Integration guide

Guide to secure device integration

Anybus embedded network interfaces

Part 1: Cybersecurity regulation and standards for Industrial automation devices

Part 2: Cybersecurity at HMS Networks

Part 3: Best practices and secure integration

Preface

BACKGROUND

In the context of ongoing industrial digitalization, industrial networks now connect machines far beyond a factory's four walls, increasing the access and potential threats to these devices.

New regulations, like the Cyber Resilience Act (CRA), have also been issued to increase awareness and importance of cybersecurity to protect the local industry.

Consequently, cybersecurity has become a mandatory consideration when integrating industrial communication interfaces, to guarantee reliable communication as well as compliance with security regulations.

Over the years, HMS Networks have closely followed the increasing demand for enhanced cybersecurity and responded by strengthening company processes and enhancing product robustness. This proactive approach has made it easier for customers to implement secure communication interface.

DOCUMENT PURPOSE

This document serves as a guide for manufacturers integrating the Anybus Embedded network interfaces into their industrial products.

This guide is composed of 3 main parts:

PART 1: Overview of the current cyber-security regulations and standards

PART 2: Cybersecurity at HMS Networks and processes followed by an overview of cybersecurity measures implemented in our solutions.

PART 3: A guide for device manufacturers on the best way to address current security expectations.

PART 1: Cybersecurity regulation and standards for industrial automation devices

As automation device manufacturers, implementing a Cybersecurity initiative is a good practice to increase product reliability and minimize potential financial and reputation losses. But nowadays, with the release of several cybersecurity regulations like CRA impacting products with communication capabilities and regulations like NIS2 impacting production and infrastructure facilities, implementing a cybersecurity strategy is not optional anymore but mandatory.

Most of these regulations still require clarification and the publication of harmonized standards are pending. This creates uncertainty for device manufacturers and machine builders which need time to adapt their portfolio and ensure compliance.

- In this part you will find a first section with the direct regulations impacting devices with communication interfaces but also indirect regulations that impact manufacturers through their own users (purchasing requirements).
- A second chapter will cover some existing cybersecurity standards that can guide already today and an initial cybersecurity strategy for industrial device manufacturers.

But to ease the burden of cyber security compliance, HMS Networks monitors these activities and implements measures to address all necessary requirements and provides ready to use and pre-certified network interfaces for industrial devices. The use of our communication solutions reduces significantly the cybersecurity implementation efforts but also the constant and detailed vulnerability monitoring and security maintenance.

1. Regulatory and purchasing requirements

Implementing cybersecurity routines is by itself a good practice for device manufactures. It increases product reliability and minimizes potential financial and reputation losses. So far, the appropriate level of cybersecurity has been the choice of each device manufacturer. With new regulations such as CRA and NIS2 cybersecurity is no longer optional, it has become mandatory.

In this chapter we address the most important cyber security regulations which directly or indirectly affect device manufacturers. In the next chapter we will analyze the technical standards available to show compliance with the regulations.

NIS2: CYBERSECURITY FOR NETWORK AND INFORMATION SYSTEMS

The EU directive known as NIS2 has replaced its predecessor NIS1. NIS1 covered cybersecurity requirements for infrastructure within energy, transport, healthcare, finance, water management, and digital infrastructure.

NIS2 additionally covers providers of public electronic communications, more digital services, waste and wastewater management, critical product manufacturing, postal and courier services, and public administration at both central and regional levels, as well as the space sector.

Medium-sized and large entities in these sectors will have to take appropriate cybersecurity risk-management measures and notify relevant national authorities of significant incidents.

European Union member states were required to transpose NIS2 into national law by 17 October 2024. 19 member states missed the deadline, and the European Commission has initiated infringement procedures against these countries.

Still NIS2 is making its impact on many organizations within the European Union. In contrast with CRA and RED cybersecurity, NIS2 does not have any harmonized standards which can be used to demonstrate presumption of conformity with the regulation. Instead, more detailed requirements are determined by each member state.

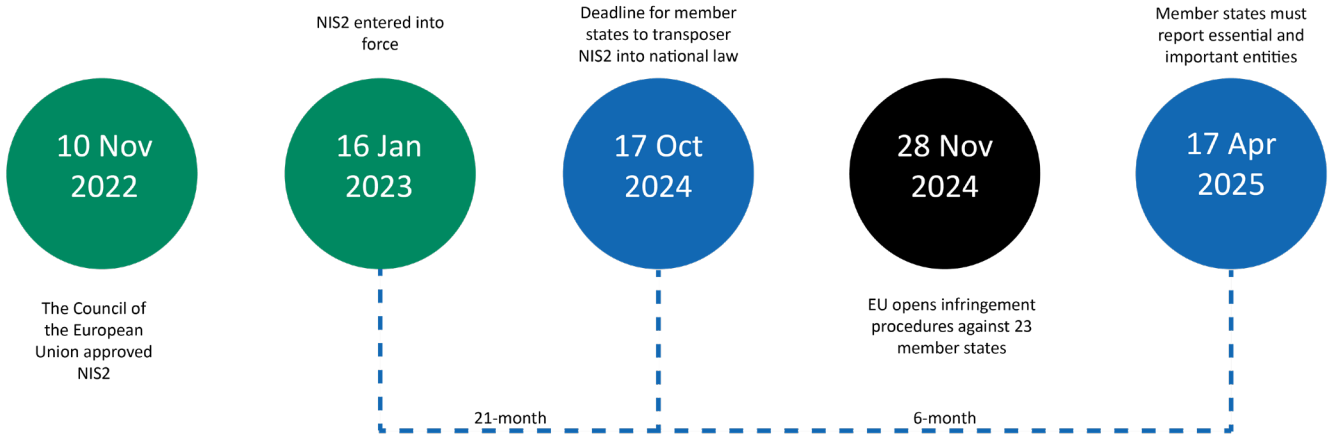

Figure 1. Key milestones for NIS2 implementation and enforcement in the EU.

With regards to IT cybersecurity, ISO 27001 is often used to demonstrate compliance with NIS2. ISO 27001 has good coverage with regards to IT systems, personnel and physical security. ISO 27001, however, is not so suitable for operational technology. For operational technology the IEC 62443 series of standards are often used to demonstrate compliance.

Device manufacturers and machine builders are normally not directly impacted by NIS2. They are, however, impacted indirectly by requirements from customers in scope of NIS2. Often the requirements to device manufacturers and machine builders are based on IEC62443 standards.

THE CYBER RESILIENCE ACT: A BROADER CYBERSECURITY FRAMEWORK FOR CONNECTED PRODUCTS

The EU Cyber Resilience Act (CRA) introduces mandatory cybersecurity requirements for all products with digital elements sold in the European Market.

It impacts manufacturers globally, requiring them to design secure products, manage vulnerabilities, and provide updates throughout the device lifecycle, and for at least five years.

From Sept. 2026, manufacturers must report actively exploited vulnerabilities and severe incidents. Full compliance becomes mandatory by 11 December 2027, including technical documentation, conformity assessments, and a Software Bill of Materials (SBOM).

The CRA also classifies products into categories with different criticality, impacting the way the compliance will be assessed. There is no grandfathering, individual products produced after the deadline must comply with the new legislation, even if development was completed before the deadline.

The European Commission has requested harmonized standards to be developed to clarify the interpretation of the regulation. The standards are also needed in order to demonstrate conformity to CRA. It is part of the request that the CRA harmonized standards should be based on the harmonized standards for RED Cybersecurity.

As of mid-2025, however, these standards are still under development, causing uncertainty among manufacturers who must prepare already today to meet the CRA deadline.

