ENGINEERING
TOMORROW

User guide

Cybersecurity for iC7 System Products

An Informative Guide for System Integrators To Achieve the Required Security Level With Danfoss iC7 System Products for Marine Industry According to UR E26 and UR E27, and IEC 62443-3-3.

drives.danfoss.com | iC7

Contents

1 Introduction

1.1 Purpose of this Document

The unified requirements E26 and E27 are 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 system products for the marine industry as a component in the system. Drives in scope for this document: iC7 Marine (Active Front End and Propulsion and Machinery Inverter units) and iC7 Hybrid (Grid Converter, Generator INU and DC/DC converter based on liquid cooled system modules), in this document are referred to iC7 system drives for marine industry.

As product supplier, Danfoss shares information on iC7 system products to be used in the marine industry 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.
- Unified requirements E26 and E27

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 System Products for marine industry 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 local control panel (LCP) or via pc software tools.

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

The target security level for iC7 System Products for the marine industry 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 UR E27 Mitigation plan can be found in section 6.5 DNV July/2023 UR E27 Requirements 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

The Unified Requirements E26 and E27 are the bases for DNV: Rules for Classification Ships Edition July 2023. In this document, DNV Rules for Classification Ships Edition July 2023 are used as an example. This guidance can be used with the other Class Societies where cybersecurity requirements are based on UR E26 and UR E27.

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

- Cyber Secure
- Cyber Secure (Essentials)
- Cyber Secure (Advanced)

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.

A list for the UR E27 mitigation plan can be found in 6.5 DNV July/2023 UR E27 Requirements Mitigation List.

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
Document 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 System Products from Danfoss:

- The *Secure product development lifecycle requirements* specified in IEC 62443-4-1 are implemented. The implementation is certified by TÜV SÜD.
- Danfoss has implemented measures to safeguard integrity in our products and our manufacturing processes.
- Danfoss 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, Danfoss production system contains screening and control procedures in our production management system (PMS).

4 Security management

4.1 Overview

Danfoss drives 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

iC7 Marine-drives are working towards IEC 62443-4-2 SL1 certification.

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 Color Code and Mitigation List

In section 6.4 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 W and 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.

6.4 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 Marine-drives 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 LCP from iC7 Marine-drive to prevent local access** Remove the LCP from the iC7 Marine-drives under normal operation. If unintended access should happen, removing the LCP will prevent access to the drive parameters. In service cases, an LCP 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** iC7 Marine-drives does not include any wireless options.
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.
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.

6.5 DNV July/2023 UR E27 Requirements Mitigation List

Drives mitigations are risk based. To control the risks iC7 Marine-drives 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 5: 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

Table 5: 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*)
Identifier management		
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		

Table 5: 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 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		
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 local 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 local 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		

Table 5: 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*)
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		
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		

Table 5: 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*)
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
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 System Products for Marine industry

7.1 iC7 Marine and iC7 Hybrid

iC7 System products for the marine industry consist of iC7 Marine and iC7 Hybrid drives.

Table 6: iC7 Marine and iC7 Hybrid

	iC7-Marine	iC7-Hybrid
Products specifications	**Integrated applications** • Propulsion & Machinery (INU) **Hardware-specific functionality** • Active Front End (3A)	**Integrated applications** • Grid converter (GC) • DC/DC converter (DC)
Voltage range	3 x 525–690 V AC/640–1100 V DC 3 x 380–500 V AC/465–800 V DC (B5)	3 x 525–690 V AC/640–1100 V DC 3 x 380–500 V AC/465–800 V DC (B5)
Current range	Active Front End 236–5750 A Inverter Unit 170–6400 A	Grid Converter 236–5750 A DC/DC converter 300–3600 A

More information can be found from iC7 Marine (www.danfoss.com) and iC7 Hybrid (www.danfoss.com)

