ENGINEERING
TOMORROW

User Guide

Cybersecurity for iC7-Automation Frequency Converters

An Informative Guide for System Integrators to Achieve the Required Security Level with Danfoss iC7-Automation Frequency Converters According to IEC 62443-3-3.

drives.danfoss.com | iC7

Contents

1 Introduction

1.1 Purpose of this Document

The IEC standard 62443-3-3 is used by the system integrator to explain the cybersecurity of a system. The system integrator or OEM must demonstrate that the system designed has the capability to support the security level intended for different parts/zones in the system.

This document is a guide with recommendations aimed at system integrators using the iC7 frequency converters as a component in the system. Drives in scope for this document: iC7-Automation Frequency Converters.

As product supplier, Danfoss shares information on frequency converters to be used in the system based on:

- IEC 62443-4-1: Development and production of the components
- IEC 62443-4-2: Description of the product, giving information on threats and mitigations, and how this product is compliant to achieve a certain security level.

The components selected to be used in the system must be able to fulfill the requirements needed for the intended/targeted security level (SL-T).

Table 1: Security Level (SL-T) and its IEC 62433-3-3 Definition

Security level (SL-T)[1]	IEC 62433-3-3 definition
SL-4	Identify and authenticate all users by mechanisms which protect against intentional unauthenticated access by using sophisticated means with extended resources, IACS specific skills, and high motivation.
SL-3	Identify and authenticate all users by mechanisms which protect against intentional unauthenticated access by using sophisticated means with moderate resources, IACS specific skills, and moderate motivation.
SL-2	Identify and authenticate all users by mechanisms which protect against intentional unauthenticated access by using simple means with low skills and low motivation.
SL-1	Identify and authenticate all users by mechanisms which protect against casual or coincidental access to unauthenticated entities.
SL-0	No specific requirements or security protection are necessary.

1) SL-0 is the lowest and SL-4 is the highest level.

The iC7 frequency converters are described in the perspective of interaction with settings and functions in the product either local or in remote operation:

Local operation is defined as manual interaction with the drive via the control panel or via pc software tools.

Remote operation is defined as an external controller, for example a PLC, interacting with the drive.

The actual target security level for iC7 frequency converters is SL-1.

Recommendations to obtain SL-1 using the drives listed above in a system can be found in the section: *Security Configuration Guidelines*.

A list for the IEC62443-4-2 Mitigation plan can be found in 5.4 IEC 62443-4-2 Mitigation List.

1.2 Extended Requirements

The IEC 62443 is the basis for the cybersecurity. If an issuer of certificates or approvals extends the requirements, it is important for the system integrator to take these requirements into account when preparing the cybersecurity documentation.

In this document, a list of issuers with extended requirements can be found.

1.2.1 DNV: Rules for Classification Ships Edition July 2023

In the document *Rules for Classification: Ships* edition July/2023, DNV has defined 3 levels of class notifications:

- Cyber Secure: The system under consideration (SuC) shall comply with requirements for security profile 0 (SP0).
- Cyber Secure (Essentials): The system under consideration (SuC) shall comply with requirements for security profile 1 (SP1).
- Cyber Secure (Advanced): The system under consideration (SuC) shall comply with requirements for security profile 3 (SP3).

Table 2: The Relations Between DNV Security Profiles and IEC 62443 Security Levels

DNV security profile (SP)	IEC 62443 security level (SL)
SP0: required for **Cyber Secure**	Selected requirements from SL1. Intended as minimum alignment with IMO MSC 828(98).
SP1: required for **Cyber Secure (Essentials)**	SL1. Protection against casual or coincidental violation.
SP2	SL2. Protection against intentional violation using simple means with low resources, generic skills, low motivation.
SP3: required for **Cyber Secure (advanced)**	SL3. Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills, moderate motivation.
SP4	SL4. Protection against intentional violation using sophisticated means with extended resources, IACS specific skills, high motivation.

This document focuses only on SP0 and SP1 requirements.

1.3 Document Version

This guide is regularly reviewed and updated. All suggestions for improvement are welcome.

The original language of this guide is in English.

Version	Remarks	Software version
BC509235134171, version 01	Preliminary release	x.x.x

2 Safety

2.1 Safety Precautions

For information on safety precautions, refer to the product-specific operating guide.

2.2 Qualified Personnel

To allow trouble-free and safe operation of the unit, only qualified personnel with proven skills are allowed to transport, store, assemble, install, program, commission, maintain, and decommission this equipment.

Persons with proven skills:

- Are qualified electrical engineers, or persons who have received training from qualified electrical engineers and are suitably experienced to operate devices, systems, plants, and machinery in accordance with pertinent laws and regulations.
- Are familiar with the basic regulations concerning health and safety/accident prevention.
- Have read and understood the safety guidelines given in all manuals provided with the unit, especially the instructions given in the operating guide.
- Have a good knowledge of the generic and specialist standards applicable to the specific application.
- Are cleared by the asset owner to have access to the work zone according to the security level in the zone.

3 Security Measures

The following measures ensure the integration of security in iC7 frequency converters from Danfoss:

- The *Secure product development lifecycle requirements* specified in IEC 62443-4-1 are implemented. The implementation is certified by TÜV SÜD.
- has implemented measures to safeguard integrity in our products and our manufacturing processes.
- constantly checks the measures relating to hardening. Operating systems are configured in such a way that points of attack via ports or connection points of unneeded services, are minimized.
- To detect weak points at an early stage, production system contains screening and control procedures in our production management system (PMS).

4 Security management

4.1 Overview

The security management is based on IEC 62443 and ISO 27001.

4.2 Procedure

1. Carry out an information security risk analysis. Determine all potential risks and define countermeasures for reducing the risk to an acceptable level.
   An information security risk analysis includes the following steps:
   - Identification of threatened objects
   - Analysis of value and potential for damage
   - Threat and weak point analysis
   - Identification of existing security measures
   - Risk evaluation
   - Evaluation of effects with respect to protection goals: confidentiality, integrity, and availability
2. Define guidelines and introduce coordinated, organizational measures. Establish awareness of the high relevance of industrial cybersecurity at all levels in the company. Define guidelines and processes for a consistent approach to security compliance.
3. Introduce coordinated technical measures.
4. Conduct a security audit to ensure that all of the measures have been implemented and that they have also eliminated or reduced the identified risks.

NOTICE

THIS IS A CONTINUOUS PROCESS.

