Nidec Drives

Knowledge Base Document

Cybersecurity and Nidec Control Techniques Drives, Intelligent Option Modules, and Controllers

Summary of Contents

The following document covers Control Techniques multi-layer approach to cybersecurity in an Industrial automation and control system (IACS) with Control Techniques Drives, Intelligent option modules, HMI, Keypad and Controllers following the IEC 62443 Industrial security series of standards.

Contents

Industrial Automation, Cybersecurity

Industrial automation and control system (IACS) organizations increasingly use commercial off-the-shelf (COTS) networked devices that are inexpensive, efficient, and highly automated. Control systems are also increasingly interconnected with non-IACS networks for valid business reasons. These devices, open networking technologies and increased connectivity provide an increased opportunity for cyber-attack against control system hardware and software.

Organizations may use business information technology (IT) cybersecurity solutions to address industrial automation and control system (IACS) security. While many business IT applications and security solutions can be applied, they need to be applied in an appropriate way to eliminate inadvertent consequences. For this reason, the approach used to define system requirements needs to be based on a combination of functional requirements and risk assessment, often including an awareness of operational issues as well.

The fundamental principle of cybersecurity is a strong cybersecurity process lifecycle. This lifecycle needs to include adequate training, tools, resources, and processes to develop, harden and maintain the resiliency of the equipment under control (EUC) against cyber-attacks. The lifecycle approach is also a fundamental premise of best practices utilized for various cybersecurity standards and approaches.

Cybersecurity of industrial control systems can often include three threat categories:

Industrial control systems threat categories	
Hacking	An attacker targeting an industrial control system this could be by creating dedicated malware.
General malicious software	An employee connects a laptop to the system network or inserts a USB stick into a server. The purpose of these actions could be benign, but there is a significant risk of infected devices transferring an infection to the automation system. Even though not designed to damage systems, it can be very harmful.
Employee mistakes	An engineer wants to update the control logic in an embedded device, but by mistake connects the engineering tool to the wrong device. Similarly, an engineer connects a network cable to the wrong port of a network switch.

Table.1 Industrial control systems common threat categories

There are various Directives, Requirements and Technical Rules which cover cybersecurity, and which use IEC 62443 Industrial communication networks - Network and system security, examples are briefly covered in this document along with IEC 62443 Industrial communication networks - Network and system security series of standards.

Note: When designing a control system to meet the set of control system requirements associated with specific target security levels, it is not necessary that every component of the proposed control system support every system requirement to the level mandated in IEC 62443 Industrial communication networks - Network and system security series of standards.

Control Techniques Drives and Intelligent Option Modules

Drive, Option modules	Detail, Recommendation
Digitax HD M75x Commander C200 & 300 Commander S Unidrive HSxx Unidrive Mxxx E300 Elevator Drive Unidrive Fxxx Unidrive Hxxx NE 200 / 300	Drives with an HMI, Keypad or communications port could provide direct access to parameters within the drives menus or initiate various actions on the drive. ▪ To prevent unauthorised access the User Security Code should be used along with controlled access to the Industrial automation and control system (IACS). Drives without an HMI, Keypad could provide access to parameters within the drives menus or initiate various actions via the drive's communications port[1]. ▪ To prevent unauthorised access via the drives communications ports a firewall or gateway device should be used along with controlled access to the Industrial automation and control system (IACS). Intelligent option modules fitted to a drive could provide access to parameters within the drive's menus via their communications port. ▪ To prevent unauthorised access via the communications port a firewall or gateway device should be used along with controlled access to the Industrial automation and control system (IACS). A Smartcard or NV Media card fitted into the drive will allow drive parameters and or onboard user programs to be uploaded or downloaded. ▪ To prevent unauthorised access the drives User Security Code should be used along with controlled access to the Industrial automation and control system (IACS). Drives with either Bluetooth or Near Field Communication (NFC) could provide direct access to parameters within the drives menus or initiate various actions on the drive. ▪ To prevent unauthorised access the User Security Code should be used along with controlled access to the Industrial automation and control system (IACS).
Ethernet fieldbus communications EIA 485 communications (Modbus RTU) MCi210 FFMCi SI-Applications Plus SI-Applications Compact SI-Safety MiS210, MiS250 SI-Ethernet SI-PROFINET SI-EtherCAT SI-CANopen SI-PROFIBUS SI-DeviceNet SI-DCP: DCP3 & DCP4 interface module SI-Interbus SI-Powerlink SI-BACnet MCz, MCe	
CI-Keypad KI-Keypad KI-Keypad (RTC) Remote Keypad (LCD), Remote Keypad (RTC) KI-HOA Keypad (RTC) Remote HOA Keypad (RTC) Exor HMI	
Smartcard NV Media card	
Bluetooth NFC (Commander S drives only)	

Table.2 Control Techniques Drives, Intelligent option modules security

[1] Drive communications ports could include Ethernet fieldbus communications or EIA 485 serial communications interfaces.

