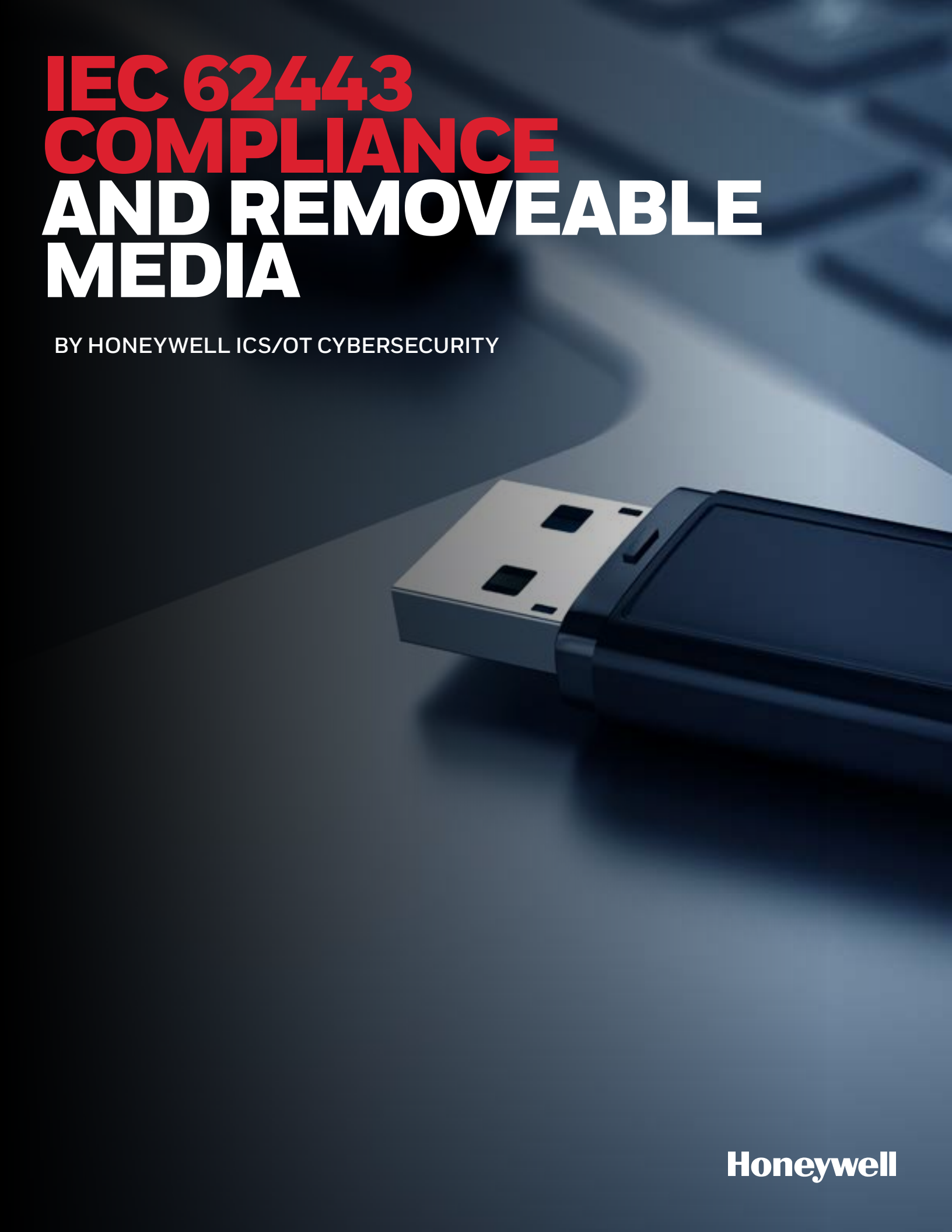
IEC 62443 COMPLIANCE AND REMOVEABLE MEDIA

BY HONEYWELL ICS/OT CYBERSECURITY



Honeywell

TABLE OF CONTENTS

ACHIEVING 62443 COMPLIANCE

REDUCING RISK OF PORTABLE MEDIA AND MALICIOUS CODE

Cybersecurity risks to industrial control systems (ICS) and operational technology (OT) are changing rapidly. Targeted ransomware, supply chain attacks and the weekly discovery of new vulnerabilities are juxtaposed with constant pressure from companies to reduce costs, increase efficiency, and bring cybersecurity spending under closer scrutiny. Every day requires hours of learning about threats and attacks, and the more we know, the more eager we are to minimize our cybersecurity risks. There appears to be a direct correlation between cybersecurity threat awareness and the willingness to mitigate cybersecurity risks proactively.