- Due to ever-changing threat scenarios, this process must be constantly repeated. Implement the security management process as a continuous process. Updates must be expected during the product lifetime.

5 IEC 62443-4-2 Certification and Mitigation Plan

5.1 Overview

As a first step, iC7 Frequency Converters will be certified to meet all requirements for a IEC 62443-4-2 Security Level 1 (SL1) certification.

Higher security levels can be achieved, as iC7 Frequency Converters are secure by design:

- Data in the frequency converter is protected against tampering due to tamper-proof hardware.
- Firmware is only executed if it is genuine due to malicious firmware prevention.
- Local storage protection due to encrypted software installed to the drive.
- Secure network connectivity due to possible end-to-end encrypted communication to and from the drive.

5.2 Color Code and Mitigation List

In section 5.3 Codes for Mitigation to be Achieved with Other Means, the following color codes are used to indicate the solution.

Table 3: Color Codes

	It is impossible to achieve the required effect with current hardware (HW) and software (SW) design.
	This is possible with additional changes with the existing frame work.
	The product partly fulfills this requirement via similar means.
	The product already fulfills this requirement.
	Applicable according to standard, but either the product does not give access or is not allowed/able to handle this.
	Not applicable, irrelevant for this product.

5.3 Codes for Mitigation to be Achieved with Other Means

Table 4: Codes for Mitigation to be Achieved with Other Means

ID	Description
M1	**Access control for enclosure or room where iC7 series frequency converters are installed** The most basic line of defense is physically shielding the drives in enclosures or rooms with access control. The enclosure or room can have access control by locking mechanism where special tools, special keys, or access codes are needed to access the enclosure or room. Only qualified personnel have the means to get access.
M2	**Remove the control panel (CP) from iC7 series frequency converter to prevent local access** Remove the control panel (CP) from the iC7 frequency converter under normal operation. If unintended access should happen, removing the CP will prevent access to the drive parameters. In service cases, a control panel can be handed out by the owner of the installation to a trusted person, for example, a trained service technician.
M3	**Access control handled on system level** On system level, the access control to the user interface (SCADA, HMI, and so on) is recommended to include an access control with password.
M4	**Wireless option is not recommended.** Alternatively "No wireless options are available for iC7 series frequency converters. For future use cases it is not recommended to use any wireless option as it will provide more open access. The same applies to the control panel with integrated wireless functionality.
M5	**Strength of password handled on system level** It is recommended to introduce guidelines for using strong passwords and how often these passwords are changed. It is recommended that the guidelines are implemented consistently in the deployed engineering tools used.

Table 4: Codes for Mitigation to be Achieved with Other Means (continued)

ID	Description
M6	**System design to ensure connection only to trusted networks** The *trusted network* should be understood, from a cybersecurity viewpoint, as being a strictly limited and well-hosted portion of a certain network or control system. For recommendations to achieve security level SL-1, see section 8.2.1 Local Access.
M7	**Utilize segmentation at network level** Segmentation can be used to divide the network into smaller parts. The purpose can both improve network performance and cybersecurity.

5.4 IEC 62443-4-2 Mitigation List

Table 5: IEC 62443-4-2 Mitigation List

IEC62443-4-2 FRs, CRs and REs	SL1 (1)	Mitigation at system level recommended (Section 3-3)
FR 1 - Identification and authentication control (IAC) - Chapter 5		
CR 1.1 - Human user identification and authentication	✓	M1, M2, M3
RE (1) Unique identification and authentication	–	–
RE (2) Multifactor authentication for all interfaces	–	–
CR 1.2 -Software process and device identification and authentic action	–	–
RE (1) Unique identification and authentication	–	–
CR 1.3 - Account management	✓	M1, M2, M3
CR 1.4 - Identifier management	✓	M1, M2, M3
CR 1.5 - Authenticator management	✓	M1, M2, M3
RE (1) Hardware security for authenticators	–	–
NDR 1.6 Wireless access management	✓	NDR does not apply to the drive now as long as no Wi-Fi bridging is available.
RE (1) Unique identification and authentication	–	–
CR 1.7 - Strength of password-based authentication	✓	M5
RE (1) Password generation and lifetime restrictions for human users	–	–
RE (2) Password lifetime restrictions for all users (human, software process, or device)	–	–
CR 1.8 - Public key infrastructure certificates	–	–
CR 1.9 - Strength of public key-based authentication	–	–
RE (1) Hardware security for public key-based authentication	–	–
CR 1.10 - Authenticator feedback	✓	Implemented
CR 1.11 - Unsuccessful login attempts	✓	M2, M3
CR 1.12 - System use notification	✓	M6
NDR 1.13 - Access via untrusted networks	✓	NDR does not apply to the drive now as long as no Wi-Fi bridging is available.
RE (1) Explicit access request approval	–	–

Table 5: IEC 62443-4-2 Mitigation List (continued)

IEC62443-4-2 FRs, CRs and REs	SL1[(1)]	Mitigation at system level recommended (Section 3-3)
CR 1.14 - Strength of symmetric key-based authentication	–	–
RE (1) Hardware security for symmetric key-based authentication	–	–
FR 2 - Use control (UC) - Chapter 6		
CR 2.1 Authorization enforcement	✓	M1, M2, M3
RE (1) Authorization enforcement for all users (humans, software processes, and devices)	–	–
RE (2) Permission mapping to roles	–	–
RE (3) Supervisor override	–	–
RE (4) Dual approval	–	–
CR 2.2 -Wireless use control	✓	Fulfilled, as soon as CR2.1. is fulfilled.
CR 2.3 - Use control for portable and mobile devices	–	–
SAR 2.4 - Mobile code	✓	Not applicable for the drive
RE (1) Mobile code authenticity check	–	–
EDR 2.4 Mobile code	✓	Mobile code is only supported via the MyDrive® Programming tool.
RE (1) Mobile code authenticity check	–	–
HDR 2.4 Mobile code	✓	Not applicable
RE (1) Mobile code authenticity check	–	–
NDR 2.4 Mobile code	✓	NDR does not apply to the drive now as long as no Wi-Fi bridging is available.
RE (1) Mobile code authenticity check	–	–
CR 2.5 Session lock	✓	M1, M2, M3
CR 2.6 Remote session termination	–	–
CR 2.7 Concurrent session control	–	–
CR 2.8 Auditable events	✓	Limited logging supported. View via MyDrive® Insight or control panel.
CR 2.9 - Audit storage capacity	✓	Implemented
RE (1) Warn when audit record storage capacity threshold reached	–	–
CR 2.10 - Response to audit processing failures	✓	View logfiles frequently using MyDrive® Insight or control panel.
CR 2.11 - Timestamps	✓	Implemented
RE (1) Time synchronization	–	–
RE (2) Protection of time source integrity	–	–
CR 2.12 - Non-repudiation	✓	Implemented
RE (1) Non-repudiation for all users	–	–
EDR 2.13 Use of physical diagnostic and test interfaces	–	–

