (1), NDR 5.2
AC-3(4)	Access Enforcement | Discretionary Access Control	CR 2.1
AC-4	Information Flow Enforcement	CR 5.1, NDR 5.2, NDR 5.2 RE (2)
AC-5	Separation of Duties	CR 1.1, CR 1.1 RE(1), CR 2.1
AC-6	Least Privilege	CR 1.1, CR 1.1 RE(1), CR 7.7, CR 2.1
AC-6(1)	Least Privilege | Authorize Access to Security Functions	CR 1.1, CR 1.1 RE(1), CR 7.7, CR 2.1
AC-6(2)	Least Privilege | Non-Privileged Access for Non-Security Functions	CR 1.1, CR 1.1 RE(1), CR 7.7, CR 2.1
AC-6(5)	Least Privilege | Privileged Accounts	CR 1.1, CR 1.1 RE(1), CR 7.7
AC-6(9)	Least Privilege | Log Use of Privileged Functions	CR 2.8, CR 6.1, CR 6.2
AC-6(10)	Least Privilege | Prohibit Non-Privileged Users From Executing Privileged Functions	CR 1.1, CR 1.1 RE(1), CR 2.1
AC-7	Unsuccessful Logon Attempts	CR 1.11
AC-8	System Use Notification	CR 1.12
AC-10	Concurrent Session Control	CR 2.7
AC-11	Device Lock	CR 2.5
AC-11(1)	Device Lock | Pattern-Hiding Displays	CR 2.5, CR 2.5 NSS RE(1)
AC-12	Session Termination	CR 2.5, CR 2.6
AC-12(1)	Session Termination | User-Initiated Logouts	CR 2.5, CR 2.6
AC-12(2)	Session Termination | Termination Message	CR 2.5, CR 2.6
AC-17	Remote Access	CR 2.1, NDR 1.13, NDR 1.13(1)
AC-17(1)	Remote Access | Monitoring and Control	CR 2.8, CR 6.2, NDR 1.13

Relevant M-M-M NIST Countermeasures		Associated ISA-62443-4-2 Requirements and Recommended NSS Requirements
ID	TITLE	
AC-17(2)	Remote Access | Protection of Confidentiality and Integrity Using Encryption	CR 4.1 NSS RE(1)
AC-17(3)	Remote Access | Managed Access Control Points	NDR 1.13, NDR 1.13(1), NDR 5.2, NDR 5.2(1)
AC-17(4)	Remote Access | Privileged Commands and Access	CR 2.1, NDR 1.13, NDR 1.13(1)
AC-17(9)	Remote Access | Disconnect or Disable Access	CR 2.6
AC-17(10)	Remote Access | Authenticate Remote Commands	CR 1.2, CR 2.1
AC-18	Wireless Access	CR 2.2, CR 7.6, NDR 1.6, NDR 1.6 RE (1), CR 2.2 NSS RE(2)
AC-18(1)	Wireless Access | Authentication and Encryption	CR 1.1, CR 1.2, CR 1.6, CR 2.1, CR 2.2, CR 4.1 NSS RE(1), NDR 1.6, CR 4.3 NSS RE(1)
AC-18(3)	Wireless Access | Disable Wireless Networking	CR 2.2 NSS RE(1)
AC-18(4)	Wireless Access | Restrict Configurations By Users	CR 2.1, CR 2.1 RE(1), CR 2.1 RE(2), CR 2.2, NDR 1.6
AC-19	Access Control for Mobile Devices	CR 1.2, CR 2.1, CR 2.2, NDR 1.6
AC-19(5)	Access Control for Mobile Devices | Full Device or Container-Based Encryption	CR 4.1, CR 4.3
AU-2	Event Logging	CR 2.8
AU-3	Content of Audit Records	CR 2.8, CR 2.11, CR 2.11 RE(1)
AU-3(1)	Content of Audit Records | Additional Audit Information	CR 2.8
AU-4	Audit Log Storage Capacity	CR 2.9
AU-5	Response to Audit Logging Process Failures	CR 2.10
AU-5(1)	Response to Audit Logging Process Failures | Storage Capacity Warning	CR 2.9
AU-6	Audit Record Review, Analysis, and Reporting	CR 6.1
AU-6(4)	Audit Record Review, Analysis, and Reporting | Central Review and Analysis	CR 6.1
AU-7	Audit Record Reduction and Report Generation	CR 2.8, CR 6.1, CR 6.2
AU-7(1)	Audit Record Reduction and Report Generation | Automatic Processing	CR 2.8
AU-8	Time Stamps	CR 2.8, CR 2.11, CR 2.11 RE(1)
AU-9	Protection of Audit Information	CR 3.9
AU-9(4)	Protection of Audit Information | Access By Subset of Privileged Users	CR 3.9