There is no “single solution” to managing a security risk in an industrial automation and control system (IACS), hence no completely secure system. Control Techniques recommend a multi-layer approach for security following the IEC 62443 Industrial communication networks - Network and system security series of standards which include:

a) Understand the general scope of the application to address the industrial automation and control system (IACS) security.
b) Understand how components of the industrial automation and control system (IACS) can be grouped or classified to define and manage the security.
c) Define the different cybersecurity objectives for control in the industrial automation and control system (IACS).

A multi-layer approach is where multiple layers of security controls are placed throughout an industrial automation and control system (IACS). Its intent is to provide redundancy in the event a security control fails, or the exploiting of a vulnerability. The multi-layer approach should prevent security breaches and allow detection of an attack. The control system LAN (local area network) or WLAN (wireless local area network) should be separated from other corporate networks with firewalls for security, and authentication.

The IEC 62443 Industrial Security Standards series address the range of coverage which may be defined and understood from several perspectives, including the following:

a) Range of functionality.
b) Specific system and interfaces.
c) Criteria for selecting included activities.
d) Criteria for selecting included assets.

Although fieldbus technologies have been evolving with regards to variable speed drives, intelligent option modules, and controllers support for authentication or any other basic cybersecurity is very limited. Therefore, variable speed drives, intelligent option modules and controllers do not offer means to secure network traffic making them vulnerable to malicious system access, data reading and manipulation by hostile parties. Control Techniques recommend that where applicable gateways, firewalls and countermeasures are used;

a) Firewalls should be used when connecting to variable speed drives and associated intelligent option modules and MCz, MCe controllers via LAN (local area network) or WLAN (wireless local area network).
b) Countermeasures such as passwords should be used to prevent direct access to variable speed drives and associated intelligent option modules via the HMI, Keypad.
c) Where communications do not extend beyond the industrial automation and control system (IACS), we recommend restricted access to authorised personnel.

The following diagram shows an example system with Control Techniques drives, intelligent option modules, and controllers with a trusted zone and potential untrusted networks. From the cybersecurity approach there are a number of cybersecurity related risks. Remote connections have been implemented typically for programming, system management and servicing. The cybersecurity target is to secure the system and connections using gateways, firewalls, user security codes and controlling access to the system and any additional local networks and operator systems.