7.2 Interfaces

7.2.1 Default Interfaces

7.2.1.1 Overview

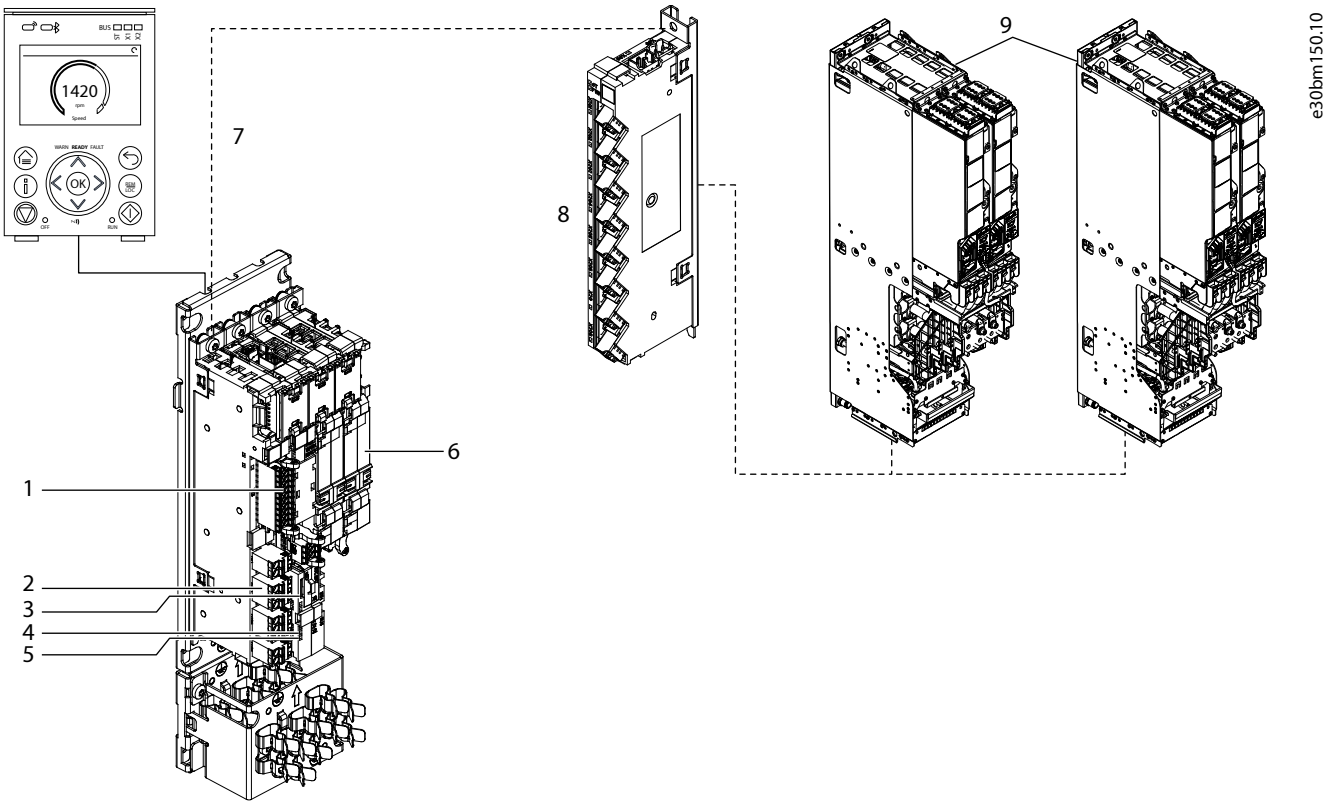

Figure 1: Interfaces of iC7 System Module

1	Basic I/O 6 × DI, 2 × DO, 2 × AI +/-10 V/0–20 mA, 1 × AO (0–10/4–20 mA)	**2**	NO/NC RO, 1 × NO RO 1 × Thermistor
3	Micro SD card for backup, firmware, logging data, setup transfer	**4**	Dual-Port Ethernet for multiple fieldbus protocols
5	Single Ethernet port for software tool	**6**	Option boards
7	Fiber optic	**8**	Star coupler board
9	Power units		

There are 3 Ethernet ports (Dual-port and Single Ethernet port) and a Micro SD card slot by default in the iC7 system module.