Relevant M-M-M NIST Countermeasures		Associated ISA-62443-4-2 Requirements and Recommended NSS Requirements
ID	TITLE	
AU-9(6)	Protection of Audit Information | Read-Only Access	CR 6.1
AU-10	Non-Repudiation	CR 2.12
AU-12	Audit Record Generation	CR 2.8
AU-12(1)	Audit Record Generation | System-Wide and Time-Correlated Audit Trail	CR 2.11, CR 2.11 RE(1), CR 2.8
AU-12(3)	Audit Record Generation | Changes By Authorized Individuals	CR 2.1, CR 3.9
CA-3(6)	Information Exchange | Transfer Authorizations	CR 1.2, CR 3.1, CR 2.1
CA-7	Continuous Monitoring	CR 6.2
CA-7(4)	Continuous Monitoring | Risk Monitoring	CR 2.8, CR 6.2
CA-9	Internal System Connections	CR 5.1, NDR 5.2, NDR 5.2(1), NDR 5.3
CM-2(2)	Baseline Configuration | Automation Support for Accuracy and Currency	CR 7.8, CR 7.6
CM-2(3)	Baseline Configuration | Retention of Previous Configurations	CR 7.3 RE(1), CR 7.4, CR 7.3
CM-5	Access Restrictions for Change	CR 2.1
CM-5(1)	Access Restrictions for Change | Automated Access Enforcement and Audit Records	CR 2.8, CR 2.1
CM-6	Configuration Settings	CR 2.8, CR 7.6
CM-6(1)	Configuration Settings | Automated Management, Application, and Verification	CR 3.3, CR 3.4, CR 7.6
CM-7	Least Functionality	CR 7.7
CM-7(1)	Least Functionality | Periodic Review	CR 7.7
CM-7(2)	Least Functionality | Prevent Program Execution	CR 3.4, CR 7.2, CR 7.7
CM-7(5)	Least Functionality | Authorized Software -- Allow by Exception	CR 7.7, CR 1.2, CR 2.1
CM-8(2)	System Component Inventory | Automated Maintenance	CR 7.8
CM-10	Software Usage Restrictions	CR 2.1
CM-11	User-Installed Software	CR 1.2, CR 1.1, CR 2.1, CR 2.8
CM-14	Signed Components	CR 1.2
CP-9	System Backup	CR 7.3
CP-9(1)	System Backup | Testing for Reliability and Integrity	CR 7.3, CR 7.3 RE(1)

Relevant M-M-M NIST Countermeasures		Associated ISA-62443-4-2 Requirements and Recommended NSS Requirements
ID	TITLE	
CP-9(8)	System Backup | Cryptographic Protection	CR 4.1, CR 4.3, CR 7.3,
CP-10	System Recovery and Reconstitution	CR 7.4
CP-10(2)	System Recovery and Reconstitution | Transaction Recovery	CR 7.4
CP-12	Safe Mode	CR 3.6
IA-2	Identification and Authentication (Organizational Users)	CR 1.1, CR 1.8, CR 2.1, CR 2.1 RE(1), CR 2.1 RE(2)
IA-2(1)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts	CR 1.1 RE(2)
IA-2(2)	Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts	CR 1.1 RE(2)
IA-2(5)	Identification and Authentication (Organizational Users) | Individual Authentication With Group Authentication	CR 1.1 RE(1)
IA-2(8)	Identification and Authentication (Organizational Users) | Access to Accounts — Replay Resistant	CR 3.8
IA-2(12)	Identification and Authentication (Organizational Users) | Acceptance of PIV Credentials	CR1.1, CR 1.1 RE(1), CR 1.1 RE(2)
IA-3	Device Identification and Authentication	CR 1.2, CR 1.2 RE(1), CR 2.1 RE(1), CR 2.1 RE(2), CR 2.1
IA-4	Identifier Management	CR 1.2, CR 1.3, CR 1.4, CR 1.1
IA-4(4)	Identifier Management | Identify User Status	CR 1.1 RE(1), CR 1.2, CR 1.3, CR 1.4, CR 1.2 RE(1), CR 1.1
IA-5	Authenticator Management	CR 1.1, CR 1.2, CR 1.5, CR 1.8, CR 1.14
IA-5(1)	Authenticator Management | Password-Based Authentication	CR 1.7
IA-5(2)	Authenticator Management | Public Key-Based Authentication	CR 1.8, CR 1.9
IA-5(6)	Authenticator Management | Protection of Authenticators	CR 1.5
IA-6	Authenticator Feedback	CR 1.10
IA-7	Cryptographic Module Authentication	CR 1.2
IA-8	Identification and Authentication (Non-Organizational Users)	CR 1.1, CR 1.2
IA-9	Service Identification and Authentication	CR 1.2
IA-11	Re-Authentication	CR 2.5
MA-2	Controlled Maintenance	CR 4.2, EDR 2.13
MA-3(3)	Maintenance Tools | Prevent Unauthorized Removal	CR 4.2