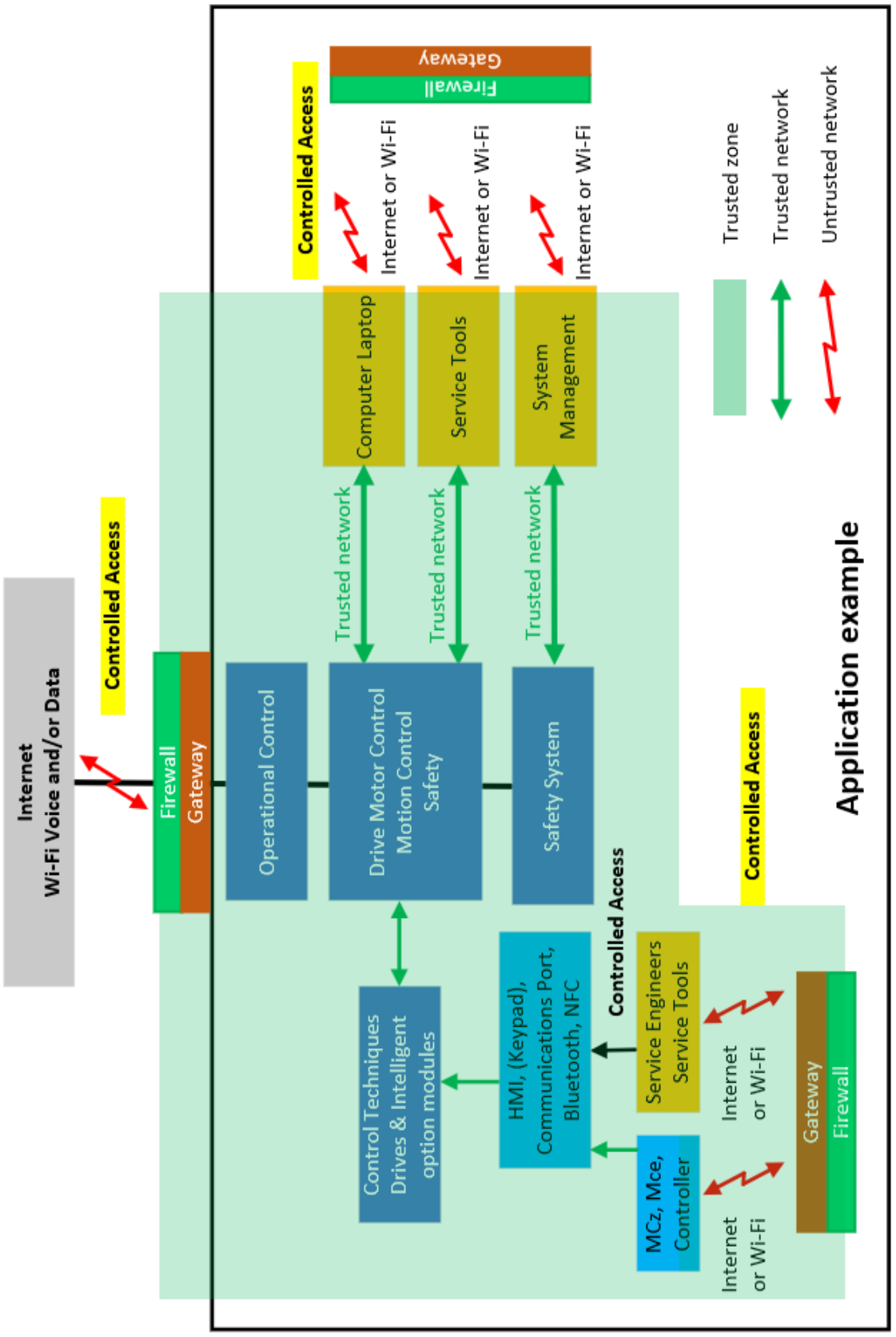

Fig.1 Application example trusted zone, trusted, untrusted networks

IEC 62443 Industrial Security Standards

The industrial automation and control system (IACS) community audience for this standard is intended to be asset owners, system integrators, product suppliers, service providers and, where appropriate, compliance authorities.

System integrators, product suppliers and service providers can use this standard to evaluate whether their products and services can provide the functional security capability to meet the asset owner's target security level requirements.

As with the assignment of target security levels the applicability of individual control system requirements and enhancement requirements need to be based on an Asset owner's security policies, procedures, and risk assessment in the context of their specific site. When designing a control system to meet the set of control system requirements associated with specific target security levels, it is not necessary that every component of the proposed control system support every system requirement to the level mandated in IEC 62443 Industrial communication networks - Network and system security.

Note some control system requirements contain specific conditions for permissible exceptions, such as where meeting the control system requirements will violate fundamental operation of a control system, which may then trigger the need for countermeasures. Compensating countermeasures can be employed to provide the required functionality to other subsystems, such that the overall target security level requirements are met at the control system level.

The IEC 62443 series of standards is based in part on principles found in a number of different national cybersecurity standards and provides a clear yet flexible framework that is equally applicable in discrete and process-oriented manufacturing environments in a diverse range of industries.

IEC 62443 takes a risk-based approach to cybersecurity, which is based on the concept that it is neither efficient nor sustainable to try to protect all assets in equal measure. Instead, users must identify what is most valuable and requires the greatest protection and identify vulnerabilities. They must then erect defence-in-depth architecture that ensures business continuity. The IEC 62443 series of standards were developed to secure Industrial Automation and Control Systems (IACS) throughout their lifecycle and currently includes 9 standards, technical reports, and technical specifications.