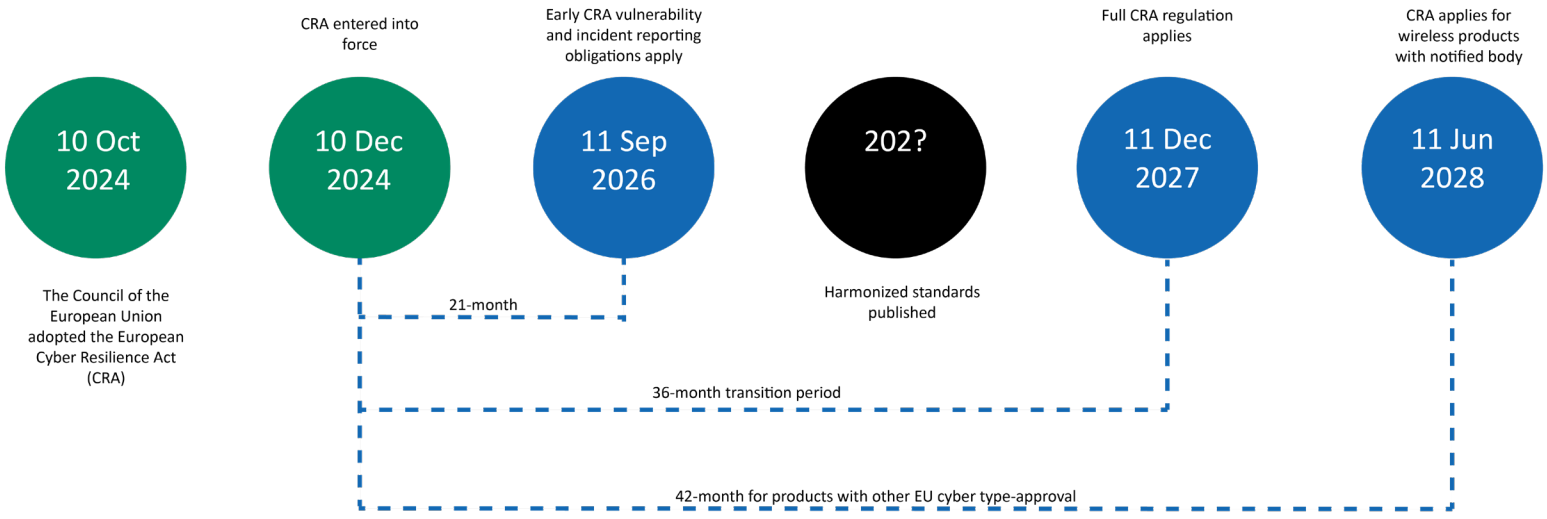

Figure 2. Timeline of key milestones for Cyber Resilience Act (CRA).

Consider a wastewater processing facility with separate stations for pumping, coagulation, sedimentation, filtration, etc. (Processes A, B, C, D), each with their own input/output (I/O) devices, PLCs, and Variable Frequency Drives (VFDs). Those process systems and their control devices – VFDs, PLCs, SCADA systems, etc. – sit at Levels 0-3.

However, many water and wastewater providers maintain flat networks with no divisions between the different processes in the Control Zone. The problem is that a device plugged in at any of the remote stations can access every other part of the facility.

This ease of connectivity is a major security risk and can lead to intentional or unintentional compromise. An employee laptop infected with malware connected to the filtration PLC, for

THE RED DIRECTIVE: STRENGTHENING CYBERSECURITY FOR WIRELESS PRODUCTS

The Radio Equipment Directive (RED) is an existing EU regulation that ensures radio equipment, such as wireless communication devices, meets health, safety, and electromagnetic compatibility requirements.

In 2021, the Delegated Regulation (EU) 2022/30 activated the essential cybersecurity requirements of the RED directive.

The requirements apply to wireless products that can connect to the Internet. These requirements apply from August 1, 2025. While industrial wired devices are not by themselves in scope of the RED Cybersecurity requirements they come in scope in case the industrial device integrates wireless connectively.

So, if for example an industrial device features wireless configuration using tablets or smartphones then the whole device may be in scope of the RED cybersecurity requirements.

Manufacturers must ensure that wireless-enabled products, including industrial devices with Wi-Fi, Bluetooth, or cellular connectivity, have safeguards to protect personal data, prevent unauthorized access, and ensure network resilience.

For factory automation, this means that connected devices used in industrial settings will need built-in cybersecurity features to meet RED compliance. This affects everything from wireless gateways to edge devices, especially those interfacing with cloud systems or user networks.

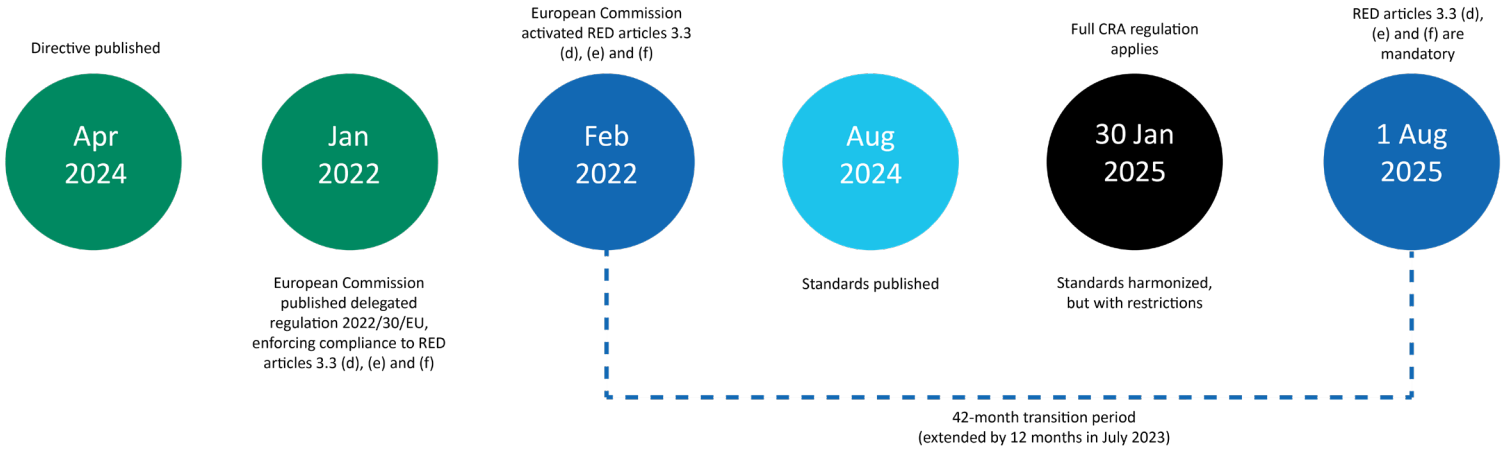

Figure 3. Key milestones for the Radio Equipment Directive (RED) cybersecurity requirements.

PURCHASING REQUIREMENTS FOR CYBERSECURITY

Larger companies and government organizations commonly have purchasing requirements on cybersecurity.

Most notably orders to US government agencies commonly need to comply with NIST cybersecurity standards, guidelines and best practices created by the National Institute of Standards and Technology (NIST).

While compliance with NIST is not a regulatory requirement it still has a wide impact due to the number of suppliers and sub-suppliers to the US government.

INSURANCE REQUIREMENTS FOR CYBERSECURITY

Increasingly cybersecurity is becoming a prerequisite for obtaining insurance for assets. One example is within shipping where new boats require approval by a rating agency in order to be insured.

The International Association of Shipping Societies has created the standard “E27 Cyber Resilience of On-board Systems and Equipment”. This standard is largely based on IEC 62443 but excludes parts which are not relevant for boats.

While the cybersecurity requirements for boats apply to the owners it also indirectly applies to device manufacturers and machine makers delivering to the maritime sector.

2. Standards

IEC 62443 Industrial communication networks - Network and system security

The IEC 62443 series of standards address security for operational technology (OT) in automation and control systems and complements the ISO 27001 standards more focused on Information Security Management Systems (IT infrastructure).

It covers everything from top level policies and procedures all the way down to components with a strong focus on integrity and availability of industrial control systems.

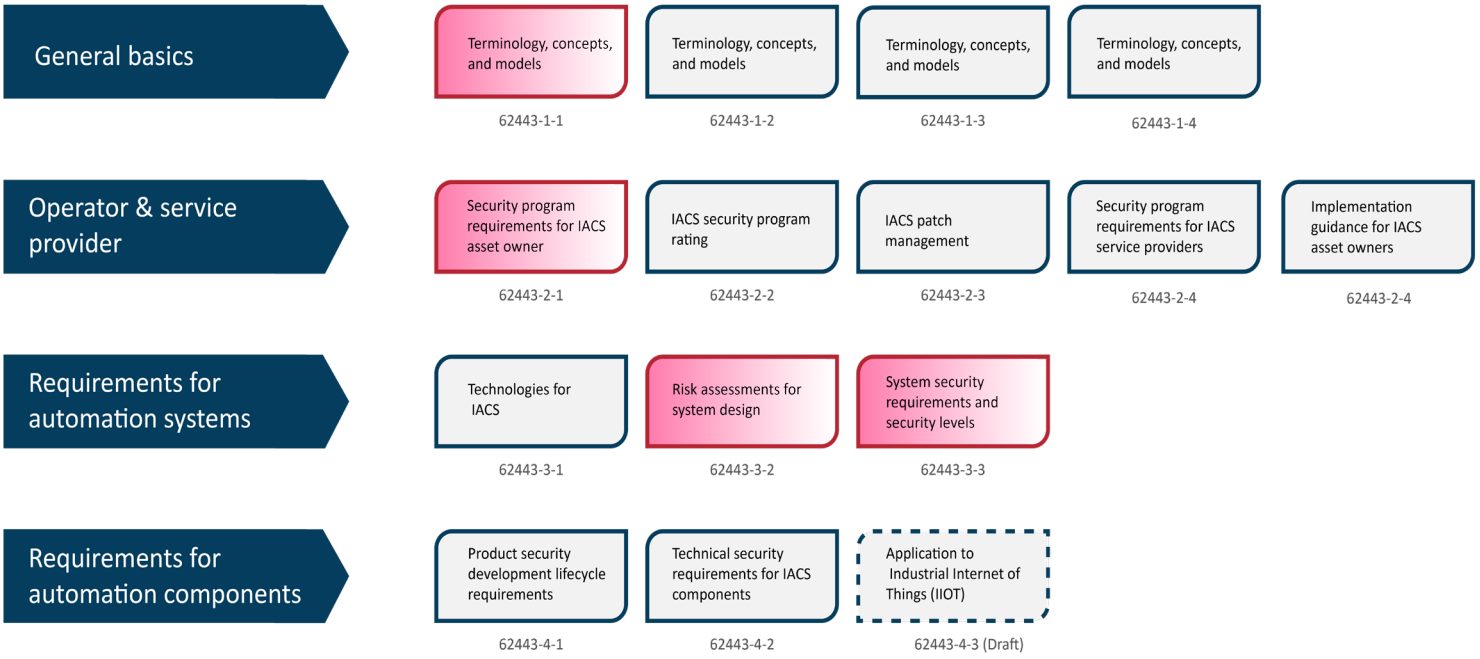

Figure 4. Structure of the IEC 62443 series of standards for industrial cybersecurity.