Table 5: IEC 62443-4-2 Mitigation List (continued)

IEC62443-4-2 FRs, CRs and REs	SL1[(1)]	Mitigation at system level recommended (Section 3-3)
RE (1) Active monitoring	–	–
HDR 2.13 - Use of physical diagnostic and test interfaces	–	Not applicable
RE (1) Active monitoring	–	–
NDR 2.13 - Use of physical diagnostic and test interfaces	–	NDR does not apply to the drive now as long as no Wi-Fi bridging is available.
RE (1) Active monitoring	–	–
FR 3 – System integrity (SI) - Chapter 7		
CR 3.1 - Communication integrity	✓	M1, M7. MyDrive® Insight supports TLS.
RE (1) Communication authentication	–	–
SAR 3.2 Protection from malicious code	✓	Not applicable
EDR 3.2 Protection from malicious code	✓	Implemented in firmware update manager.
HDR 3.2 Protection from malicious code	✓	Not applicable
RE (1) Report version of code protection	–	–
NDR 3.2 Protection from malicious code	✓	NDR does not apply to the drive now as long as no Wi-Fi bridging is available.
CR 3.3 - Security functionality verification	✓	Included, MyDrive® Insight can verify the configuration of the drive.
RE (1) Security functionality verification during normal operation	–	–
CR 3.4 - Software and information integrity	✓	Included
RE (1) Authenticity of software and information	–	–
RE (2) Automated notification of integrity violations	–	–
CR 3.5 - Input validation	✓	HMI supports this.
CR 3.6 - Deterministic output	✓	Output reaches a predetermined state based on user configuration. • Fieldbus failure • Safety function failure • Any other fault
CR 3.7 - Error handling	✓	HMI supports this.
CR 3.8 - Session integrity	–	–
CR 3.9 - Protection of audit information	–	–
RE (1) Audit records on write-once media	–	–
EDR 3.10 Support for updates	✓	Fulfilled
RE (1) Update authenticity and integrity	–	–
HDR 3.10 - Support for updates	✓	Not applicable
RE (1) Update authenticity and integrity	–	–
NDR 3.10 - Support for updates	✓	NDR does not apply to the drive now as long as no Wi-Fi bridging is available.
RE (1) Update authenticity and integrity	–	–

Table 5: IEC 62443-4-2 Mitigation List (continued)

IEC62443-4-2 FRs, CRs and REs	SL1[(1)]	Mitigation at system level recommended (Section 3-3)
EDR 3.11 Physical tamper resistance and detection	–	–
RE (1) Notification of a tampering attempt	–	–
HDR 3.11 Physical tamper resistance and detection	–	–
RE (1) Notification of a tampering attempt	–	–
NDR 3.11 Physical tamper resistance and detection	–	–
RE (1) Notification of a tampering attempt	–	–
EDR 3.12 Provisioning product supplier roots of trust	–	–
HDR 3.12 Provisioning product supplier roots of trust	–	–
NDR 3.12 Provisioning product supplier roots of trust	–	–
EDR 3.13 Provisioning asset owner roots of trust	–	–
HDR 3.13 Provisioning asset owner roots of trust	–	–
NDR 3.13 Provisioning asset owner roots of trust	–	–
EDR 3.14 Integrity of the boot process	✓	Implemented
RE (1) Authenticity of the boot process	–	–
HDR 3.14 Integrity of the boot process	✓	Not applicable
RE (1) Authenticity of the boot process	–	–
NDR 3.14 Integrity of the boot process	✓	NDR does not apply to the drive now as long as no Wi-Fi bridging is available.
RE (1) Authenticity of the boot process	–	–
FR 4 – Data confidentiality (DC) - Chapter 8		
CR 4.1 - Information confidentiality	✓	Implemented
CR 4.2 - Information persistence	–	–
RE (1) Erase of shared memory resources	–	–
RE (2) Erase verification	–	–
CR 4.3 - Use of cryptography	✓	Implemented
FR 5 – Restricted data flow (RDF) - Chapter 9		
CR 5.1 - Network segmentation	✓	M7
NDR 5.2 Zone boundary protection	✓	Not applicable
RE (1) Deny all, permit by exception	–	–
RE (2) Island mode	–	–
RE (3) Fail close	–	–
NDR 5.3 - General purpose, person-to-person communication restrictions	✓	Not applicable
FR 6 – Timely response to events (TRE) - Chapter 10		
CR 6.1 - Audit log accessibility	✓	M1, M2, M3
RE (1) Programmatic access to audit logs	–	–
CR 6.2 - Continuous monitoring	–	–

Table 5: IEC 62443-4-2 Mitigation List (continued)

IEC62443-4-2 FRs, CRs and REs	SL1[1]	Mitigation at system level recommended (Section 3-3)
FR 7 – Resource availability (RA) - Chapter 11		
CR 7.1 - Denial of service protection	✓	Monitoring and alarming are handled on control system level. The risk for a DoS event happening only on a drive level is seen as very low. Drive recovers after a flood attack.
RE(1) Manage communication load from component	–	–
CR 7.2 - Resource management	✓	Fulfilled by task management (priority schema in OS).
CR 7.3 - Control system backup	✓	MyDrive® Insight backup files.
RE (1) Backup integrity verification	–	–
CR 7.4 - Control system recovery and reconstitution	✓	MyDrive® Insight backup files.
CR 7.5 - Emergency power	–	To be handled on control system level.
CR 7.6 - Network and security configuration settings	✓	Implemented
RE (1) Machine-readable reporting of current security settings	–	–
CR 7.7 - Least functionality	✓	Unused ports and services can be disabled.
CR 7.8 - Control system component inventory	–	–

1) SL1: Protect the integrity of the IACS against casual or coincidental manipulation.