IEC 62443 Industrial Security Standards Series	
IEC 62443 Part 1: General Covers topics that are common to the entire series.	1-1: Terminology, concepts, and models. A technical security specification for industrial automation and control systems (IACS). Addresses a range of applications (i.e. industry types).
IEC 62443 Part 2: Policies and procedures Focuses on methods and processes associated with IACS security.	2-1: Establishing an industrial automation and control systems (IACS) security program. A list of all existing parts of the IEC 62443 series, published under the general title Industrial communication networks – Network and system security, can be found on the IEC website.
	2-3: Patch management in the industrial automation and control systems (IACS) environment. A Technical Report, describing requirements for asset owners and industrial automation and control system (IACS) product suppliers that have established and are now maintaining an IACS patch management program.
	2-4: Security program requirements for industrial automation and control systems (IACS) service providers. Specifies requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution.
IEC 62443 Part 3: System Covers requirements at the system level.	3-1: Security technologies for industrial automation and control systems (IACS).
	3-2: Security risk assessment for system design.
	3-3: System security requirements and security levels. Addresses the issue of security for industrial automation and control systems (IACS).
IEC 62443 Part 4: Components and requirements Provides detailed requirements for industrial automation and control systems (IACS) products.	4-1: Secure product development lifecycle requirements. Specifies the process requirements for the secure development of products used in industrial automation and control systems (IACS).
	4-2: Technical security requirements for industrial automation and control systems (IACS) components. Provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs). a) identification and authentication control (IACS) b) use control (UC) c) system integrity (SI) d) data confidentiality (DC) e) restricted data flow (RDF) f) timely response to events (TRE) g) resource availability (RA)

Table.3 IEC 62443 Industrial Security Standards Series

The following details how the developed product relates to maintenance and integration capabilities defined in IEC 62443-2-4 and to its operation by the asset owner. The product supplier develops products using a process compliant with the IEC 62443 series of standards.

Those products may be a single component, such as an embedded controller, or a group of components working together as a system or subsystem. The products are then integrated together, usually by a system integrator, into an Automation Solution using a process compliant with the IEC 62443 series of standards.

The Automation Solution is then installed at a particular site and becomes part of the industrial automation and control system (IACS). Some of these capabilities reference security measures defined in IEC 62443-3-3 that the service provider ensures are supported in the Automation Solution (either as product features or compensating mechanisms).

Below the Automation Solution is illustrated to contain one or more subsystems and optional supporting components such as advanced control. The dashed boxes indicate that these components are “optional”.

Note: Automation Solutions typically have a single product, but they are not restricted to this. In general, the Automation Solution is the set of hardware and software, independent of product packaging, that is used to control a physical process (for example, continuous or manufacturing) as defined by the asset owner. In some industries, there may be a hierarchical product structure.

Note: If a service provider provides products used in the Automation Solution, then the service provider is fulfilling the role of product supplier in this diagram.