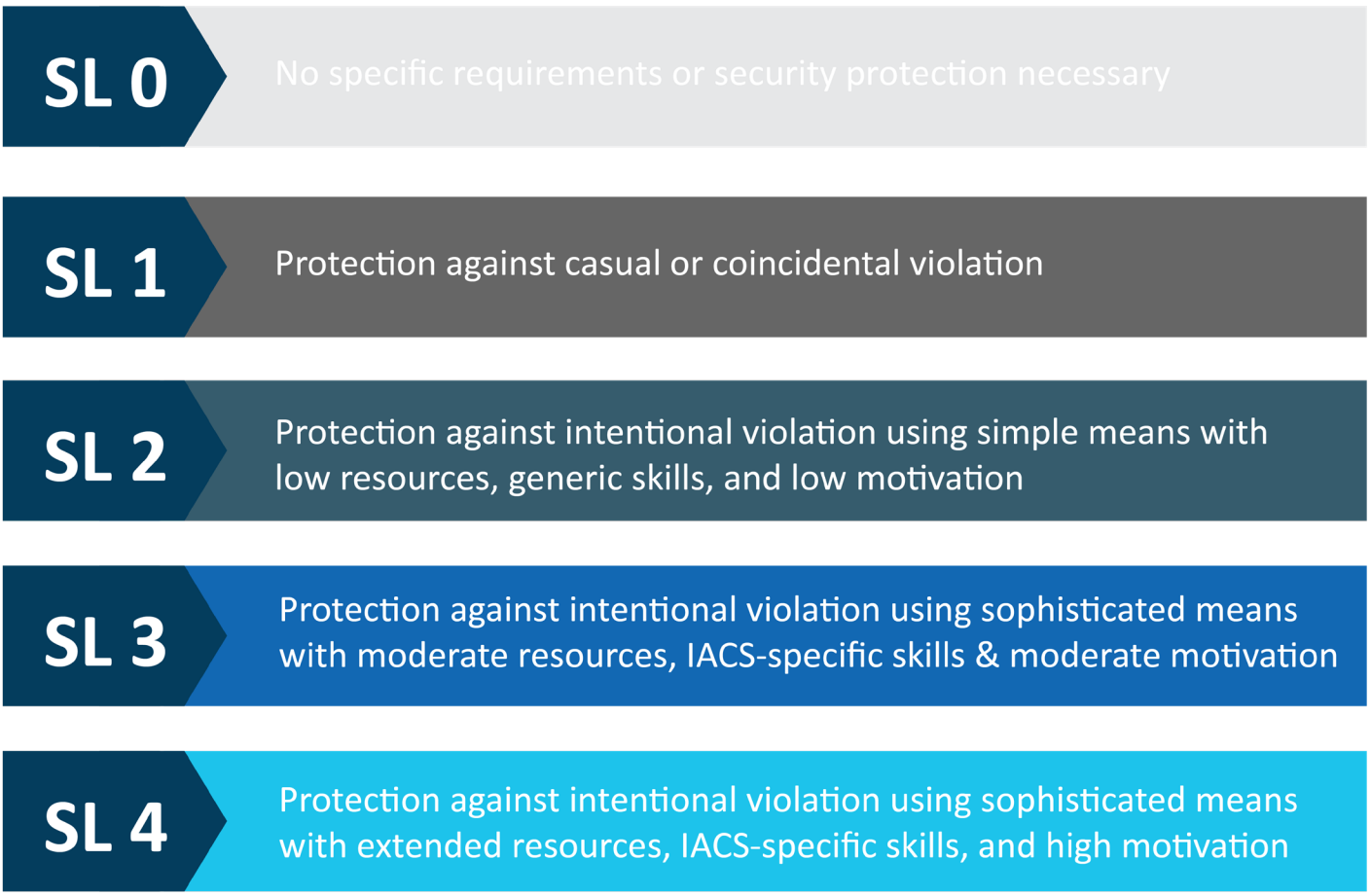

Figure 5. IEC 62443 security levels from SL 0 to SL 4.

The standard defines 5 security levels from security level zero to security level four. For security level zero no requirements are defined.

The standards enable facility owners to achieve an appropriate level of cyber security and also serves as documentation towards external entities:

- Demonstrate compliance with regulatory requirements such as NIS2.
- Demonstrate appropriate security levels towards insurance companies.
- Demonstrate appropriate level of cyber security towards customers and shareholders.

One of the guiding principles for facilities is the segmentation of their OT networks and the implementation of conduit to monitor and control the industrial communication inside critical machines and production lines limiting the exposure of automation devices.

To achieve the required security level of the facility the systems and components also need to meet cybersecurity requirements.

To meet these expectations the device manufactures can rely on the 62443-4-x standards to get a structured and in-depth guidance for requirements to address documentation and implementation of cybersecurity in automation components.

From CRA perspective IEC 62443 is important because work is underway to expand the standards so that they can be harmonized for CRA.

This work involves creating European extensions to IEC 62443-4-1 and IEC 62443-4-2 as well as creating a range of new IEC 62443-5-x so called “profile standards” as well as a range of new IEC 62443-6-x standards detailing evaluation methods.

EN 18031 COMMON SECURITY REQUIREMENTS FOR RADIO EQUIPMENT

The EN 18031 series of standards are the harmonized standards for the European radio Equipment Directive (RED). When radio equipment is tested against these standards conformity with the cybersecurity requirements of the directive can be presumed.

From CRA perspective these standards are important because the European Commission has requested that the standardization organizations create harmonized standards for CRA which are based on the RED cyber security standards. For this reason, EN 18031 is a good starting point when preparing for CRA compliance.

EN 18031 is also the first cybersecurity standard to be harmonized. One of the requirements for a standard to be harmonized is that it should provide legal certainty when testing against the standard.

In other words, passing testing against the standard should not be dependent on the person performing the testing. In this way EN 18031 is different from IEC 62443 which takes a more risk-based approach to testing.

NIST FIPS AND SPECIAL PUBLICATIONS

The National Institute of Standards and Technology (NIST) under the United States department of commerce has published a number of Federal Information Processing Standards (FIPS) as well as a number of so called “Special Publications” with regards to cyber security.

FIPS standardizes important aspects of cyber security. Some examples include:

- Advanced Encryption Standard (AES). Also known by its original name Rijndael it is used by virtually all web servers and most other aspects of encrypted communications.
- Secure Hash Algorithms (SHA). A family of cryptographic hash functions.
- Cryptographically strong random number generators. Most modern microcontrollers have a FIPS approved hardware based random number generator.

The special publications commonly contain guidelines with regards to cyber security. One example is NIST Special Publication 800-63B which has recommendations on passwords.

FIPS and the special publications are mandatory purchasing requirements for most US federal agencies but are also widely used outside US federal agencies. Both IEC 62443 and EN18031 refer to NIST publications with regards to best practice for cyber security.

UL 2900 STANDARD FOR SOFTWARE CYBER SECURITY FOR NETWORK CONNECTABLE PRODUCTS

UL 2900 is a family of standards for cyber security in network connectable products. Some of the UL standards have also been standardized by ANSI. ANSI/UL 2900-1 covers general product requirements and mostly contains requirements on secure development and testing.

Part 1 can be seen as a horizontal standard applicable to all products.

Part 2 is a set of vertical standards addressing specific product categories:

- ANSI/UL 2900-2-1 is requirements for network connectable healthcare products.
- UL 2900-2-2 is for industrial control systems (has so far not been adopted by ANSI)
- UL 2900-2-3 is for security and life safety signalling systems (also not adopted by ANSI)

The US food and drug administration has recognized ANSI/UL 2900-1 and ANSI/UL 2900-2-1 as a way to show compliance to government regulations.