CYBERSECURITY AWARENESS

COMPANY 1

Unaware of Cybersecurity Risks & Threats

- Less likely to mitigate, as cybersecurity is abstract or foreign concept
- Managers, Leaders

COMPANY 2

Informed of Cybersecurity Risks & Threats

- Compelled to mitigate, knowing how others are attacked
- Cybersecurity Professionals Engineering

Those informed are more willing to proactively mitigate cybersecurity spending.
Decision-making and priorities are influenced by awareness and experience of cyber attacks

THE IMPORTANT ROLE OF CYBERSECURITY STANDARDS

1

Types of Documents

- Concepts, terminology, models, metrics
- Security program requirements
- Supplier requirements
- Implementation guidance
- Risk assessment
- System design and engineering
- Certification of development
- Systems and components
- And more

2

Applicable Audiences

- Asset owners & operators
- ICS/OT product suppliers
- ICS/OT product integrators
- EPCS
- Service providers
- Consultants
- Cybersecurity product suppliers

3

Use Cases & Lifecycle

- Risk assessment
- Security levels based on threat level
- Specification
- Design
- Configuration
- Testing
- Patch management
- Audit & compliance
- And more

When decision-makers have two approaches to cybersecurity risk, they are more likely to choose an external standard over the advice of their staff.

A working group of industry experts from different industries, regions, and experience levels develops ISA/ISO/IEC 62443 standards. Around 2001, the International Society of Automation (ISA) formed a committee (also called ISA99) on industrial cybersecurity and produced its first technical report (TR1). ISA99 has evolved and is now commonly known as 62443, with its agreements with ANSI, IEC, and ISO. It is the only standard with over 20 years of experience and worldwide recognition by ISA, ANSI, IEC, and ISO. Using these 62443 standards adds depth and credibility to those who utilize them.

The ISA99 committee has several documents planned in the series; ome have been published, but many are under development and revision. Unlike country- or industry-specific guides, each document meets the needs of different audiences, use cases, and ICS/OT lifecycles.

The standard most commonly used in ICS/OT development is 62443-3-3: "Security for Industrial Automation and Control Systems - Part 3-3: System Security Requirements and Security Levels."[1] Part 3-3 provides a list of security controls that should be part of an ICS/OT system, and the security levels correspond to the threat level they are intended to mitigate. These include recommended security controls for authentication, access control, authorization, usage control, cryptography, and network security, among others.

There is also the 62443-2-1 standard: "Part 2-1: Security Program Requirements for IACS Facility Owners." Part 2-1 provides a requirements framework that facility owners can use to evaluate, plan, implement, and measure the effectiveness of their cybersecurity management system (CSMS) for ICS/OT. The published 2009 version and the latest ISA99 Working Group (WG2) draft currently being developed should be referenced.

These standards can help internal staff justify their cybersecurity efforts by identifying gaps where their system or security program does not meet the requirements of 62443. When decision-makers see that they are behind in implementing industry standards, it makes a more compelling argument for funding improved cybersecurity measures.

PORTABLE MEDIA WITH MALICIOUS CODE CONTINUES TO BE A TOP ATTACK VECTOR

In addition to network connectivity, portable USB storage devices with malicious code are a vital cybersecurity attack vector and a common denominator in attacks on airborne systems.[2]

Universal Serial Bus (USB) ports are included in virtually every cyber asset, as they are needed to support peripherals such as keyboards and mice but are also practical for networking, audio, video, printers, and storage. USB ports are ubiquitous, as are USB storage devices that allow files to be quickly and easily transferred from one system to another.

Unfortunately, cyber researchers and attackers have realized how they can use USB storage devices to inject malicious code into systems they want to attack. In practice, many USB attack platforms (UAPs) take advantage of USB ports.