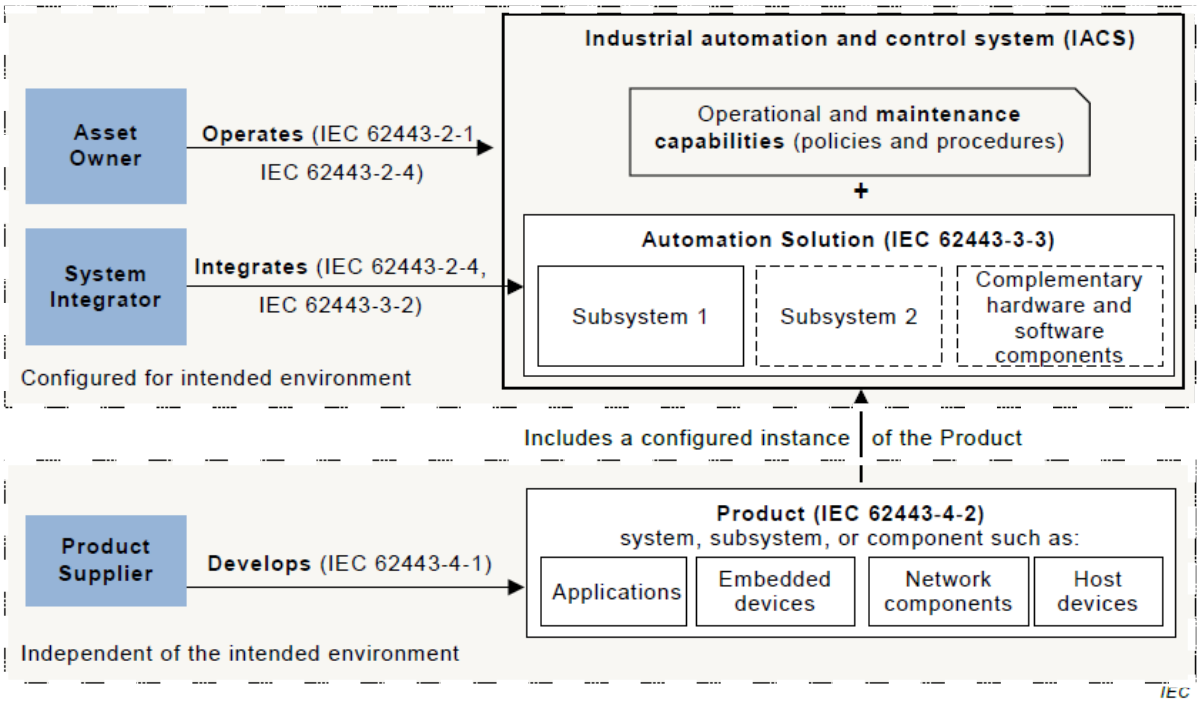

Fig.2 Example scope of product life cycle

Directive (EU) 2022/2555 - NIS 2 Directive Legislative Act Aiming to Achieve a High Common Level of Cybersecurity Across the EU

The NIS 2 Directive (Directive (EU) 2022/2555) is a legislative act that aims to achieve a high common level of cybersecurity across the European Union.

IEC 62443 Industrial communication networks - Network and system security series of standards is used to evaluate whether products and services can provide the functional security capability to meet the asset owner's target security level requirements and the NIS 2 Directive ((EU) 2022/2555).

As with the assignment of target security levels the applicability of individual control system requirements and enhancement requirements need to be based on the asset owner's security policies, procedures, and risk assessment in the context of their specific site.

Technical Regulation for Operational Safety TRBS - Part 1 Cybersecurity for Safety-relevant Measurement, Control, and Control Devices

This technical rule specifies the Industrial Safety Ordinance with regards to the identification and definition of necessary cybersecurity measures to ensure the functionality of safety-relevant measuring, control, and regulation devices (MSR devices), which are used as technical protective measures for safe use of work equipment including a system that requires monitoring.

The procedure for defining, implementing, and testing cybersecurity measures presented in TRBS is also suitable for protecting parts of the work equipment (e.g. necessary means of communication) or other technical infrastructure against cyber-threats that go beyond security relevant MSR facilities is considered necessary because of the risk assessment.

IEC 62443 Industrial communication networks - Network and system security series of standards is used to evaluate whether products and services can provide the functional security capability to meet the asset owner's target security level requirements and TRBS 1115 Part 1 Cybersecurity for Safety-relevant Measurement, Control, and Control Devices.

ISO 8102-20:2022 Electrical Requirements for Lifts, Escalators and Moving Walks - Part 20: Cybersecurity

ISO 8102-20:2022 Electrical Requirements for Lifts, Escalators and Moving Walks - Part 20: Cybersecurity has been developed in response to market requirements and enhanced cybersecurity awareness. The cybersecurity standards for operational technology is IEC 62443 Industrial communication networks - Network and system security series of standards.

ISO 8102-20:2022 addresses the industry-specific requirements that are necessary when applying the IEC 62443 Industrial communication networks - Network and system security series of standards.

Note: In ISO 8102-20:2022, lift, escalator and moving walk control systems are considered to be computer systems.

Domain	Description	Non-comprehensive list of functions under the domains as examples
Safety	SIL-rated control functions.	- Electric safety devices. - Electrical protective devices. - Motor and brake control functions.
Essential	Function or capability that is required to ensure the availability of the lift, escalator or moving walk, and its compliance to safety regulations, and which do not belong to Safety or Alarm function domains.	**Lifts:** - Normal control. - Car and landing call devices. - Access control. - Energy saving (car light, ventilation, etc.). - Car and landing indicators. - Hoisting machine motor control. - Door control including its protective devices. - Load control. - Run time limiter. - Fire service operation. - Return to normal operation of the lift. - Re-opening of the door. - Remote monitoring and interaction. **Escalator and moving walks:** - Start and stop functionalities. - Timetable and system clock operations. - Direction indicators. - Preventing from starting when permitted stopping distance exceeded. - Protection of motors. - Automatic operation: starting in predetermined direction. - Remote monitoring and interaction.
Alarm	Devices used to verify entrapment, to call for help and to rescue passengers in case of entrapment.	- Alarm, intercom, and video devices. - Emergency supply. - Evacuation device. - Displays and voice announcements used for rescue.
Other	Additional functions not related to safety, essential or alarm domains.	— Advertising displays. — Music and gaming devices. — User applications.

Table.4 Domains of the EUC functions