ENGINEERING
TOMORROW

User Guide

Cybersecurity for Danfoss Drives

An informative Guide for System Integrators to Achieve the Required Security Level with Danfoss drives FC 102, FC 103, FC 202, FC 301, FC 302 According to IEC 62443-4-2.

drives.danfoss.com | VLT®

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.

omponent in the system. Drives in scope for this document: FC 102, FC 103, FC 202, FC 301 and FC 302, in this document referred to as FC-drives.

As Product Supplier, Danfoss shares information on FC-drives 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

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

The FC-drives are described based on their interaction with settings and functions in the product, either in local or in remote operation:

Local operation is defined as manual interaction with the drive via the local control panel (LCP) or via VLT® Motion Control Tool MCT 10.

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

Target security level for Danfoss FC-Drives 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 Chapter 5.

1.2 Extended requirements

The IEC 62443 is the bases 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
- 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

Since the objective for this document is IEC 62443-4-2 SL1, only SP0 and SP1 with extended requirements (“H” marked) will be discussed. Also, for these DNV security profiles, mainly connectivity to untrusted networks is in scope.

A list for the DNV mitigation plan can be found in section 6.2 DNV Rules for Classification Ships edition July/2023.

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
M0045101, document version 01	Preliminary release	x.x.x

2 Safety

2.1 Safety

When designing AC drives, some residual dangers cannot be avoided constructively. One example is the discharge time, which is important to observe to avoid potential death or serious injury. For the Danfoss VLT® drives, the discharge time is from 4–40 minutes depending on the drive size.

For further 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 work zone according to the security level in the zone.

3 Security Measures

Integration of security measures to handle misuse or tampering with the functioning of the product.

The following measures ensure the integration of security in FC-drives from Danfoss:

- The *Secure product development lifecycle requirements*specified in IEC 62443-4-1 are implemented.
- The implementation is TÜV certified with maturity level 2.
- Analyze functions are used to identify any errors in the programming code.
- 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

A security management process according to IEC 62443 and ISO 27001 forms the basis for implementation of industrial cyber security.

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
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 Security Mitigation Plan IEC 62443-4-2

5.1 Overview

IEC62443-4-2 mitigation list 20231208.pdf contains information on how to achieve the required security level. The recommendations to achieve SL-1 are mentioned in the following list.

Products in scope: FC 102, FC 103, FC 202, FC 301, FC 302

5.2 Color codes used in Mitigation list

In 5.4 IEC 62443-4-2 Mitigation List and 6.3 DNV July/2023 Extended Requirements Mitigation List the following color codes indicate the status of the mitigation.

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 products 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 FC-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. For recommendations to achieve security level SL-1, see sections 8.2.1 Local Access and 8.2.2 Remote Access.
M2	**Remove LCP from FC-drive to prevent local access** Remove the LCP from the FC-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 LCP103 is recommended not to be used** For the FC-drives, it is possible to connect 3 different LCP types. It is recommended to use only LCP101 or LCP 102. The LCP 103 opens up for access via a smart phone, which gives a more open access.
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 and 8.2.2 Remote 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	✓	M4 and change the default password for WLCP (***parameter 30-92***) even if not used.
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	✓	Only pass or fail feedback is given.

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 1.11 - Unsuccessful login attempts	✓	M1, use LCP to unlock drive for BUS.
CR 1.12 - System use notification	✓	M1
NDR 1.13 - Access via untrusted networks	✓	M6
RE (1) Explicit access request approval	–	–
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
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	✓	M1+M4 or change the default password for WLCP (***parameter 30-92***) even if not used.
CR 2.3 - Use control for portable and mobile devices	✓	The product does not use mobile code.
SAR 2.4 - Mobile code	✓	The product does not use mobile code.
RE (1) Mobile code authenticity check	–	–
EDR 2.4 Mobile code	✓	The product does not use mobile code.
RE (1) Mobile code authenticity check	–	–
HDR 2.4 Mobile code	✓	M1 to protect against usage of HW modules that allow execution of customized code.
RE (1) Mobile code authenticity check	–	–
NDR 2.4 Mobile code	✓	The product does not use mobile code.
RE (1) Mobile code authenticity check	–	–
CR 2.5 Session lock	✓	Set the access levels and passwords in *parameter group 0-6**.
CR 2.6 Remote session termination	–	–
CR 2.7 Concurrent session control	–	–
CR 2.8 Auditable events	✓	Auditable events must be compiled on the system level - software updates, drive unlocked (***parameter 16-94***, bit 18), configuration changes, service actions, etc.
CR 2.9 - Audit storage capacity	✓	Auditable events must be stored on the system level.