Illustration 2: Secure Media Exchange, SMX

79%

OF THREATS HAVE THE POTENTIAL TO CAUSE A MAJOR DISRUPTION IN ICS

30%

INCREASE YEAR OVER YEAR OF USB USE IN PRODUCTION FACILITIES

37%

OF THREATS DESIGNED TO LEVERAGE REMOVABLE MEDIA

45%

TOTAL # OF USB THREATS REMAIN CONSISTENT (FROM 44%)

[2] ISA-62443-2-1 draft "Security Program Requirements" draft subject to change, Copyright © ISA, used with permission, www.isa.org on Secure Media Exchange (SMX) ›

USB ATTACK PLATFORMS (UAPS)

Plug-and-Deploy UAPs

Execute attack upon insertion

- Rubber Ducky
- Bash Bunny
- USB Chaos Drive

Remote Access UAPs

Leverage wireless communication for command & control

- Key Croc
- Keysweeper
- O.MG Cable

UAP Appliances

Comprehensive exploitation toolkits

- P4WNP1 A.L.O.A.
- Kali NetHunter
- USB Armory (Mk II)

CHALLENGES WITH USB SECURITY:

- USB ports are not completely disabled; they are needed for the keyboard and mouse.
- By default, all USB device types are trusted by the operating system and set up automatically.
- USB has replaced floppy disks, CDs, and DVDs for transferring information.
- Portable USB storage devices may contain software-based threats in the files on the storage media.
- USB devices may contain hardware-based attacks hidden in the firmware or hardware chips. Since all USB device types are trusted, they can appear to the user as storage devices and hide keystrokes, network, and microphone functions.
- It is difficult to restrict the use of USB and portable media.
- Domain-level controls (e.g., GPO) and policies can be easily bypassed by malware and UAPs.
- Antivirus solutions cannot detect or prevent hardware-based attacks hidden in USB.
- Even harder to report and manage

As mentioned earlier, portable USB storage devices are among the top four threats, and security professionals and engineers must continue to impress upon their executives the importance of mitigating the associated risks. The information above should reveal the risks to your organization and why continuous improvement is needed.

* ESET 2021 report on malware frameworks used to target air-gapped systems.

A REFERENCE TO 62443

The Following Requirements Are Associated With Portable Media And Malicious Code:

62443-3-3 SR 2.3	Use control for portable and mobile devices
62443-3-3 SR 2.3 (1)	Enforcement of security status of portable and mobile devices
62443-3-3 SR 2.4	Mobile code
62443-3-3 SR 2.4 (1)	Mobile code integrity check
62443-3-3 SR 3.1 (1)	Cryptographic integrity protection
62443-3-3 SR 3.2	Malicious code protection
62443-3-3 SR 3.2 (1)	Malicious code protection on entry and exit points
62443-3-3 SR 3.2 (2)	Central management and reporting for malicious code protection
62443-3-3 SR 3.4	Software and information integrity
62443-2-1-Draft COMP 2.1	Verify portable media is free of malware
62443-2-1-Draft COMP 2.2	All devices shall have malware protection
62443-2-1-Draft COMP 2.3	Validate malware protections and timely installation

If the ICS/OT system does not have these capabilities, asset owners, integrators, and consultants must find third-party solutions to add these compensating controls. The Honeywell Secure Media Exchange (SMX) solution helps meet these requirements.

THE HONEYWELL SECURE MEDIA EXCHANGE (SMX) SOLUTION

SMX is a removable media security solution that provides operators with control and visibility to more securely use USB storage devices and USB devices with the latest advanced threat detection.

Honeywell SMX can help you address challenges associated with USB security

- USB storage devices are first scanned by the SMX Gateway to detect the presence of file-based threats.
- Within the critical system, the SMX TRUST client better protects USB ports from hardware- and firmware-based threats from malicious USB attack tools, keyboards, and mice and restricts the use of other device types based on their role and configuration rules.
- The SMX TRUST client driver is designed to prevent portable storage devices from being connected to the system that an SMX Gateway has not previously scanned. This measure prevents bypassing the SMX Gateway, which serves as a defense-in-depth layer.
- Full auditing and logging of all devices, files, and malware detection results are possible via a central Enterprise Threat Management portal and the local SMX TRUST client.
- Increase efficiency and visibility into all USB device usage with the Enterprise Threat Management portal. Create custom file policies to whitelist common patches or updates and blacklist new industry-targeted malware. User accounts ensure that all employees see only the necessary logs and data.

Features alone do not justify improved controls for portable media; decision-makers want to know how they support 62443.