6 Extended Requirements

6.1 Overview

In this section, requirements in relation to specific approvals or certificates are listed. These requirements can either have been extended or limited towards IEC 62443.

6.2 DNV Rules for Classification Ships Edition July/2023

The DNV document, *section 21: Cybersecurity*, provides definitions on which security profile is to be used for the Class notifications:

- **Cyber Secure:** The system under consideration (SuC) shall comply with requirements for security profile 0 (SP0).
- **Cyber Secure (Essentials):** The system under consideration (SuC) shall comply with requirements for security profile 1 (SP1).
- **Cyber Secure (Advanced):** The system under consideration (SuC) shall comply with requirements for security profile 3 (SP3).

In DNV document, *Section 21 Chapter 4.1.2 Security Profile Adaptations*, differences between IEC 62443-3-3 (SL) and security profiles (SP) are listed:

1. SP0 is a security profile that is not based on any security level of IEC 62443-3-3. The level of risk reduction is less than SL1 in IEC 62443-3-3.
2. Requirements listed with *H* are more stringent than IEC 62443-3-3 since these apply for an SP that is lower than the corresponding SL in IEC 62443-3-3.
3. Requirements indicated with *L* are less stringent than IEC 62443-3-3 since these apply for an SP that is higher than the corresponding SL in IEC 62443-3-3.

NOTICE

- DNV Rules for Classification Ships Edition July/2023 is used as an example of UR E26 and E27 requirements, and therefore mitigations are compliant with other class societies rules regarding UR E26 and E27 based cybersecurity requirements.

6.3 DNV July/2023 UR E27 Requirements Mitigation List

Drives mitigations are risk based. To control the risks iC7-Automationdrives create for the system, take different countermeasures on control system, network, and physical security level. All proposed mitigations create low or very low risk on a system level.

Table 6: DNV July/2023 UR E27 Requirements Mitigation List

DNV rules for classification ships edition July/2023 requirements	SP1 (1)	Mitigation at system level recommended (*Chapter 6.2.3*)
User identification and authentication		
Human users shall be identified and authenticated for access to the system.	YES	M1, M2, M3
Multifactor authentication is required for human users when accessing the system from or via an untrusted network.	YES H	–
Identification and authentication of devices and software processes shall be implemented on interfaces providing access to the system.	YES H	M1, M2, M3
Account management		
It shall be possible to manage all accounts (human user accounts and non-human user accounts). This shall at least include adding, activating, modifying, disabling, and removing accounts.	YES	M1, M2, M3
Identifier management		

Table 6: DNV July/2023 UR E27 Requirements Mitigation List (continued)

DNV rules for classification ships edition July/2023 requirements	SP1[(1)]	Mitigation at system level recommended (*Chapter 6.2.3*)
It shall be possible to manage identifiers in the system. The intention is to allow for segregation of duties and least privilege by assignment of different privileges depending on user, role, group, or interface.	YES	M1, M2, M3
Authenticator management		
It shall be possible to manage authenticators in the system. This implies, for example, initializing, changing, and protecting passwords from unauthorized disclosure when stored and transmitted.	YES	M1, M2, M3
Wireless access management		
All users (human and non-human) shall identify and authenticate themselves to access the system by wireless communication.	YES	–
Strength of password-based authentication		
It shall be possible to configure minimum length of passwords.	YES	M5
Authenticator feedback		
The system shall obscure feedback during the authentication process (for example, display asterisks instead of password characters during the login process).	YES	M1, M2, M3
Unsuccessful login attempts		
The system shall enforce a limit of consecutive invalid login attempts during a specified time period. Access shall be denied for a configurable period of time or until an administrator unlocks the account. For critical services, the control system shall provide the capability to disallow interactive logons with the service account.	YES	M1, M2, M3
System use notification		
It shall be possible to configure a notification message to be shown when a human user authenticates to the system.	YES	M6
Access via untrusted networks		
Any access from or via untrusted networks shall be monitored (for example, logged, indicated, alarmed) and controlled (for example, denied, restricted).	YES	M6
The system shall deny access from or via untrusted networks if the request is not approved by authorized personnel on board.	Yes [H]	M6
Authorization enforcement		
On all interfaces, human users shall be assigned authorizations in accordance with the principles of segregation of duties and least privilege.	YES	M1, M2, M3
Wireless use control		
The system shall authorize, monitor, and enforce usage restrictions for wireless connectivity.	YES	–
Use control for portable and mobile devices		
The system shall enforce usage restrictions of portable and mobile devices.	YES	M1
Mobile code		
The system shall restrict use of mobile code such as java scripts, ActiveX, and PDF.	YES	Mobile code is only supported via the MyDrive® Programming tool.
Session lock		

Table 6: DNV July/2023 UR E27 Requirements Mitigation List (continued)

DNV rules for classification ships edition July/2023 requirements	SP1 (1)	Mitigation at system level recommended (*Chapter 6.2.3*)
The system shall be able to prevent further access after a configurable time of inactivity or following activation of the manual session lock.	YES	M1, M2, M3
Remote session termination		
The system shall automatically terminate a remote session after a configurable time of inactivity, or by manual termination by a responsible crew member. The effect of terminating a remote session during on-going operations shall be considered and not endanger the vessel or its crew.	YES H	M1
Auditable events		
The system shall generate audit records for access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity, and audit log events. Each record shall include timestamp, source, category, type, event ID, and event result.	YES	Limited logging supported. View via MyDrive® Insight or control panel.
Audit storage capacity		
Sufficient storage capacity for audit records shall be provided. As part of the audit, storage capacity for such records shall be monitored.	YES	–
Response to audit processing failures		
The system shall alert responsible personnel and prevent loss of essential or important functions in the event of an audit processing failure.	YES	View log file frequently using MyDrive® Insight or control panel.
Timestamps		
The system shall timestamp each audit record.	YES H	–
Communication integrity		
The system shall protect the integrity of transmitted information.	YES	M1, M7
The system shall apply cryptographic algorithms to protect the integrity of transmitted information.	YES H	MyDrive® Insight supports TLS. Fieldbus protocols do not support security.
Malicious code protection		
The system shall have protection mechanisms against malicious code or unauthorized software. This shall include prevention, detection, reporting and mitigating countermeasures. The protection mechanism shall be kept updated, see also DNV-CG-0325.	YES	–
Malicious code protection shall also be implemented on entry and exit points to the system (for example, removable media, remote access servers, and so on).	YES	–
Security functionality verification		
It shall be possible (at least during test phases and scheduled maintenance) to verify that the required security functions operate as intended.	YES	MyDrive® Insight can verify the configuration of the drive.
Input validation		
Inputs that may directly impact control functions shall be validated. This requirement does not address human error when entering, for example, commands or setpoints at a local HMI.	YES	HMI supports this. Fieldbuses are not covered.
Deterministic output		