Relevant M-M-M NIST Countermeasures		Associated ISA-62443-4-2 Requirements and Recommended NSS Requirements
ID	TITLE	
MA-4	Nonlocal Maintenance	EDR 2.13, CR 2.6
MA-4(1)	Nonlocal Maintenance | Logging and Review	EDR 2.13, CR 2.8
MA-4(3)	Nonlocal Maintenance | Comparable Security and Sanitization	CR 4.2
MP-6	Media Sanitization	CR 4.2
MP-7	Media Use	CR 2 NSS CR (1)
RA-5(4)	Vulnerability Monitoring and Scanning | Discoverable Information	CR 2.2
RA-5(5)	Vulnerability Monitoring and Scanning | Privileged Access	CR 1.1, CR 1.2
SC-4	Information In Shared System Resources	NDR 1.13, NDR 5.2, NDR 5.2 RE (2), NDR 5.2 RE (1)
SC-5	Denial of Service Protection	CR 7.1, CR 7.1 RE(1)
SC-7	Boundary Protection	CR 5.1, CR 7.7, NDR 1.13, NDR 5.2, NDR 5.2 RE (2)
SC-7(3)	Boundary Protection | Access Points	CR 5.1, CR 7.7, NDR 5.2
SC-7(4)	Boundary Protection | External Telecommunications Services	CR 5.1, CR 7.7, NDR 5.2
SC-7(5)	Boundary Protection | Deny By Default — Allow By Exception	CR 5.1, CR 7.7, NDR 5.2 RE (1), NDR 5.2
SC-7(7)	Boundary Protection | Split Tunneling for Remote Devices	CR 5.1, CR 7.7, NDR 5.2
SC-7(8)	Boundary Protection | Route Traffic to Authenticated Proxy Servers	CR 5.1, CR 7.7, NDR 5.2
SC-7(28)	Boundary Protection | Connections to Public Networks	CR 5.1, CR 7.7, NDR 5.2
SC-8	Transmission Confidentiality and Integrity	CR 3.8, CR 4.1, CR 4.1 NSS RE(1), CR 3.1, CR 3.1 RE(1)
SC-8(1)	Transmission Confidentiality and Integrity | Cryptographic Protection	CR 3.1, CR 4.1, CR 4.1 NSS RE(1)
SC-13	Cryptographic Protection	CR 4.3, CR 4.3 NSS RE(1)
SC-17	Public Key Infrastructure Certificates	CR 1.8
SC-18	Mobile Code	EDR 2.4
SC-23	Session Authenticity	CR 3.8
SC-23(1)	Session Authenticity | Invalidate Session Identifiers At Logout	CR 3.8
SC-28	Protection of Information At Rest	CR 4.1 NSS RE(1)
SC-41	Port and I/O Device Access	CR 2 NSS CR(1)