ISO/IEC 27000 INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS)

The ISO/IEC 27000 family of standards address requirements for information security management systems. It addresses relevant aspects of information security and provides organizational controls, people control, physical controls as well as technological controls.

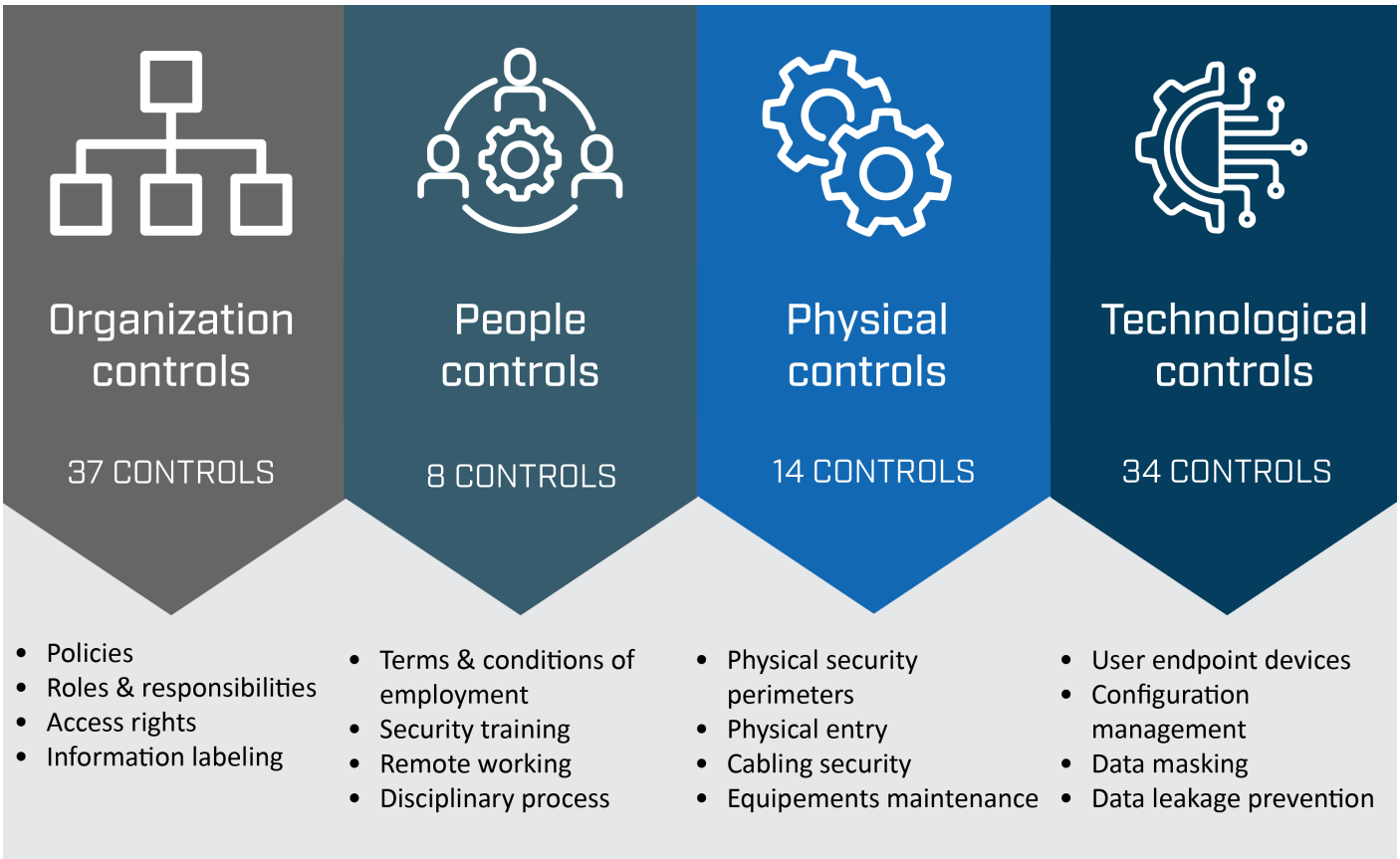

Figure 6. ISO/IEC 27000 control categories for information security management systems.

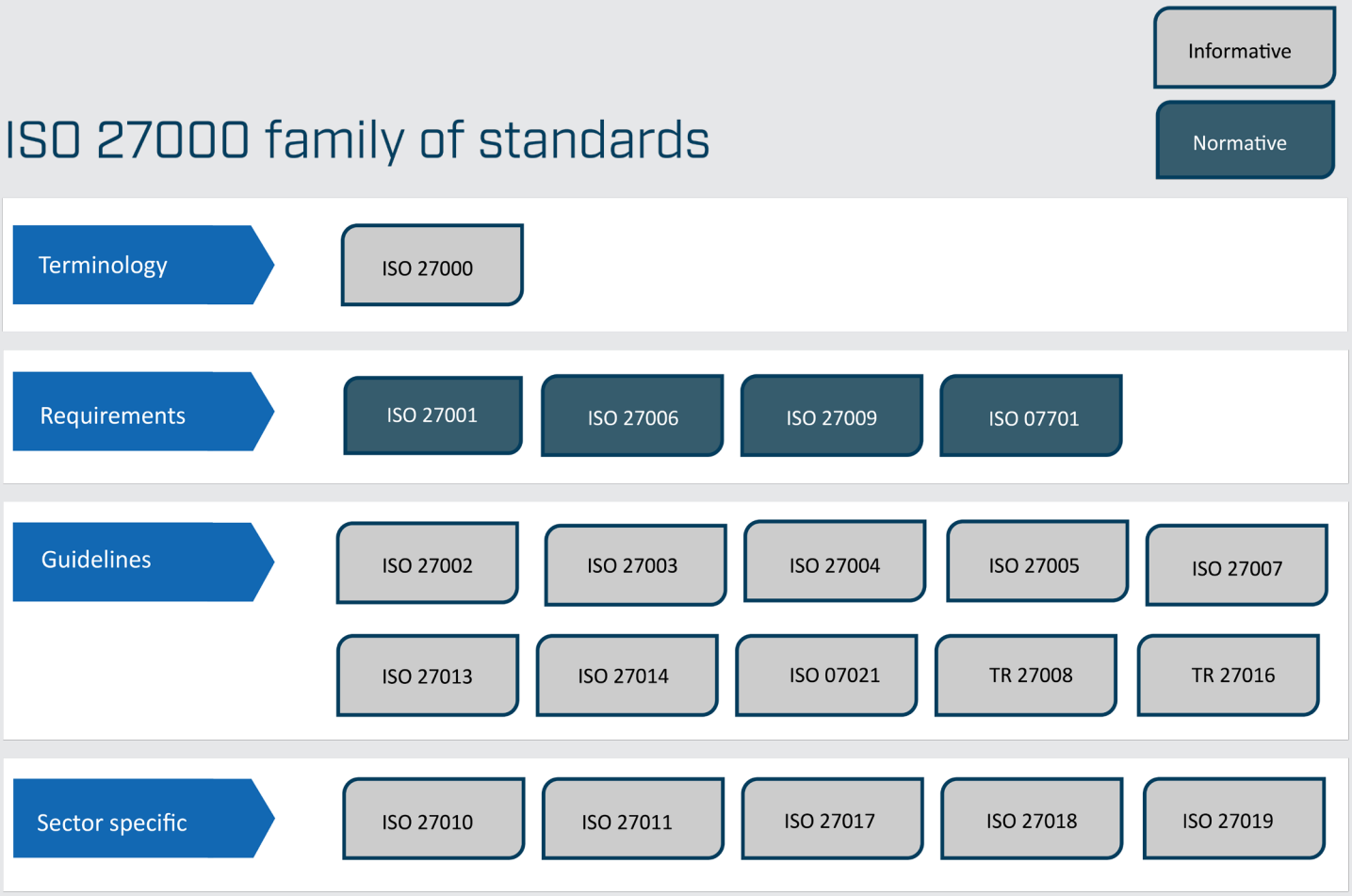

Figure 7. More than 20 standards are part of the ISO/IEC 27000 family of standards. They address different levels of abstraction as well as sector specific aspects.

3. Cyber security requirements for device manufacturers and machine builders

Device manufacturers and machine builders have two primary sources of cyber security requirements:

- Direct government regulation
- Purchasing requirements from customers

In addition, device manufacturers and machine builders have an own interest to ensure good cyber security to minimize financial losses and maintain good reputation.