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) Warn when audit record storage capacity threshold reached	–	–
CR 2.10 - Response to audit processing failures	✓	M1 depends on system.
CR 2.11 - Timestamps	✓	Set date and time and use VLT® Real-Time Clock MCB 117 or date and time be updated regularly (after each power cycle at least).
RE (1) Time synchronization	–	–
RE (2) Protection of time source integrity	–	–
CR 2.12 - Non-repudiation	✓	Has the cabinet been hacked? Is the control room or system control device accessed?
RE (1) Non-repudiation for all users	–	–
EDR 2.13 Use of physical diagnostic and test interfaces	–	–
RE (1) Active monitoring	–	–
HDR 2.14 - Use of physical diagnostic and test interfaces	–	–
RE (1) Active monitoring	–	–
NDR 2.15 - Use of physical diagnostic and test interfaces	–	–
RE (1) Active monitoring	–	–
FR 3 – System integrity (SI) - Chapter 7		
CR 3.1 - Communication integrity	✓	The system integrator protects the communication channel with shielded wires, Wi-Fi LCP default password (***parameter 30-92***) is changed.
RE (1) Communication authentication	–	–
SAR 3.2 Protection from malicious code	✓	Application does not support mobile code.
EDR 3.2 Protection from malicious code	✓	M1 to protect against usage of HW modules that allow execution of customized code.
HDR 3.2 Protection from malicious code	✓	M1 to protect against usage of HW modules that allow execution of customized code.
RE (1) Report version of code protection	–	–
NDR 3.2 Protection from malicious code	✓	M1 to protect against usage of HW modules that allow execution of customized code.
CR 3.3 - Security functionality verification	✓	Automated test guidance document for customers.
RE (1) Security functionality verification during normal operation	–	–
CR 3.4 - Software and information integrity	✓	M1, M3
RE (1) Authenticity of software and information	–	–

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 (2) Automated notification of integrity violations	–	–
CR 3.5 - Input validation	✓	Unused I/O configurations are set to *No operation*, all inputs scaling are set and constantly monitored for unusual changes. Harden the parameter configuration by examining all the minimum/maximum limits.
CR 3.6 - Deterministic output	✓	Configure control word timeout and live zero actions as needed.
CR 3.7 - Error handling	✓	Configure and monitor the warning word. Examine the alarm log for past events.
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	✓	M1 + MCT 10 **Not an SR in 3-3!**
RE (1) Update authenticity and integrity	–	–
EDR 3.11 - Physical tamper resistance and detection	–	–
RE (1) Notification of a tampering attempt	–	–
EDR 3.12 - Provisioning product supplier roots of trust	–	–
EDR 3.13 - Provisioning asset owner roots of trust	–	–
EDR 3.14 Integrity of the boot process	✓	M1 **Not an SR in 3-3!**
RE (1) Authenticity of the boot process	–	–
FR 4 – Data confidentiality (DC) - Chapter 8		
CR 4.1 - Information confidentiality	✓	M1, M4, M6 Confidentiality to be handled on system level. It is recommended to only connect to trusted networks. Use of wireless connections is not recommended.
CR 4.2 - Information persistence	–	–
RE (1) Erase of shared memory resources	–	–
RE (2) Erase verification	–	–
CR 4.3 - Use of cryptography	✓	M1
FR 5 – Restricted data flow (RDF) - Chapter 9		
CR 5.1 - Network segmentation	✓	M7
NDR 5.2 Zone boundary protection	✓	M7
RE (1) Deny all, permit by exception	–	–
RE (2) Island mode	–	–
RE (3) Fail close	–	–