Table 6: DNV July/2023 UR E27 Requirements Mitigation List (continued)

DNV rules for classification ships edition July/2023 requirements	SP1 (1)	Mitigation at system level recommended (*Chapter 6.2.3*)
The system shall respond in a fail-to-safe manner as per Pt.4 Ch.9 Sec.2 [2.2] if normal operation may not be maintained as a result of a cyber incident.	YES	Output reaches a predetermined state based on user configuration. • Fieldbus failure • Safety function failure • Any other fault
Session integrity		
The system shall protect the integrity of sessions. Invalid session IDs shall be rejected.	YES H	HMI supports this. Fieldbuses are not covered.
The system shall invalidate session IDs after user logout or other session termination (including browser sessions).	YES H	HMI supports this. Fieldbuses are not covered.
The system shall generate a unique session ID for each session. Unexpected session IDs shall be treated as invalid.	YES H	HMI supports this. Fieldbuses are not covered.
Information confidentiality		
The system shall be able to protect the confidentiality of information at rest or in transit that has read authorization.	YES	–
Use of cryptography		
If cryptography is required, the system shall use algorithms, key sizes, and mechanisms for key establishment and management based on best practices and recommendations.	YES	–
Network segmentation		
Separation of zones in [3.2] shall be implemented by logical or physical network segmentation.	YES	M7
Physical network segmentation is required for OT/IT systems and safety systems. See [3.2.3] and [3.2.5].	YES H	M7
Zone boundary protection		
Communication traversing zone boundaries shall be controlled and monitored to enforce the compartmentalization for zones and conduits.	YES	M7
Communication traversing zone boundaries shall be controlled according to the principle of deny by default, allow by exception.	YES H	M7
It shall be possible to manually stop communication between zones serving essential or important services, including boundaries to safety functions and IT zones (island mode).	YES H	M7
General purpose person-to-person communication restrictions		
External general purpose person-to-person messages shall not be received by the system.	YES	–
Application partitioning		
Data, applications, and services shall be subject to partitioning or separation in accordance with the zoning model. This implies that different zones shall not depend on the same data, applications, or services.	YES	M7
Audit log accessibility		
The system shall provide read-only access to audit records for authorized users.	YES	M1, M2, M3

Table 6: DNV July/2023 UR E27 Requirements Mitigation List (continued)

DNV rules for classification ships edition July/2023 requirements	SP1 (1)	Mitigation at system level recommended (*Chapter 6.2.3*)
Denial of service protection (DoS)		
The system shall be able to operate in a degraded mode during a DoS event. Amendments: • This requirement shall be seen in context with Pt.4 Ch.9 Sec.4 [3.1.3]. • Monitoring and alarming of network status shall follow the requirements in Pt.4 Ch.9 Sec.4 [3.1.4].	YES	Monitoring and alarming are handled on the control system level. The risk for a DoS event happening only on drive level is seen as very low. Drive recovers after a flood attack.
Resource management		
The system shall be able to schedule system resources for higher priority software processes such as, shutdowns, alarming, and monitoring over lower priority tasks, such as network scans.	YES	There is task management (Priority schema in OS).
Control system backup		
It shall be possible to create a complete backup of the system during normal operation.	YES	MyDrive® Insight backup files.
Control system recovery and reconstitution		
It shall be possible to recover and reconstitute the system after a cyber incident.	YES	MyDrive® Insight backup files.
Emergency power		
If the system is supplied from 2 or more power sources, switching between these sources shall not affect security functions of the system.	YES	Handled on control system level
Network and security configuration		
It shall be possible to configure the system's network and security parameters according to recommended guidelines from the supplier. An interface shall exist to monitor these settings.	YES	–
Least functionality		
Unnecessary functions, ports, protocols, and/or services shall be disabled, prohibited, or removed from the system.	YES	Unused ports and services can be disabled

1) SP1: Required for cybersecure (Essential). Corresponds to IEC 62443 SL1 – Protection against casual or coincidental violation.

7 iC7-Automation Frequency Converters

7.1 Overview

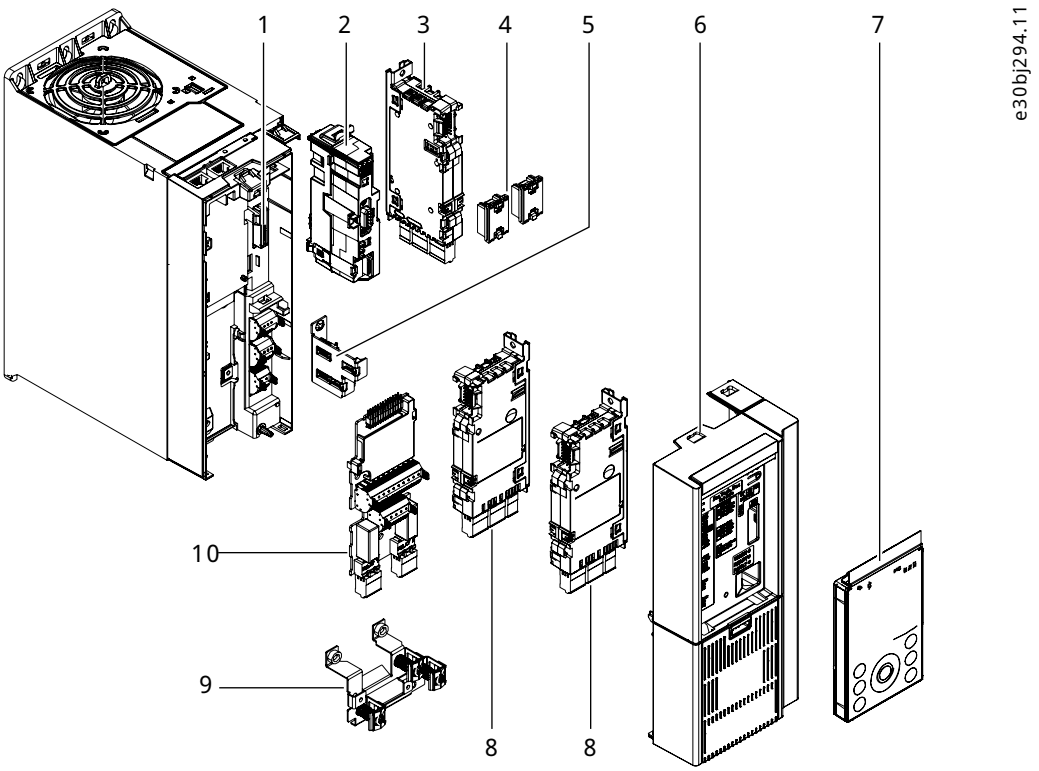
The iC7 series frequency converter is built as a modular, configurable drive, which can be complemented with functional extensions to match application needs. All options are configurable and can be selected when ordering the drive. Functional extensions, fieldbuses, and additional software can also be added later as a field upgrade.