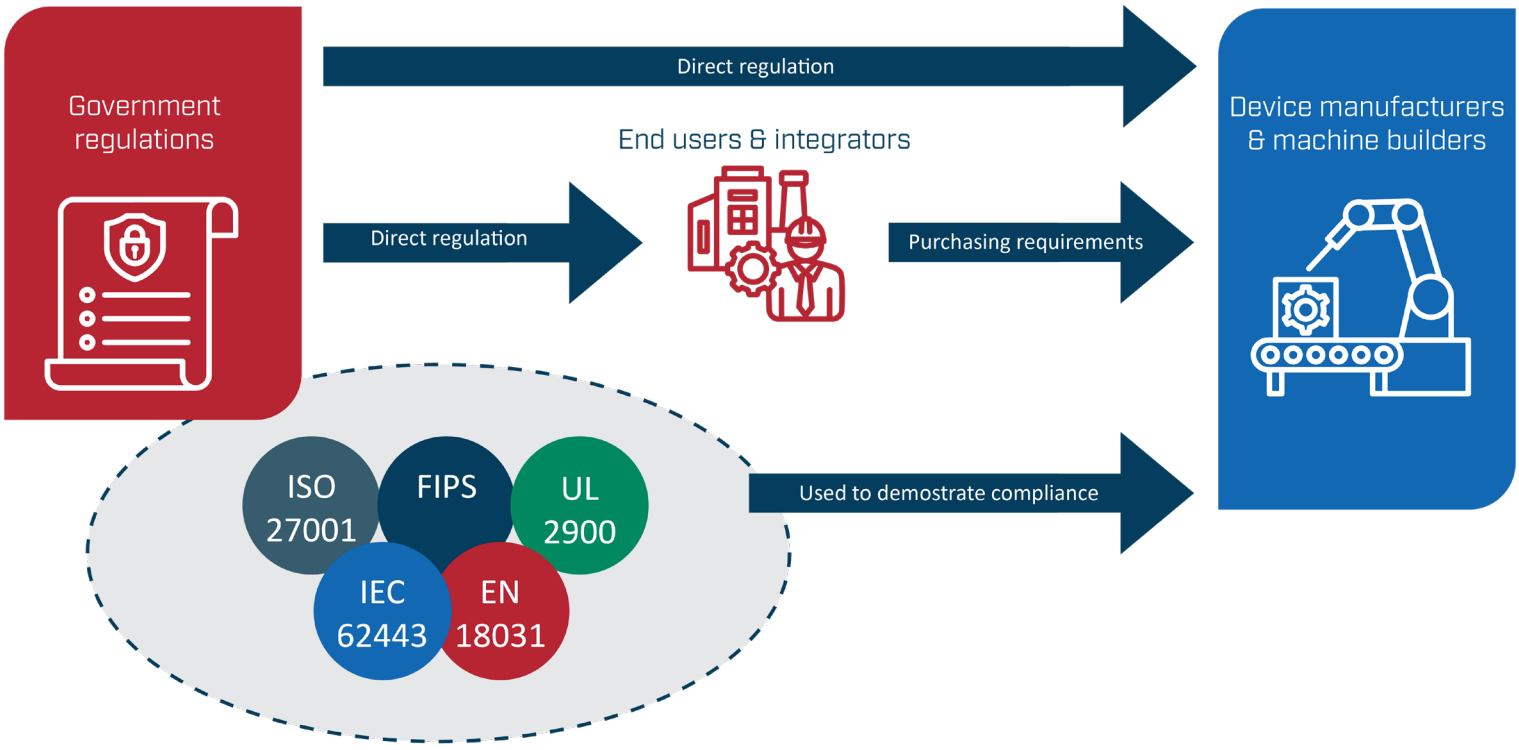

Figure 8. Sources of cybersecurity requirements for device manufacturers and machine builders.

To comply with both direct government regulation and purchasing requirements, device manufacturers and machine builders need to implement a minimum level of cyber security functionality in their products and document secure development practices.

To ease the burden of cyber security compliance device manufacturers and machine makers can use pre-certified network interfaces.

These interfaces already implement the majority of cyber security defenses necessary and have been pre-certified to relevant cyber security standards.

The EU cyber resilience act (CRA) has been approved at the end of 2024,

but so far, the necessary harmonized standards have not been created. This creates uncertainty for device manufacturers and machine builders which need time to ensure that all products comply with the new regulation.

With regards to purchasing requirements the uncertainty is even larger, because the end users and integrators so far do not have full clarity on the impact of NIS2 and similar regulation. In addition, the end users and integrators need to translate top level requirements to purchasing requirements.

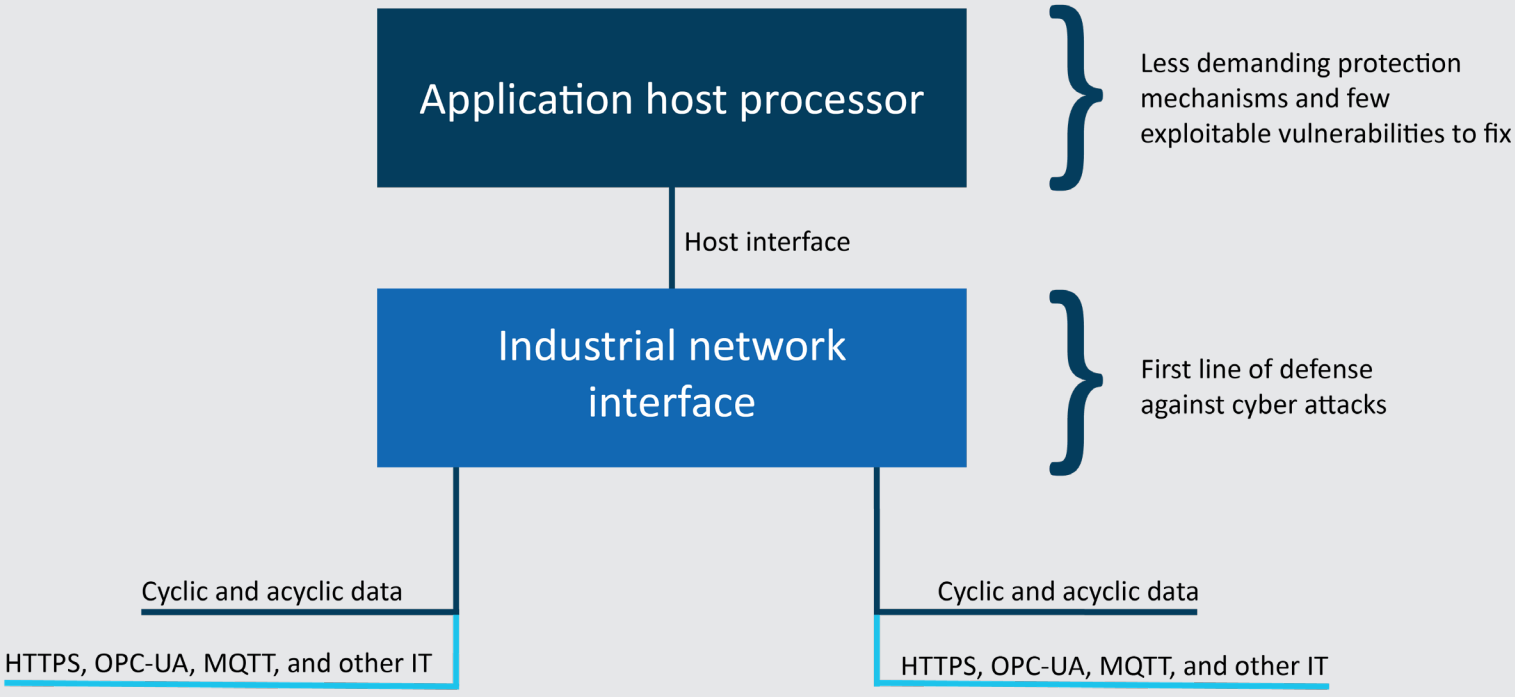

Figure 9. Pre-certified network interfaces can act as a first line of defense against cyberattacks.

One example of this is CRA which has an extensive list of requirements which must be fulfilled to legally sell products in the European market after December 2027.

As shown below many of the required CRA tasks can be fulfilled by using a pre-certified network interface.