7.2.1.2 Ethernet Ports

- 2 Ethernet ports are used for fieldbus connection.
- One Ethernet port is used for PC tool connections.

Ethernet ports can be configured by parameters to be enabled/disabled. Daisy chaining the fieldbus is supported for typical protocols, such as Modbus TCP and PROFINET RT.

7.2.1.3 Micro SD Card Slot

The Backup feature in MyDrive® Insight stores the parameter settings of the drive into a new or existing project file, RAM, or Flash memory of the drive, or to an optional microSD card. To utilize the microSD card as a storage device, the microSD card must be inserted in the slot.

The microSD cards supported are: SD, SDHC, or SDXC which must be formatted for the FAT32 file system. SDHC is the recommended type, as they are delivered preformatted to FAT32.

7.2.2 Optional Interfaces

7.2.2.1 Control Panel and Keypad

The control panel is typically the standard user interface and used when frequent interaction with the drive is required. The option enables easy setup of the drive via parameters, monitor drive status, and also shows notifications, in case of an event.

7.2.2.2 Display

Figure 2: Display

- 2.8" monochromatic user interface with a display resolution of 240 x 160 pixels.

- Visual LEDs to identify drive status, fieldbus communication.
- Halo indicator with 3 colors to show drive status at a glance.
- A display which can be customized to show required or essential information.
- Buttons to control the drive locally, including a toggle button to easily switch between local and remote control.
- Parameter widgets which support alphanumeric and special characters, integers, floating points, date time formats, choice lists, and commands to configure application data.
- Help texts to support the operation.

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.

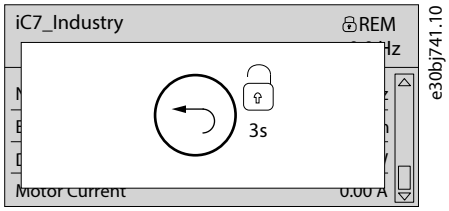

Figure 3: Control Panel Lock Screen

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.

7.2.2.3 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 (DI1 and DI2).
- When local control is active, the start/stop commands can be executed from the keypad.

7.2.2.4 Fiber Optic and Star Coupler Board

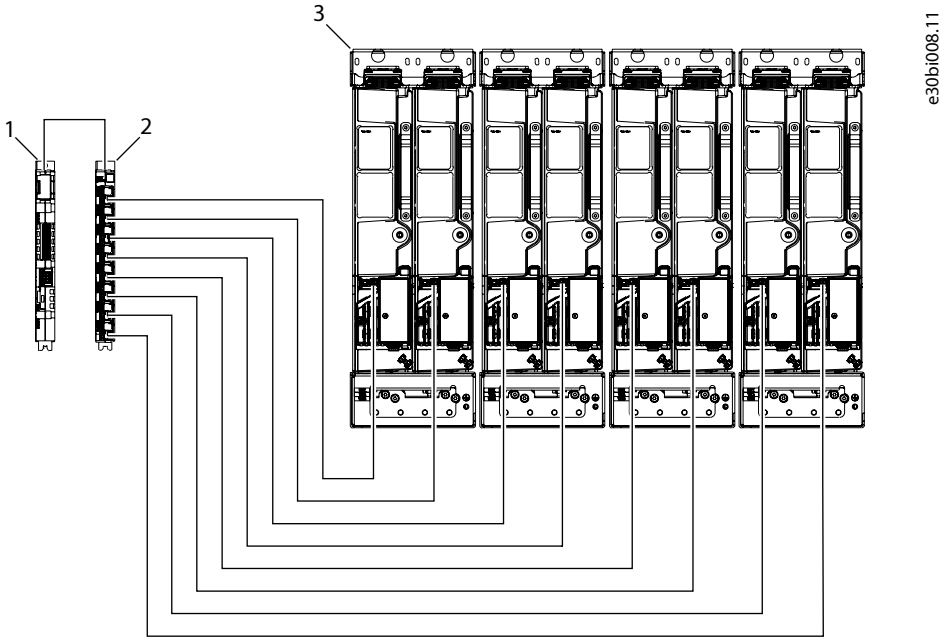

Figure 4: Example Control Connection with a Star Coupler Board: 8 Power Units in Parallel

1	Control board	**2**	Star coupler board
3	Maximum 16 power units		

The system modules are controlled with the modular control unit. The control unit and the system modules are connected via fiber optics. When 2 or more parallel system modules are used, a star coupler board is needed. The modular control unit provides an interface towards the upper control system.