HOW SMX HELPS SUPPORT 62443

OVERVIEW

62443-3-3	FR2 - USE CONTROL
SR 2.3	Usage control for portable and mobile devices
SR 2.3 (1)	Enforcement of security status of portable and mobile devices
SR 2.4	Mobile code
SR 2.4 (1)	Mobile code integrity verification

62443-3-3	FR3 - SYSTEM INTEGRITY
SR 3.1 (1)	Cryptographic integrity protection
SR 3.2	Protection against malicious code
SR 3.2 (1)	Protection against malicious code at entry and exit points
SR 3.2 (2)	Centralized management and reporting of malicious code protection
SR 3.4	Software and information integrity

62443-2-1 (DRAFT)	COMP 2 - MALWARE PROTECTION
COMP 2.1	Malware-free
COMP 2.2	Protection against malicious software
COMP 2.3	Validation and installation of software to protect against malicious software

FR2 - USE CONTROL

REQUIREMENT	REQUIREMENT NAME	HOW SMX CAN HELP MEET THIS REQUIREMENT FOR THE ENTIRE ICS/OT SYSTEM
SR 2.3	Use control for portable and mobile devices	A. The TRUST driver installed on the endpoints assists with enforcement and prevents unauthorized and unscanned media from being read or accessed by the ICS. B. The TRUST driver enables the configuration of restrictions for portable and mobile USB devices based on contextual factors such as user, device type, and time of connection. C. SMX Gateways scan portable storage media for malicious code and authorize the media for use within the ICS.
SR 2.3 (1)	Enforcement of the security status of portable and mobile devices	Following SR 2.1, the SMX Gateways can be connected to one or more endpoints with the TRUST driver, controlling which SMX Gateways can authorize files for security zones of the ICS.
SR 2.4	Mobile code	A. SMX Gateways are the malicious code scanning checkpoints connected to Honeywell's Enterprise Threat Management Portal and GARD Threat Engine. B. Using user-defined file policies (file whitelist), the system scans for malicious or untrusted code and prevents it from being allowed for use. C. The SMX client prevents the transmission of code. D. Reports on checked-in files and client file access logs are available in the threat portal.
SR 2.4 (1)	Mobile code integrity check	The SMX system looks for malicious or untrusted code and prevents an endpoint from being accessed with the TRUST driver.

FR3 - SYSTEM INTEGRITY

REQUIREMENT	REQUIREMENT NAME	HOW SMX CAN HELP MEET THIS REQUIREMENT FOR THE ENTIRE ICS/OT SYSTEM
SR 3.1 (1)	Cryptographic integrity protection	Data on portable media is "checked in" at the SMX Gateway, and file integrity hashes are created and cryptographically signed. This enables the detection of tampering or changes to files on the USB media before it is plugged into an endpoint running the TRUST driver.
SR 3.2	Protection against malicious code	The SMX Gateway scans portable USB media as it moves in and out of the ICS. The Gateway helps detect and prevent malicious code as it is checked into the ICS; it also detects malicious code that may have been acquired as it is checked out of the ICS. Reporting on all SMX Gateway scanning activity is available in the Enterprise Threat Detection Portal. SMX gateways are connected to our GARD Threat Engine and receive continuously updated virus definitions.
SR 3.2 (1)	Protection against malicious code at entry and exit points	The TRUST driver is a USB driver replacement currently available for Microsoft Windows. It prevents hardware- and software-based malicious threats on all Microsoft Windows devices when deployed. We are evaluating market demand for drivers for other platforms (e.g., Linux).
SR 3.2 (2)	Centralized management and reporting for malicious code protection	All SMX Gateway scan results from the ICS are available online in the Honeywell Enterprise Threat Portal. Logs are available to track authorized and unauthorized USB media use at the site where the TRUST driver is deployed. We are currently evaluating market demand for centralized management and deployment of the TRUST driver across multiple endpoints.
SR 3.4	Software and information integrity	Data on portable media is "checked in" at the SMX Gateway, and file integrity hashes are created and cryptographically signed. This enables the detection of tampering or changes to files on the USB media before it is plugged into an endpoint running the TRUST driver.

COMP 2 - MALWARE PROTECTION

REQUIREMENT	REQUIREMENT NAME	HOW SMX CAN HELP MEET THIS REQUIREMENT FOR THE ENTIRE ICS/OT SYSTEM
COMP 2.1	Malware free	As described in SR 3.2, the SMX Gateway scans portable media for malware and marks it as "checked in." Only checked-in media is allowed in the ICS, and the TRUST driver enforces this.
COMP 2.2	Malware protection	SMX Gateways can detect malicious software on behalf of devices that do not have anti-malware software installed. If more than half of the devices do not support antivirus, SMX can detect malicious software before it is connected to the critical ICS/OT.
COMP 2.3	Validation and installation of malware protection software	SMX Gateways can be constantly connected to Honeywell's Enterprise Threat Management Portal and GARD Threat Engine to ensure the latest protections and seamless updates. Because the SMX Gateway is external to the ICS/OT system, there is virtually no need to test malware definition files directly on the ICS/OT. By utilizing the latest threat intelligence, Honeywell's ICS/OT is better protected.