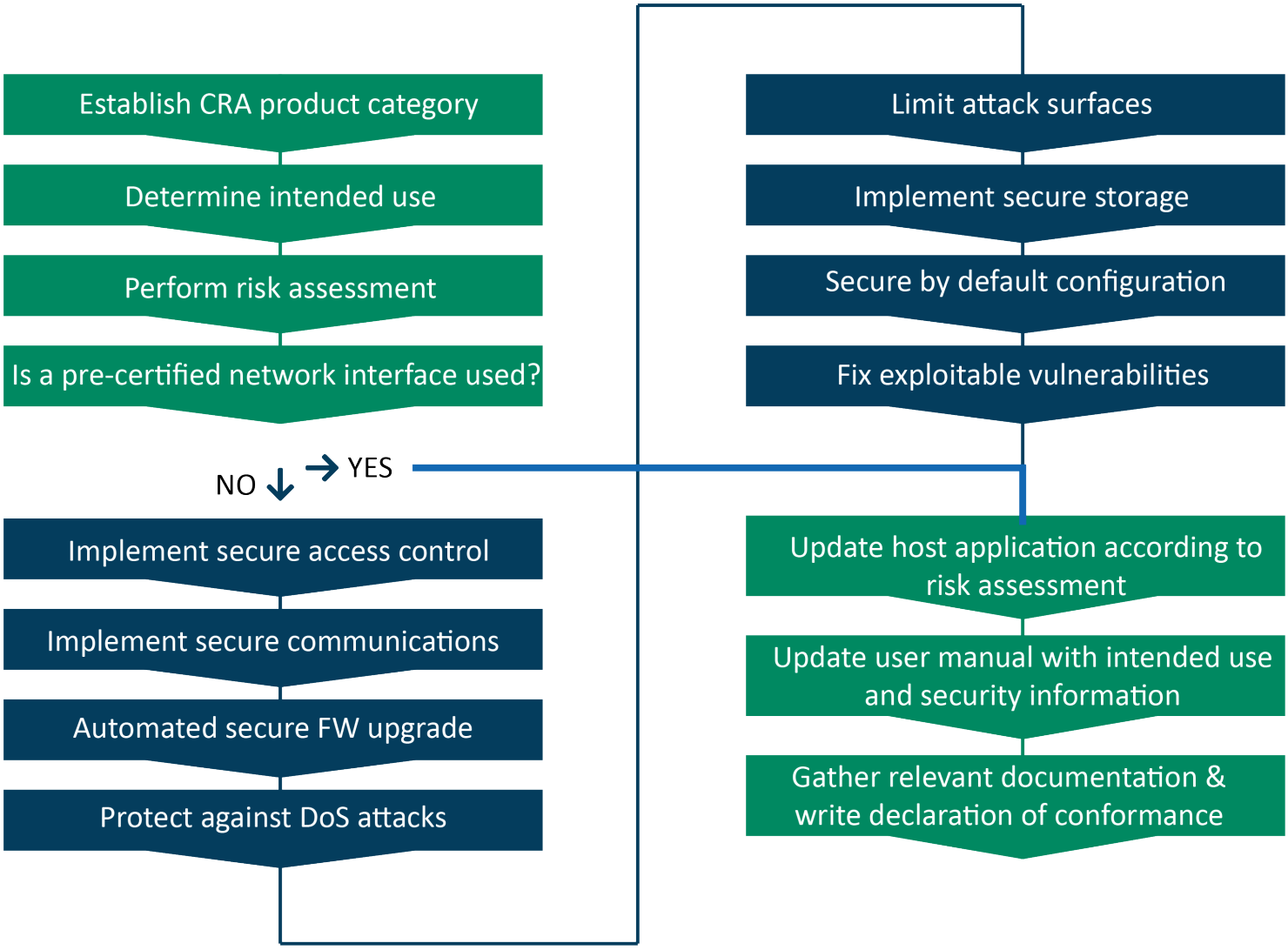

Figure 10. CRA compliance workflow and tasks, highlighting benefits of using pre-certified network interface.

PART 2: Cybersecurity at HMS Networks

HMS Networks is a market leader in the Industrial Information and Communication Technology (ICT) sector, with over 35 years of experience.

Globally, thousands of companies have integrated over 10 million HMS Network products, enabling their industrial machines and devices to communicate and share information effectively.

HMS Networks is dedicated to delivering and maintaining secure communication products that customers can rely on with confidence. As an experienced, stable, and financially secure company, HMS Networks can implement and manage the long-term challenges of cybersecurity.

The combination of industry leadership, extensive experience, technical expertise, and guaranteed product maintenance makes HMS Networks products a secure investment for any manufacturer looking to integrate HMS products with their own devices or machines.

Within HMS Networks, the responsibility for the industrial embedded communication interfaces is within the Industrial Network Technology (INT) division and made available under the Anybus Brand.

"Within INT we focus on real-time communications, industrial control and cyber security. We see this as the 3 pillars of industrial automation." - Bartek S. Candell, Senior Vice President Industrial Network Technology Division, HMS Networks.

For more information about the HMS Networks, visit:
www.hms-networks.com/about

4. HMS security standards & processes

INFORMATION SECURITY MANAGEMENT SYSTEM AND SECURITY-RELATED CERTIFICATIONS

HMS Networks implements an Information Security Management System (ISMS) to ensure the highest level of quality and security. As part of the ISMS process, HMS Networks adheres to the following certifications:

- ISO 9001: Development processes comply with the ISO 9001 standard, ensuring the highest quality and reliability.
- ISO27001: System to manage risks and to safeguard confidentiality, integrity, and availability of data & information handled.
- IEC62443-4-1 ML3: Anybus Product development process can meet the requirements for maturity level 3, providing enhanced security management throughout the development process and entire product lifecycle.

HMS Networks adheres to the regulations set forth by the General Data Protection Regulation (GDPR). The Anybus Embedded network interfaces operate without the need for, or transmission of, personal user information. For more information, visit: HMS Customer Privacy Policy www.hms-networks.com/privacy-policy

SECURITY MEASURES FOR ISMS IMPLEMENTATION

To ensure confidentiality and integrity throughout the Anybus Embedded Network interfaces life cycle, HMS Networks implements the security measures for Anybus Embedded network interfaces described in Table 1:

Requirement	HMS implementation
Data confidentiality	Full implementation of ISMS Controls in accordance with the security-related certificates listed in section 5.1.
Secure development and manufacturing environment	• Restricted physical and logical access is provided only to authorized personne • Doors are locked, and alarms are activated outside of working hours. • HMS Networks maintains a full audit trail that details all access and changes. • Visitors are accompanied by HMS employees. • Photography or similar recordings are prohibited.
Assurance of integrity over the complete supply chain	The software uses certificates for both firmware and PC-based configuration software and drivers. The hardware uses well-known industrial EMS suppliers, and HMS Networks audits all suppliers. Internal product integrity checks are conducted to ensure the product's integrity.

Table 1. Security measures.

SECURITY BY DESIGN

Security is an integral part of every step in the Anybus development process, including requirements gathering, design, coding, testing, deployment, and documentation.

Security trained employees

All employees receive cyber security awareness training. Developers also receive training in secure coding and conduct source code reviews.

Security product testing and validation

The security-by-design approach includes comprehensive testing with a focus on identifying potential vulnerabilities.

This involves running security-focused test cases that aim to uncover any unintended product functionality or configuration that could be exploited.

Table 2 shows how HMS Networks reviews and tests the code used in the Anybus CompactCom 40. HMS selects the tests and reviews that align with the product's requirements.

Following product release, HMS Networks conducts regular product interface testing to ensure resilience against emerging threats.

Type of Review or Test	Compliance
Code Review	All code is reviewed before check-in.
Penetration tests	Performed based on product requirements - parts of products tested
Static Code Analysis	Synopsis Coverity tool
Fuzz Testing / Robustness Testing	Netload for the PROFINET versions. Achilles for all other versions.
Vulnerability Scanner	Achilles

Table 2. Anybus CompactCom testing.

5. Product documentation and information

PRODUCT DOCUMENTATION, DESIGN GUIDES, DECLARATION OF CONFORMITY

Dedicated product and Network user manuals provide comprehensive descriptions of the product's features, capabilities, and guidance for implementing and configuring the product within automation devices.

This security Design Guide complements the existing product user manuals with product security content and guidance for the design and lifecycle management of the Anybus embedded network interfaces.

Additional product security datasheets cover detailed and product specific security information and instructions.

Declaration of conformity documents are issued for compliance to relevant network technology or regional standards such as EU and UK.

These documents are available under:

- the HMS Networks technical support webpage - select the product reference / Support & Download section: www.hms-networks.com/technical-support
- The HMS Developer Portal for Anybus CompactCom: www.hms-networks.com/embedded-network-interfaces/developer-portal/overview

LIFE CYCLE MANAGEMENT

HMS Networks has established processes to manage the product life cycle. Functional and security maintenance is made according to their maturity phase. Product specific details, if available, may be found on product dedicated Security Datasheet.

For more details: www.hms-networks.com/product-life-cycle

NEW FIRMWARE UPDATES

Please contact our tech support team to get the latest Firmware available for your product.

To get notified on new firmware releases register to the HMS Customer and Distributor Information System (CDIS). Select the "Subscribe to Alerts" button in the "Product and security alerts" section of our support page. www.hms-networks.com/technical-support

Several solutions are available to update the Anybus Embedded Networks interfaces and dedicated mechanisms are validating the validity of the Firmware during this process. For specific information refer to the "Best practice" section of this manual and to the product security datasheet.

USE OF OPEN SOURCE

HMS Networks may incorporate open-source software in the Anybus embedded network interfaces. This software is integrated into product firmware, with HMS Networks taking responsibility for the software's validation and ensuring that security vulnerabilities are addressed appropriately.