Relevant M-M-M NIST Countermeasures		Associated ISA-62443-4-2 Requirements and Recommended NSS Requirements
ID	TITLE	
SC-45	System Time Synchronization	CR 2.11, CR 2.11 RE(1)
SC-47	Alternate Communications Paths	CR 3.1
SI-2	Flaw Remediation	EDR 3.10, EDR 3.10 RE(1)
SI-3	Malicious Code Protection	CR 3.4 RE(1), EDR 3.2
SI-4	System Monitoring	CR 2.8, CR 6.2, EDR 2.13 RE(1), EDR 3.2, NDR 1.13
SI-4(4)	System Monitoring | Inbound and Outbound Communications Traffic	NDR 1.13
SI-4(5)	System Monitoring | System-Generated Alerts	CR 6.1, CR 6.2, EDR 3.11
SI-4(12)	System Monitoring | Automated Organization-Generated Alerts	CR 2.8, CR 6.1, CR 6.2
SI-4(20)	System Monitoring | Privileged Users	CR 6.1, CR 6.2, CR 1.1, CR 1.2
SI-7	Software, Firmware, and Information Integrity	CR 3.4, EDR 2.4 RE(1), EDR 3.10 RE(1)
SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks	CR 3.4, CR 3.4 RE(1), EDR 2.4 RE(1), EDR 3.10 RE(1)
SI-7(7)	Software, Firmware, and Information Integrity | Integration of Detection and Response	CR 3.4, CR 6.2
SI-7(9)	Software, Firmware, and Information Integrity | Verify Boot Process	EDR 3.14, EDR 3.14 RE(1)
SI-7(10)	Software, Firmware, and Information Integrity | Protection of Boot Firmware	EDR 3.14, EDR 3.14 RE(1)
SC-7(18)	Boundary Protection | Fail Secure	NDR 5.2 RE(3)
SC-24	Fail In Known State	CR 3.6
SI-10	Information Input Validation	CR 3.5
SI-10(6)	Information Input Validation | Injection Prevention	EDR 3.2, CR 3.5
SI-11	Error Handling	CR 3.7
SI-16	Memory Protection	EDR 3.2
SR-10	Inspection of Systems or Components	EDR 2.13, EDR 3.11
SR-11(2)	Component Authenticity | Configuration Control for Component Service and Repair	CR 7.4, CR 7.6, CR 7.8, EDR 2.13
SR-12	Component Disposal	CR 4.1, CR 4.2
SC-2	Separation of System and User Functionality	CR 1.1 RE(1), CR 2.1, CR 1.1

Relevant M-M-M NIST Countermeasures		Associated ISA-62443-4-2 Requirements and Recommended NSS Requirements
ID	**TITLE**	
SI-4(22)	System Monitoring | Unauthorized Network Services	CR 2.8, CR 6.2
SI-15	Information Output Filtering	CR 3.4
AC-20(2)	Use of External Systems | Portable Storage Devices – Restricted Use	CR 2 NSS CR 1
SR-4	Provenance	EDR 3.12, EDR 3.13
SI-4(10)	System Monitoring | Visibility of Encrypted Communications	CR 4.1, CR 6.2
SC-28(1)	Protection of Information At Rest | Cryptographic Protection	CR 4.1 NSS RE(1), CR 4.3, CR 4.3 NSS RE(1)
CM-8	System Component Inventory	CR 7.8
SC-7(18)	Boundary Protection | Fail Secure	NDR 5.2 RE (3)

Appendix F: Summary of Recommended NSS Requirements and Enhancements

NEW NSS Smart Controller Security Requirements				Requirement Description	NSS Security Rationale
FR 2	**Use Control**				
	CR 2.2	**Wireless Use Control**			
		CR 2.2 NSS RE(1)	**Disabling of Wireless Capabilities**	**If a component has wireless capabilities, it must: a) have the capability to physically disable the wireless interfaces via a switch or other means, and b) be disabled by default within the operating system or application settings.**	Within the OT environment, the increasing use of wireless networking places OT implementations at greater risk from adversaries who are in relatively close physical proximity but do not have direct physical access to the equipment. Having wireless access to sensors and final elements allows for direct manipulation of the physical processes within the OT environment, which could potentially render the OT system inoperable. Examples of potential attacks include: Unauthorized client accesses, Denial of Service (DoS) attacks, Man-in-the-Middle attacks, side-channel attacks (through dual-homed connections), IP spoofing, and hijacking. Organizations that manage NSS OT/ICS networks may choose to disable the wireless interfaces within components to reduce these risks. Note: These organizations may prefer to utilize components that do not have built in wireless capabilities.
		CR 2.2 NSS RE(2)	**Disabling of SSID Broadcast**	**If a smart controller has the capability to be a wireless access point, it must have the SSID broadcast disabled by default.**	When SSID broadcast is enabled, the SSID, or network name, is continuously advertised by the wireless access point (AP). This makes the network easily detectable by nearby devices, including those of potential attackers. Disabling SSID broadcasts hides the network from casual scanning, reducing the visibility to unauthorized users who may attempt to gain access.