The drive consists of a power unit, a control unit, and an application software package. In addition, a range of options and accessories are available

More detailed product specifications can be found in the *iC7-Automation Design Guide* iC7-Automation (www.danfoss.com)

7.2 Control Unit and Interfaces

The drive has an integrated control unit, which consists of a control board with integrated functional safety, integrated Ethernet ports, option slots for additional option boards, and a control panel. See Figure 1 for an illustration of the control unit mechanics.



1	Control board	**2**	Interface board
3	Option placed in slot C	**4**	Option connectors
5	EMC plate	**6**	Terminal cover
7	Control panel	**8**	Options placed in slots A and B
9	EMC plate	**10**	Basic I/O board

Figure 1: Control Unit Mechanics

iC7-Automation is delivered with the **Industry** application software package. Optional applications can be included from the factory or added later with a proof-of-purchase token.

7.3 Control Board and Standard I/O

The control board concept offers a high level of flexibility in use due to its scalability, protects the setup and operation of the drive, and is easy to connect with the pluggable terminals.

- Increased security: Integrated crypto-chip-based security features in the drive protect against unauthorized changes to the settings and software of the drive.
- Memory card reader: The microSD card reader enables software upgrades, data logging, or copying settings from one drive to another drive. Data is protected by the security features of the drive.
- Pluggable control terminals: The terminals are pluggable and allow bridging of control wires.
- PELV (galvanic) isolated control terminals: All control terminals and output relay terminals are galvanically isolated from mains power. The isolation meets the protective extra-low voltage (PELV) requirements for isolation.
- Integrated functional safety (SIL 3): The control board provides the Safe Torque Off (STO) safety function with a dual-channel, galvanically isolated input up to PL e and SIL 3 and an STO feedback signal for diagnostic purposes.
- Flexible basic I/O: The optional basic I/O board adds 4 digital inputs, 2 combined digital inputs/outputs, 2 analog inputs, 1 analog output, and 2 relay outputs to extend the connectivity of the drive. More I/O options can be added in up to 4 option slots. The options offer added functionality such as relays, digital and analog I/O, encoder/resolver support, temperature measurement, and functional safety I/O.
- 24 V DC external supply: The drive is fitted with the possibility to connect an external 24 V DC supply to the control board to allow continued operation of fieldbus and control programs, when mains power is switched off.

7.4 Communication Interfaces

The drives have built-in communication ports:

- Ethernet ports X1 and X2 allow connections to fieldbus systems with support for daisy chaining and single connections. The selected protocol comes preconfigured from the factory. Modbus TCP is offered as standard, and other protocols such as PROFINET RT and EtherNet/IP are available either preinstalled from the factory, or alternatively, they can be activated later with a proof-of-purchase token. Safe fieldbus protocols are also supported.
- Ethernet port X0 is available to connect to a PC or similar tools used for commissioning or service.

Additionally, the OPC UA monitoring protocol can be added as a secondary bus to standard Ethernet-based fieldbus protocols.

7.5 Control Panel and Keypad

7.5.1 Control Panels

The iC7 series offers a broad range of interfaces showing simple status readouts over wireless communication to advanced user interfaces giving access to drive parameters and settings.

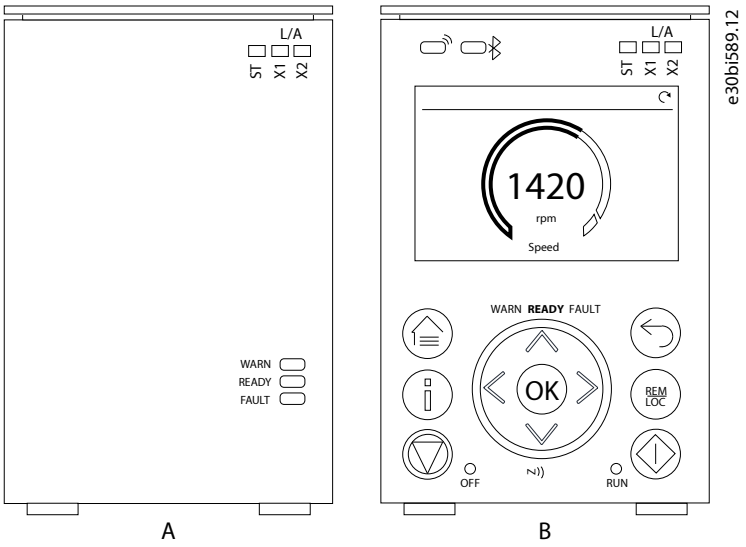


Figure 2: Control Panel Options

- **Blind Panel OPX00**: The Blind Panel has indicators showing the status of the drive and the fieldbus connection. It is typically used when limited interaction is required with the drive after installation and commissioning, or when the drives are controlled by fieldbus.
- **Control Panel 2.8 OPX20**: The Control Panel 2.8 is typically used when regular interaction with the drive is expected. The Control Panel 2.8 has the basic status and fieldbus indicators, a 2.8 inch graphical display, and tactile feedback buttons. The halo around the navigation buttons indicates the drive status and is visible from a long distance.

Mounting kits are available for external mounting of control panels.

7.5.2 Display

To avoid unintended interaction via the control panel, the control panel display can be locked. To lock the control panel, press the [*Back*] button for 3 s. After 3 s, the following screen is shown.