Details about the utilized open-source software and corresponding licensing information are in the relevant network guides, which are available on the HMS Networks technical support webpage at: www.hms-networks.com/technical-support

SBOM

HMS can provide a Software Bill of Materials (SBOM) for relevant firmware upon request.

VULNERABILITY MANAGEMENT AND COMMUNICATION

Information about security vulnerabilities is published on the following website, and users can subscribe to RSS feeds directly from the website to receive notifications about updated content. www.hms-networks.com/cyber-security

HMS Networks has an HMS Responsible Disclosure Program, enabling anyone to report a potential product vulnerability. For information, see www.hms-networks.com/cyber-security/responsible-disclosure-program

BACKDOOR FREEDOM DECLARATION

The Anybus Embedded network interfaces do not contain undocumented backdoors or hidden accounts to any external interfaces.

The Anybus Embedded network interfaces do not include remote access functionality nor establish specific external communication with cloud-based services.

6. Anybus embedded network interface connectivity overview

The Anybus embedded network interfaces are intended to be integrated by device manufacturers to enable them to share their data through industrial networks.

They provide several communication interfaces to cover the following functions:

- Industrial Ethernet networks for process data exchange with automation controllers
- Web-based functionality for optional configuration and diagnostic
- IIoT protocols for information exchange with IT applications
- APIs to support the integration within the host application

A detailed product specific description of these communication ports, interfaces and protocols is provided in the product security datasheet.

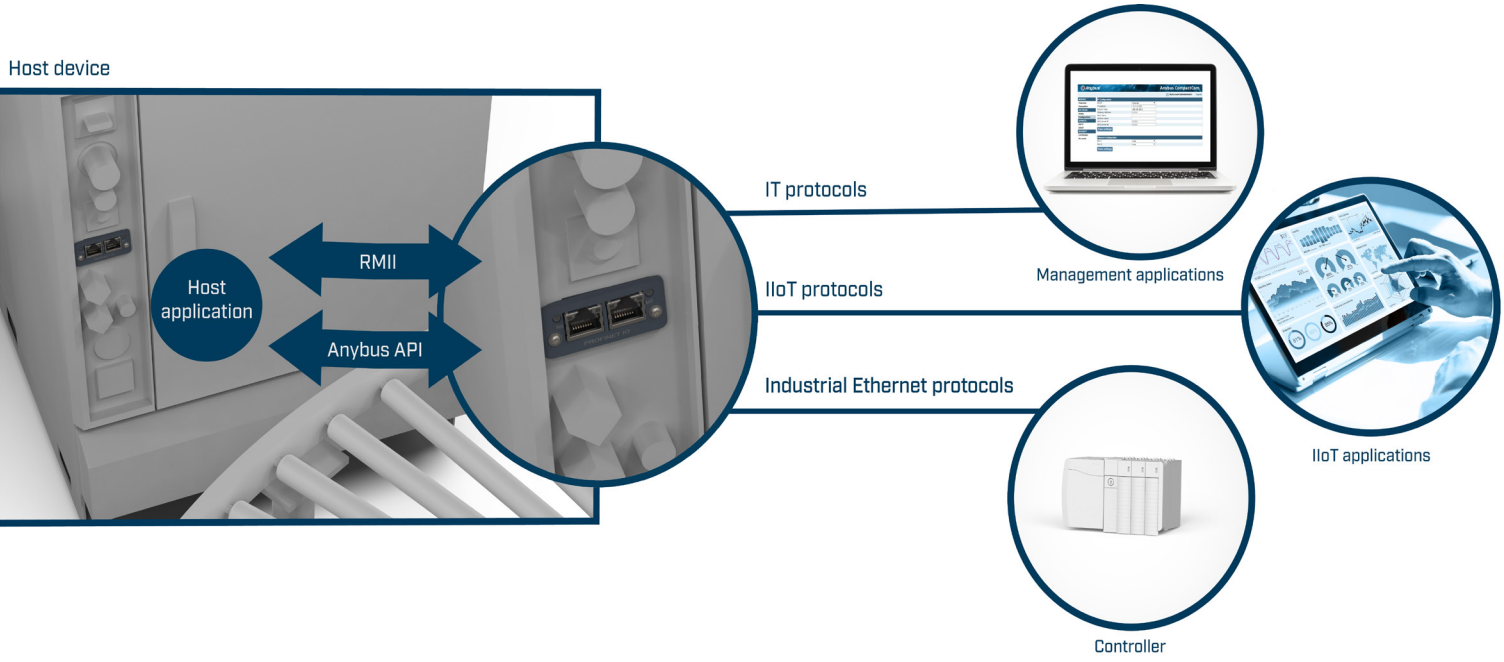

Figure 11. The Anybus CompactCom 40.

ANYBUS COMPACTCOM 40 AS STANDARD OR IIOT SECURE VARIANTS

The Anybus CompactCom 40 embedded network interfaces are available as standard variants and as IIoT Secure variants.

The Anybus CompactCom 40 standard variant focuses on industrial communication capabilities for serial or Ethernet based protocols and includes few IT focused management protocols.

The Anybus CompactCom 40 IIoT Secure variant focuses on a combination of Ethernet based protocols (PROFINET or EtherNet/IP), additional IIoT protocols (OPC UA, MQTT) and IT management communications. This version provides additional security functionality as well.

The related product security datasheets provide detailed information about each variant.

SECURITY CONSIDERATION FOR INDUSTRIAL ETHERNET PROTOCOLS AND THEIR SECURITY EXTENSIONS

In response to evolving cybersecurity requirements, industrial communication organizations are developing new protocol extensions that introduce advanced security mechanisms to safeguard both communication and applications.

Currently, these extensions concern the PROFINET, EtherNet/IP, Modbus TCP and BACnet protocols. Their implementation status ranges from early-stage applicability to ongoing discussions. For POWERLINK and EtherCAT there are currently no standards available supporting security extensions.

The Anybus CompactCom 40 IIoT Secure has been designed to meet best practice within cyber security.

Currently there is little market acceptance for secure Industrial Ethernet, but from hardware perspective the product is ready to support encrypted OT protocols. Also we have already tested secure OT protocols with other vendors:

- Interoperability testing has been performed for Modbus Security within the framework of modbus.org.
- CIP Security has been integrated with other vendors within ODVA and demonstrated at tradeshows worldwide.

SECURITY CONSIDERATION FOR SERIAL INDUSTRIAL NETWORKS

Serial-based networks are mainly logically isolated communication networks, meaning that highly dedicated effort is required for cyberattacks and so these networks have low vulnerability exposure.

Consequently, Anybus CompactCom products with serial-based industrial communication protocols are not addressed in this document.

PART 3: Best practices and secure integration

This section outlines best practices for device manufacturers integrating the Anybus embedded network interfaces, to strengthen the security of their devices or machines and be prepared for the coming security regulations.

This section focusses on our latest Anybus Compact Com 40 product family, the latest available interface family, in active product phase and guaranteed by HMS networks to address coming CRA requirements.

Note: This list of best practices is not exhaustive and does not guarantee compliance alone with any regulation. Each project and application should be considered individually to define the risk assessment and the appropriate measure to the desired security level.

Details about the functionalities described below and how to integrate them can be found in the respective product user manuals.

7 Intended use - The appropriate Anybus CompactCom

SECURELY INTEGRATED

The Anybus CompactCom should be integrated into an end product. The end product should ensure that the host interface or any internal parts are not accessible by unauthorized persons.

In case an unauthorized person gained access to the host interface it would be possible to eavesdrop on the communication and change the configuration.

The Anybus CompactCom IIoT Secure has support for secure communications. The confidential cryptographic keys are stored in a security chip and cannot be accessed even if physical access is gained to the hardware.

SECURE NETWORK

The Anybus CompactCom should be connected only to a trusted network. This restriction is needed due to the use of Industrial Ethernet protocols without security.

The Anybus CompactCom IIoT Secure has support for secure communications for protocols other than Industrial Ethernet.

These protocols can be used on untrusted networks, but still it must be ensured that the untrusted networks is not allowed access to the Industrial Ethernet communications. This can be achieved by means of a Firewall or data diode.