NEW NSS Smart Controller Security Requirements				Requirement Description	NSS Security Rationale
	CR 2.5	**Session Lock-Initiation**			
		CR 2.5 NSS RE(1)	**Use of Pattern-Hiding Displays**	**When a session lock is initiated, smart controllers with a connected display must have the capability to use configurable pattern-hiding display screens, such as a blank screen, solid colors, clock, or other selectable screen.**	Utilizing pattern-hiding displays conceals sensitive information previously visible on the display screen before the session lock. This reduces the risk of information disclosure to unauthorized individuals within close proximity of the components. Users should be able to configure the pattern hiding display to continuously show information and maintain functionality that is determined to be non-sensitive, critical to the operations, or safety instrumented system information and life safety controls.
	CR 2 NSS CR(1)	**Restricted Use of Removable Media Devices**		**Smart Controllers must provide the capability to restrict the use of unauthorized removable media devices that may connect directly to the smart controller.**	Removable media device types that should be restricted include, but are not limited to, USB devices, laptops, flash drives, SD cards, external hard drives, and other portable storage devices. These media devices may serve as an entry point for malware into OT networks that bypasses traditional network security. Malicious software can be intentionally or inadvertently transferred onto these devices from external sources and then brought into secure network environments, compromising critical systems. Malicious software (e.g., malware, viruses, ransomware) specifically designed to target industrial systems can exploit vulnerabilities in OT systems. Once introduced, malware can spread rapidly across networks, causing operational disruptions, data breaches, or physical damage. By restricting the use of removable media devices, organizations can significantly reduce the attack surface and enhance the security posture of their OT networks. Note: This restriction may be accomplished by logically shutting down available connection ports or physically disabling them.

NEW NSS Smart Controller Security Requirements				Requirement Description	NSS Security Rationale
FR 4	**Data Confidentiality**				
	CR 4.1	**Information Confidentiality**			
		CR 4.1 NSS RE(1)	**Use of Cryptography to Protect Confidentiality**	**Smart controllers must support the capability to encrypt information in transit over all enabled and active external interfaces, as well as information at rest.** **Note: ISA's use of the phrases "information in transit" and "information at rest" is synonymous with the NIST phrases "data in transit" and "data at rest". While the requirement reflects the ISA language, the intent is the same as the aligned NIST countermeasure.**	Protecting information in transit involves encrypting data as it moves from one location to another over any external interface, including both traditional wired networks and wireless communication channels. This includes all protocols, such as routable protocols (e.g., TCP/IP), serial communication (e.g., Modbus RTU), and both internal and external interfaces used for control and monitoring systems. Each level of the network should be safeguarded to ensure confidentiality and integrity, whether it is the data traveling across local network boundaries, between control systems, or externally over remote access links. Encryption must extend to these varying transmission methods, whether the data is passing through physical cables or wireless signals, and includes data sent between industrial equipment or to remote devices. Protecting information at rest involves encrypting data that is stored on physical media, such as hard drives, databases, or any other storage devices, awaiting retrieval or use. This type of data is not actively being transferred but must still be protected from unauthorized access. The implementation of security architecture and encryption technologies must not degrade the operational performance of the end devices within the OT enclave. Exemptions for the requirement are permitted if the encrypted information at rest would greatly impact processing times. Examples of this are the operating system files and other files needed for the boot process. Encryption technologies must meet CR 4.3 NSS RE (1) requirements.

NEW NSS Smart Controller Security Requirements				Requirement Description	NSS Security Rationale
	CR 4.3	**Use of Cryptography**			
		CR 4.3 NSS RE(1)	**Use of Approved Cryptographic Security Measures**	**Smart Controllers must utilize NSA-approved cryptographic security mechanisms.**	Cryptography is fundamental to securing critical infrastructure systems that support the mission-critical services essential for the operation of NSS. By leveraging approved cryptologic algorithms listed in the Commercial National Security Algorithm (CNSA) suite (see CNSS Policy 15) and Federal Information Processing Standards (FIPS) 140-2 or newer, these systems are fortified against advanced and evolving cyber threats. These cryptographic frameworks provide robust protection for data both in transit and at rest, mitigating the risks of unauthorized access, tampering, and data breaches. To maintain long-term resilience, cryptographic agility is crucial. This means the ability to adapt and migrate to stronger cryptographic algorithms and protocols as they evolve over time, ensuring the systems remain secure against future threats. Additionally, utilizing secure OT communication protocols further reinforces the integrity and security of critical infrastructure systems, ensuring that all data exchanges and remote operations are safeguarded. Note: Deprecated algorithms, such as SSL, 3DES, and SSH 1.0, should be avoided. These outdated algorithms have known vulnerabilities that can be exploited by cyber adversaries, posing significant risks to both the integrity of systems and national security.