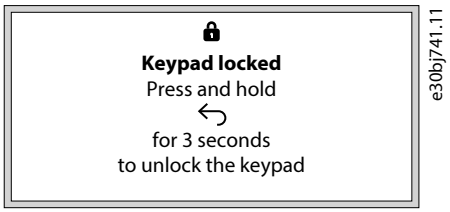


Figure 3: Control Panel Lock Screen

When the control panel is locked, pressing the control panel buttons has no effect. To unlock the control panel, press the [*Back*] button for 3 s.

7.5.3 Local and Remote Operation

- Use the [*REM/LOC*] button to switch between local and remote control
- When remote control is active, the start/stop commands can be executed from Fieldbus or from I/O terminal.
- When local control is active, the start/stop commands can be executed from the keypad.

7.6 Functional Extension Options

7.6.1 Overview

More I/O functions can be added to the iC7-Automation frequency converters to match the specific needs of applications. Depending on the frequency converter frame, up to 4 functional extensions can be added.

A full overview of available options can be found in the *iC7-Automation Design Guide* on iC7-Automation (www.danfoss.com)

7.6.2 Option Slots

The options are placed in option slots A–E. For more information on the detailed physical positions of the option slots, see Figure 4.

As the connections to some option positions are established via other options, the following dependencies must be observed when designing the system:

- Option in slot B requires an option in slot A.
- Option in slot D requires an option in slot C.
- Option in slot E requires options in both slot C and slot D.

> **TIP:** When ordering frames Fx02–Fx05 without options or an option in slot A only, it is important to consider carefully if more than 1 option is needed later. Adding more options increases the depth of the frequency converter. To ensure upgradability, select code +CBX0 when ordering a frequency converter.

Table 7: Number of Functional Extensions per Frame

Frame	Number of options	Option slot
FA02a–FA05a	1	A
FA02b	2	A, B
FA03b–FA04b	3	A, B, C
FA05b	4	A, B, C, D
FA06–FA12	4	A, C, D, E
FB09–FB12		
FK06–FK12		

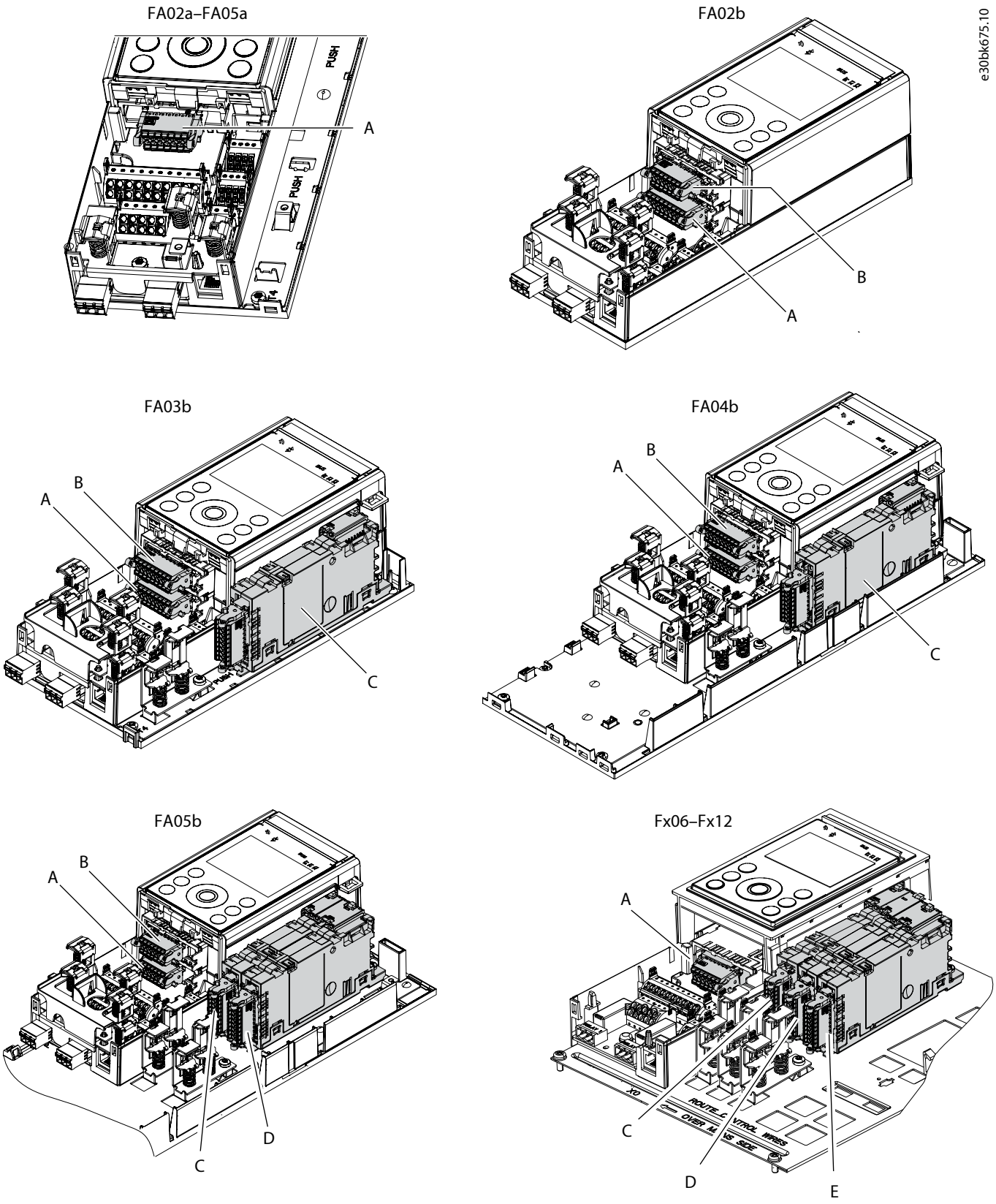


Figure 4: Option Slot Locations in iC7-Automation Frequency Converters

7.7 Tools and Software for iC7-Automation Frequency Converters

MyDrive® Insight

MyDrive® Insight is a pc software tool that gives easy access to iC7 series frequency converters, locally or remotely. Use it for commissioning, monitoring, and troubleshooting of drives.