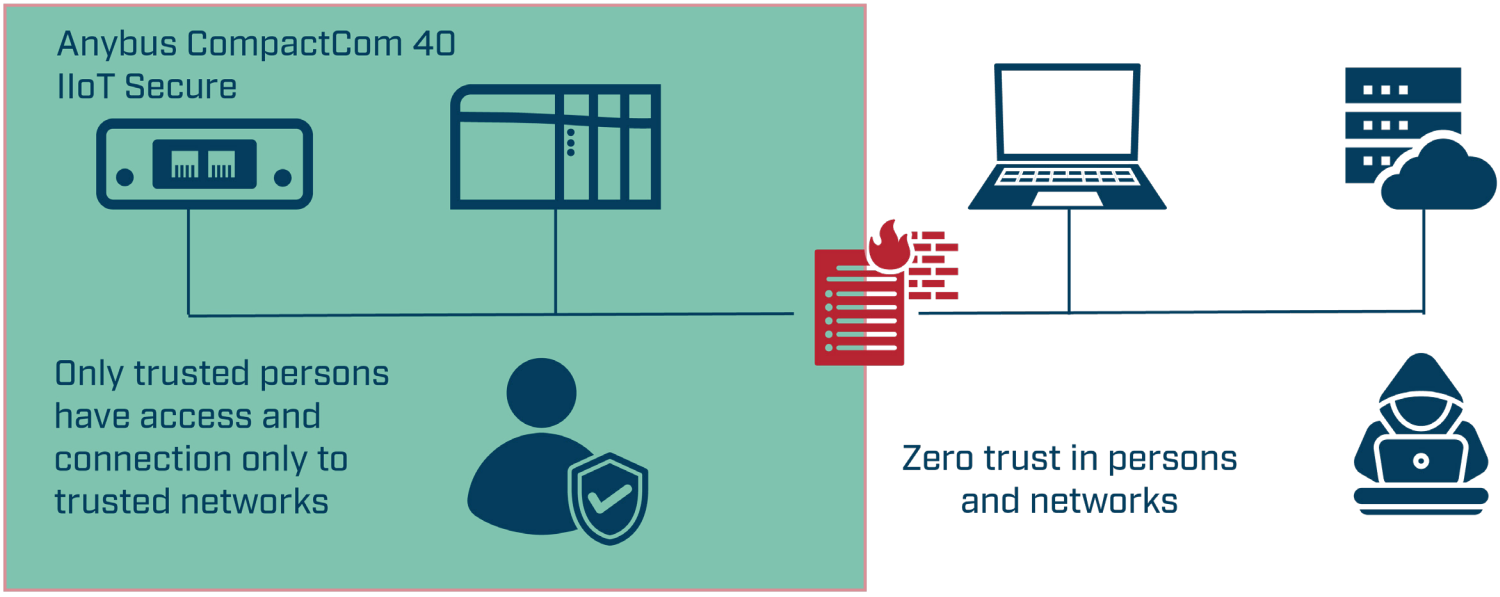

Figure 12. The Anybus CompactCom 40 IIoT Secure variant ensures only trusted persons can access trusted networks.

SELECTING THE RIGHT ANYBUS COMPACTCOM

The Anybus CompactCom 40 Industrial Ethernet as standard variant is suitable for industrial applications within trusted environment and trusted networks (See CRA section).

This standard variant is available for all industrial protocols (Serial based or Ethernet based).

The Anybus CompactCom 40 IIoT Secure variant is the optimal choice for applications requiring both Industrial Ethernet communication and IIoT or web server connectivity. This option provides additional security functionality,

reduces the need for additional external security measures from customers and enables secure communication outside trusted network.

The Anybus CompactCom 40 IIoT Secure is also a future proof solution that will be able to address the long-term security requirements and encrypted OT communication extensions. This evolution would mainly be made available through firmware updates.

Existing applications using the standard Anybus CompactCom 40 can be updated to the IIoT Secure variant with minimal effort due to the common Anybus Host API.

SECURE BY DEFAULT - THE COMMUNICATION INTERFACE

Manufacturers must close or disable all logical or physical interfaces on the Anybus CompactCom that are not required for the device's application.

- Deactivate any unused physical communication port, such as a second Ethernet port. Alternatively, provide the end user with the capability to activate or deactivate unused Ethernet ports.
- Disable any communication capabilities, such as a web server, FTP, SNMP... that are not needed for the device's intended operation.
- Activate (as far as possible) the encryption capabilities for protocols (like MQTT or OPC UA)

CONFIGURE, BACKUP AND RECOVERY

This chapter outlines the recommended approaches to configuring Anybus CompactCom 40 interfaces and ensuring reliable backup and recovery of device settings. The goal is to simplify device configuration, improve security, and maintain predictable behavior throughout the device lifecycle.

General recommendations

When configuring Anybus CompactCom 40 interfaces:

- Limit configuration points: Use a single interface or as few interfaces as possible to define the device's behavior and configuration.
- Secure configuration channels: Prefer secure communication interfaces. When available, define access permissions and assign user roles with configuration privileges (e.g., via the integrated web server for IIoT Secure variants).
- Plan for backup and recovery: Whenever possible, use configuration methods that support backup and restoration of settings. If such functionality is not inherent, implement it within the device application.

Specify fixed functionalities and behaviors in the host application

For device applications with static behaviors or fixed communication features, prioritize implementing these directly in the host application firmware.

- This ensures consistent and predictable device behavior without requiring separate backup or restoration steps.
- Firmware-defined behaviors can be updated as part of standard firmware updates, preserving intended operation across device versions.

Key benefit: Simplifies maintenance and eliminates the need for external configuration management for fixed functionalities.

Utilize network description files for user device configuration

If your device supports user-defined options, such as variable data mapping or optional behaviors, leverage industrial protocol initialization mechanisms like GSD, EDS, or similar network description files. These files:

- Allow users to define configuration parameters within the PLC environment.

- Transmit parameters automatically to the device during each initialization.
- Store the configuration inside the controller project file, ensuring persistence and consistency.

Key benefit: Enables flexible, user-specific configuration without needing manual intervention on the device itself.

Device configuration via a proprietary software tool

If the device requires configuration through a dedicated software tool:

- The host application should receive the configuration data or file from the tool.
- It should then store and apply the configuration through the Anybus CompactCom 40 host API.

In this setup, the following must be addressed within the proprietary tool and host application:

- Backup and restore capabilities for configuration data.
- Authentication and access control for sensitive configuration parameters.

Key benefit: Centralizes management of configuration data (host application and communication interface) while ensuring security and recoverability.

Anybus web server for configuration

The integrated web server in Anybus CompactCom 40 can be used to configure network settings and host custom web pages for device-specific configuration. Important notes:

- The built-in web server does not support back-up or restore of configuration parameters.
- Manufacturers must implement access protection and user authentication to safeguard the configuration interface.
- For IIoT and Secure variants, the web server supports:
  - Encrypted communication
  - User and role-based access control

However, backup and restore functionality remains unavailable even in these variants.
Key benefit: Provides an accessible interface for configuration, deal for devices requiring remote setup, but requires users to take care about backup strategies.

ACCESS PROTECTION AND USER MANAGEMENT

When using IT management features such as FTP or a web server, establish a user structure tailored to the specific application requirements.

This structure should define various user roles, each with distinct levels of access permissions. Activate, user and password identification for the interfaces. Use complex password to prevent unauthorized access to the interface.

IDENTIFICATION AND VERSIONING

Use the Anybus Identification objects from our API for device's version, status, and diagnostic information. Anybus CompactCom 40 uses the dedicated identification elements or mechanisms from the respective protocol specifications to share in a standardized way this asset management information with application controllers or network management tools.

The relevant information elements or mechanisms are listed in the Anybus CompactCom network guides.

PROVIDE DOCUMENTATION

Provide comprehensive device documentation and security description that outlines the global device interface capabilities based on the implementation of the Anybus CompactCom 40 functionalities.
Use the provided Anybus CompactCom 40 security datasheet to create the device security description.

To maintain effective version management of the entire system, integrate versioning related to the Anybus CompactCom 40. This should include the specific components of the host application and firmware, which can be reflected in the Anybus CompactCom interface.

Manufacturers can (or should) include the HMS statements for open-source software or hardware used in the Anybus CompactCom 40 and complement it according to the implementation in their own documentation. The HMS open-source statements are available in the relevant network guide.

ENSURE NETWORK COMMUNICATION COMPLIANCE

Ensure the entire device implementation passes the relevant industrial network's performance and conformance test to obtain a network certificate. HMS is ensuring that each new Hardware or Firmware release is compliant and pre-certified for the corresponding protocol technologies, simplifying so the compliance of the device integrating the interface.

Maintain this network conformance up to date through the complete device lifecycle according to the different network organization policies.

KEEP YOUR DEVICES UP TO DATE

Keep the Anybus CompactCom module up to date to maintain a consistently high level of security.

Stay informed about Anybus CompactCom product news, firmware updates and security advisories and register to our proactive communication channels (see corresponding chapter).

Manufacturers are responsible for evaluating the relevance and impact of the product change notifications and security advisories published by HMS in relation to their device's application.

Do not forget to update the versioning information for accurate traceability of devices installed in the field.

DECOMMISSIONING

When decommissioning the Anybus CompactCom, performing a factory reset will eliminate user accounts, and specific module configuration information, stored on the Anybus CompactCom.

Work with HMS.
The number one choice for Industrial ICT - Information and Communication Technology.

www.hms-networks.com