There is also an Ethernet port in star coupler board. The port is used for fault tracking purposes and it is disabled by default. Credentials are needed to enable the port.

7.2.2.5 Functional Extensions

Additional functional extensions can be added to incorporate analog and digital inputs and outputs as well as other functionality such as temperature measurement or voltage measurement.

The modular control unit can be mounted nearby to or remotely from the power unit. The control unit consists of various boards installed on a mounting plate. The boards are connected to each other with option connectors. Several boards and mounting plates can be installed in parallel.

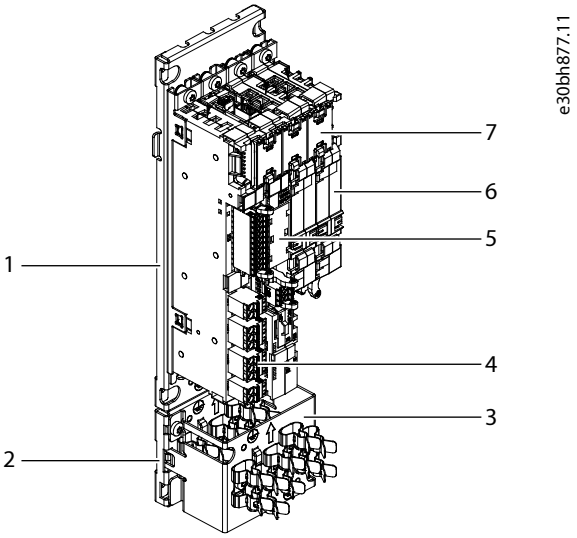

Figure 5: Example of the Modular Control Unit

1	Mounting plate	**2**	Base grounding plate
3	Grounding plate extension	**4**	I/O and relay option
5	Control board	**6**	Option board
7	Option connectors		

There are 3 different mechanical board types in the modular control unit:

- Control board
- Star coupler board
- Functional extensions, for example:
  - I/O and Relay Option (OC7C1)
  - Encoder/Resolver Option (OC7M0)
  - Temperature measurement option (OC7T0)
  - Voltage measurement option (OC7V0)

See more information on the option boards in the iC7 Series Functional Extension Options Installation Guide, the iC7 Series Functional Extension Options Operating Guide, and the iC7 Series Voltage Measurement Option OC7V0 Operating Guide.

7.3 Tools and Software for iC7 Marine and iC7 Hybrid Drives

MyDrive® Insight

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

Table 7: 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 Marine drives from Software for iC7 Marine (www.danfoss.com) and for iC7 Hybrid from Software for iC7 Hybrid (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 system products. 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 will normally give a good security level and fulfill SL-1.

8.2 Security Recommendations

8.2.1 Local Access

Protection methods: Recommendations for iC7 system products

- IC7 system products 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, the following prevention methods are recommended:
  - Removing the LCP from the iC7 system products under normal operation.
  - If unintended access should happen, removing the LCP will prevent access to the drive parameters, and so on.
  - In service cases, an LCP 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: Ethernet option 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 system 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 system 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 Marine (www.danfoss.com)
- Software for iC7 Hybrid (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:

The design guide provides specification and information to be used	iC7 Marine Documents (www.danfoss.com)
The operating guide provides detailed information for the installation and start-up of the drive	
The iC7 Series Active Front End Application Guide	
The iC7 Series Propulsion and Machinery Application Guide	
The iC7 Series DC/DC Converter Application Guide	iC7 Hybrid Documents (www.danfoss.com)
The iC7 Series Grid Converter Application Guide	

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.

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