Table 8: Features and Functions

Feature	Function
Discovery	Auto and direct
Parameter Management	Read/write, auto-sync, and compare, for efficient commissioning
Status	Drive info, notification, events, network topology, visualization
Monitoring	Scope, multi-device scope, Trending log, datalogger
Diagnostics	Event log, fault/warning notifications and details
Operating panel	Start, stop, reference, reset, automatic motor adaptation (AMA)
Backup/Restore	Parameters and user: set, backup, and restore
Reports	Commissioning, functional safety, scope, and service reports
Functional safety	Functional safety parametrization and online monitoring
Software update	Tool software, drive, and multi-drive package
Fundamentals	Integrated help, personalized user settings

For software packages and supporting documents, refer MyDrive® Insight

Software

Download software for iC7-Automation frequency converters from Software for iC7-Automation (www.danfoss.com).

8 Security Configuration Guidelines

8.1 Introduction to Recommendations

There are different possibilities to prevent local or remote access, to change settings, and to view data or settings in iC7 Frequency Converters. Below a number of principals are proposed. It is up to the system integrator to decide which principle gives the needed protection for the system.

Reduction of the attack surface

Minimizing the risk of attacks is to keep the attack surface as limited as possible and only to have configured necessary functions. The systems only have the software required for the necessary tasks, only the necessary ports and connection points are open or accessible. Also, only the necessary services are activated during operation.

Protection of access to enclosures and rooms

The most basic line of defense is physically shielding the drives in enclosures or rooms with access control. The enclosure or room can have access control by locking mechanism where special tools, special keys, or access codes are needed for accessing. Only qualified personnel have the means to get access.

This normally gives a good security level and fulfills SL-1.

8.2 Security Recommendations

8.2.1 Local Access

Protection methods: Recommendations for iC7-Automation frequency converters

- iC7-Automation frequency converters with protection class IP20 are to be used for installation in a lockable control cabinet/ switching room. The locked control cabinet/switching room must provide sufficient protection against access by unauthorized persons.
- For installation where the above described access preventions are not possible (often the case for installations with drives which are installed on a wall or floor mounted, especially drives with protection class IP21 or IP54), the following prevention methods are recommended:
  - Removing the control panel from the drives under normal operation.
  - If unintended access should happen, removing the control panel will prevent access to the drive parameters, and so on.
  - In service cases, a control panel can be handed out by the owner of the installation to a trusted person, for example, a trained service technician.

8.2.2 Connection to Trusted/Untrusted Networks

The *trusted network* is a carefully controlled and restricted segment within a specific network or control system.

If the network deployment occurs in an uncontrolled environment lacking adequate physical access control and account/domain management, it should be restricted to a carefully controlled and limited segment within a designated network or control system.

The drives must only be connected inside the trusted networks, which ensures that the measure for access is under control.

This connection must be created so that the drive connects only to the PLC point-to-point or via switches. Switches must be protected in a way that there is no possibility of exposing the drive to other devices and untrusted personnel.

Recommendations to ensure that only trusted devices have a connection to the drive:

- Protection for each network by allocating firewall solutions to the front of internal trusted networks of each network.
- Carefully manage firewalls, their configurations, and access rules.

The drives do not have internet connection capability without PLC interface. Ethernet-based control options allow for communication to the drive's IP address.

In-built Ethernet: The Ethernet module must be positioned in a trusted network.

All services are enabled by default. It is recommended to disable services that are not used after commissioning:

- PC tool communication
- Ping response
- iC7 series products do not support wireless connections at the moment. Remote access is possible only via other devices. It is not recommended to provide remote access through any devices other than PLC.

8.2.3 Unused Ports

If there are unused ports, integrators must do protection measures to protect the integrity of the drive.

Ethernet ports can also be configured by parameters to be enabled/disabled.

8.2.4 Secure Password Recommendations

Access protection can be compromised easily by using passwords that are not secure enough. Attackers can use compromised access data to log into systems and manipulate the behavior of the drive. This can result in the wrong operation of the drives and damage the installed equipment.

It is important to:

- Develop guidelines for password renewal. Do not keep the same password for a longer period. This excludes persons earlier having or not supposed to be having access anymore.
- Develop guidelines on handling access data. Make sure that the guidelines are implemented consistently in the deployed engineering tools.
- Always keep the access data secret. It is the installation owner's responsibility to ensure that only an authorized group of people is given access to the equipment to be able to change critical data.

When updating passwords, consider the following guidelines:

- Do not assign passwords that can be easily guessed, for example, simple number combinations like 1111 or 1234
- Assign, if possible, passwords with the required maximum length. This makes it more complicated to gain access unintentionally.

8.2.5 Service

The service is done using PC software tools which are operated on the service PC. iC7 series products have an Ethernet port interface to provide a connection for service PC. During the service, a trusted person, for example, a trained service technician is allowed to attach only trusted devices to the drive.

Recommendations for PC service:

- Do not have internet or other wireless connections active during the service.
- PC is hardened and enforces device security.

9 Software and Firmware Updates

- MyDrive® Insight
- Software for iC7-Automation (www.danfoss.com)

There is malicious firmware prevention, meaning that firmware is only executed if it is authenticated as genuine firmware.

10 Supplier Documentation

Various resources are available to give a better understanding of installation and make use of advanced drive operation and directives compliance. The following list of documents are available for the product:

Additional resources are available to help understand the features, and safely install and operate the iC7 series products:

- Safety guides, which provide important safety information related to installing iC7 series drives and power converters.
- Installation guides, which cover the mechanical and electrical installation of drives, power converters, or functional extension options.
- Design guides, which provide technical information to understand the capabilities of the iC7 series drives or power converters for integration into motor control and monitoring systems.
- Operating guides, which include instructions for control options, and other components for the drive.
- Application guides, which provide instructions on setting up the drive or power converter for a specific end use. Application guides for application software packages also provide an overview of the parameters and value ranges for operating the drives or power converters, configuration examples with recommended parameter settings, and troubleshooting steps.
- Other supplemental publications, drawings, and guides are available at www.danfoss.com.

Latest versions of Danfoss product guides are available for download at https://www.danfoss.com/en/service-and-support/documentation/.

Optional equipment is available that may change some of the information described in these publications. Be sure to follow the instructions supplied with the options for specific requirements. For regulary updated information related to cybersecurity vist: https://www.danfoss.com/en/about-danfoss/our-businesses/drives/knowledge-center/cyber-security/

Contact a Danfoss supplier or visit www.danfoss.com for more information.

ENGINEERING
TOMORROW

Danfoss A/S
Ulsnaes 1
DK-6300 Graasten
drives.danfoss.com

M00467