FR2 - USE CONTROL

REQUIREMENT	REQUIREMENT NAME	REQUIREMENT TEST	SECURITY LEVEL	HOW SMX HELPS FULFILL THE REQUEST ON BEHALF OF THE ZONE, CONDUIT, COMPONENT, OR SYSTEM.
		Part 3-3		
SR 2.3	Use control for portable and mobile devices	The control system shall provide the ability to enforce automatically configurable usage restrictions that include the following: A. Preventing the use of portable and mobile devices; B. Requiring context-specific authorization; and C. Restricting the transfer of code and data to/from portable and mobile devices.	SL1	A. The TRUST driver installed on the end devices assists in enforcement and prevents unauthorized and unscanned media from being read or accessed by the ICS. B. The TRUST driver enables the configuration of restrictions for portable and mobile USB devices based on contextual factors such as user, device type, and time of connection. C. SMX Gateways scan portable storage media for malicious code and authorize the media for use within the ICS.
SR 2.3 (1)	Enforcement of the security status of portable and mobile devices	The control system must provide the ability to verify that portable or mobile devices attempting to connect to a zone meet the security requirements of that zone.	SL3	Following SR 2.1, the SMX Gateways can be connected to one or more endpoints with the TRUST driver, controlling which SMX Gateways can authorize files for security zones of the ICS.
SR 2.4	Mobile code	The control system shall provide the ability to enforce usage restrictions on mobile code technologies based on the potential for harm to the control system, which shall include: A. Preventing the execution of mobile code; B. Requiring proper authentication and authorization for the origin of the code; C. Restricting the transfer of mobile code to/from the control system; and D. Monitoring the use of mobile code.	SL1	A. SMX Gateways are the checkpoints for malicious code scanning connected to Honeywell's Enterprise Threat Management Portal and GARD. B. Using user-defined file policies (file whitelist), the system scans for malicious or untrusted code and prevents it from being allowed for use. C. The SMX client prevents the transmission of code. D. Reports on checked-in files and client file access logs are available in the threat portal.
SR 2.4 (1)	Integrity check of the mobile code	The control system must provide the ability to verify the integrity of the mobile code before allowing the code to execute.	SL3	The SMX system looks for malicious or untrusted code and prevents an endpoint from being accessed with the TRUST driver.

FR3 - SYSTEM INTEGRITY

REQUIREMENT	REQUIREMENT NAME	REQUIREMENT TEST	SECURITY LEVEL	HOW SMX HELPS FULFILL THE REQUEST ON BEHALF OF THE ZONE, CONDUIT, COMPONENT, OR SYSTEM.
		Part 3-3		
SR 3.1 (1)	Cryptographic integrity protection	The control system shall provide the capability to use cryptographic mechanisms to detect changes to information during communications. Note: The use of cryptographic mechanisms for message authentication and integrity should be determined after careful consideration of the security requirements and the potential impact on system performance and the ability to recover from a system failure.	SL3	Data on portable media is "checked in" at the SMX gateway, and file integrity hashes are created and cryptographically signed. By using this feature, any tampering or alterations made to files on USB media can be detected prior to being plugged into an endpoint that is running the TRUST driver.
SR 3.2	Protection against malicious code	The control system must be able to employ protection mechanisms to prevent, detect, report, and mitigate the effects of malicious code or unauthorized software. The control system must provide the ability to update the protection mechanisms.	SL1	The SMX Gateway scans portable USB media as it moves in and out of the ICS. The Gateway helps detect and prevent malicious code as it is checked into the ICS; it also detects malicious code that may have been acquired as it is checked out of the ICS. Reporting on all SMX Gateway scanning activity is available in the Enterprise Threat Detection Portal. SMX Gateways are connected to our GARD Threat Engine at all times and receive continuously updated virus definitions that are constantly improved by our AI/ML capabilities.
SR 3.2 (1)	Protection against malicious code at entry and exit points	The control system must be able to deploy protection mechanisms against malicious code at all entry and exit points. Note: Mechanisms at this level may include removable media, firewalls, unidirectional gateways, web servers, proxy servers, and remote access servers.	SL2	The TRUST driver is a USB driver replacement currently available for Microsoft Windows. It prevents hardware- and software-based malicious threats on all Microsoft Windows devices when deployed. We are evaluating market demand for drivers for other platforms (e.g., Linux).
SR 3.2 (2)	Centralized management and reporting for malicious code protection	The control system must provide the ability to manage mechanisms to protect against malicious code. Note: Such mechanisms can be provided by centralized endpoint infrastructure management and SIEM solutions.	SL3	All SMX Gateway scan results coming in and out of the ICS are available online in the Honeywell's Enterprise Threat Portal. At the site where the TRUST driver is deployed, logs are available to track authorized and unauthorized USB media use. We are currently evaluating market demand for centralized management and deployment of the TRUST driver across multiple endpoints.
SR 3.4	Software and information integrity	The control system must be able to detect, record, report, and protect against unauthorized software changes and stored information.	SL2	Data on portable media is "checked in" at the SMX Gateway, and file integrity hashes are created and cryptographically signed. This enables the detection of tampering or changes to files on the USB media before it is plugged into an endpoint running the TRUST driver.

COMP 2 - MALWARE PROTECTION

REQUIREMENT	REQUIREMENT NAME	REQUIREMENT TEST	SECURITY LEVEL	HOW SMX HELPS FULFILL THE REQUEST ON BEHALF OF THE ZONE, CONDUIT, COMPONENT, OR SYSTEM.
Part 2-1				
COMP 2.1	Malware free	The facility owner must ensure that all devices and portable media (if they are approved for use in IACS) are checked to ensure that they are free of known malware before their use in IACS.	n/a	As described in SR 3.2, the SMX Gateway scans portable media for malware and marks it as "checked in." Only checked-in media is allowed in the ICS, and the TRUST driver enforces this.
COMP 2.2	Malware protection	The facility owner must ensure that, to the extent possible, all equipment has malware protection software installed that has been verified to detect and respond to known malware and has been tested for compatibility with the equipment.	n/a	SMX Gateways can detect malicious software on behalf of devices that do not have anti-malware software installed. If more than half of the devices do not support antivirus, SMX can detect malicious software before it is connected to the critical ICS/OT.
COMP 2.3	Validation and installation of malware protection software	The asset owner shall ensure that malware protection software and its malware definition files are tested for compatibility with IACS before installation, approved for installation, and promptly installed once approved.	n/a	SMX Gateways can be constantly connected to Honeywell's Enterprise Threat Management Portal and GARD Threat Engine to ensure the latest protections and seamless updates. Because the SMX Gateway is external to the ICS/OT system, there is virtually no need to test malware definition files directly on the ICS/OT. By utilizing the latest threat intelligence, Honeywell's ICS/OT is better protected..

HOW HONEYWELL CAN HELP

Cybersecurity solutions help protect OT-based assets, operations, and people from digital age threats. With over 20 years of industrial cybersecurity experience and over 50 years of industrial experience, Honeywell can help your company understand the complexities of today's IT/OT cybersecurity and reduce your cyber risk. We provide innovative cybersecurity software, services, and solutions to protect assets, operations, and people at thousands of industrial facilities and critical infrastructure sites worldwide.

Our vendor-neutral solutions go far beyond Honeywell's proprietary devices and equipment to help protect all assets on your ICS network.

HONEYWELL CYBERSECURITY SOLUTIONS FOR ICS/OT		
ICS/OT Cybersecurity Products	**Cybersecurity Consulting Services**	**Managed Security Services**
Secure remote access Active-passive detection and monitoring of assets Network and file-based threat detection Risk and compliance management Patch, av and backup management Centralized management and reporting	Assessments & audits Architecture & design Network security Endpoint protection Situational awareness Training Response & recovery	Rapidly deployed managed service Industrial grade secure remote access Industrial-grade 24/7 Proactive threat detection & response
Full OT Cybersecurity Lifecycle: Assess > Advise > Design > Install > Test > Validate > Support > Audit and other services		

This document describes Honeywell's best practices and solutions for portable USB media and malicious code prevention to help you implement and comply with ISA/ISO/IEC 62443 cybersecurity standards for your industrial control systems (ICS) and operational technology (OT).

Learn how Honeywell's Secure Media Exchange (SMX) solution can help you better mitigate USB portable media and malicious code risks while complying with 62443 standards).

For more information
www.honeywellforge.ai

Honeywell Connected Enterprise
715 Peachtree Street NE
Atlanta, Georgia 30308

White Paper | Rev | 11/23

THE FUTURE IS WHAT WE MAKE IT

Honeywell