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)
NDR 5.3 - General purpose, person-to-person communication restrictions	✓	M7
5.4 Application partitioning	–	**There is no component level requirement associated with IEC 62443-3-3 SR 5.4**
FR 6 – Timely response to events (TRE) - Chapter 10		
CR 6.1 - Audit log accessibility	✓	M1
RE (1) Programmatic access to audit logs	–	–
CR 6.2 - Continuous monitoring	–	–
FR 7 – Resource availability (RA) - Chapter 11		
CR 7.1 - Denial of service protection	✓	M1
RE(1) Manage communication load from component	–	–
CR 7.2 - Resource management	✓	Some tasks, such as LCP/bus tasks, have low priority, do not impact critical fast task execution.
CR 7.3 - Control system backup	✓	Use CSIV files, offsite project files. With M1, an LCP can be used as a system configuration backup.
RE (1) Backup integrity verification	–	–
CR 7.4 - Control system recovery and reconstitution	✓	Drive init with the CSIV files, offsite project files. With M1, an LCP can be used as a system configuration backup.
CR 7.5 - Emergency power	–	–
CR 7.6 - Network and security configuration settings	✓	M4, M6
RE (1) Machine-readable reporting of current security settings	–	–
CR 7.7 - Least functionality	✓	M1, M2
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

In the DNV document, section 21: Cybersecurity, 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)

For the Danfoss Premium frequency converters, the highest IEC 62443-4-2 security level is defined as SL-1.

This is related to the DNV SP1 and will be the focus on identifying extended requirements.

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.

Since SL-1 is defined as Danfoss Premium Frequency Converter level, only *H* marked parts of the table in DNV document section 21 chapter 4.2 Identification and authentication will be addressed.

6.3 DNV July/2023 Extended Requirements Mitigation List

Table 6: DNV July/2023 Extended Requirements Mitigation List

DNV rules for classification ships edition July/2023 extended requirements (*H*)	IEC SL1[1]	DNV SP1	Mitigation at system level recommended DNV
Section 4.2.2 User identification and authentication of human users			
See IEC-62443-3-3 SR 1.1 RE2 Multifactor authentication is required for human users when accessing the system from or via an untrusted network.	✓	YES^{H}	M6
Section 4.2.3 Identification and authentication of software and devices			
See IEC-62443-3-3 SR 1.2 Identification and authentication of devices and software processes shall be implemented on interfaces providing access to the system Amendments: • For SP0 and SP1, this applies for communication with or via untrusted networks.	–	YES^{H}	M5, M6
Section 4.2.14 Access via untrusted networks			

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

DNV rules for classification ships edition July/2023 extended requirements (*H*)	IEC SL1[1]	DNV SP1	Mitigation at system level recommended DNV
See IEC-62443-3-3 SR 1.13 RE1 The system shall deny access from or via untrusted networks if the request is not approved by authorized personnel on board Amendments: • see also Pt. 4 Ch.9 Sec 4. [3.1.14].	–	YES^H	M5, M6
Section 4.3.7 Remote session termination			
See IEC-62443-3-3 SR 2.6 The system shall automatically terminate a remote session from/via untrusted network after a configurable time of inactivity, or by manual termination by a responsible crew member. The effect of terminating a remote session during ongoing operation shall be considered and not endanger the vessel or crew.	–	YES^H	M3, M5, M6
Section 4.3.12 Timestamp			
See IEC-62443-3-3 SR 2.11 The system shall timestamp each audit record.	✓	YES^H	Set date and time and use the VLT® Real-Time Clock MCB 117 or date and time be updated regularly (after each power cycle at least).Timestamp to be used on system level.
Section 4.4.2 Communication integrity			
See IEC-62443-3-3 SR 3.1 RE1 The system shall apply cryptographic algorithms to protect the integrity of transmitted information. Amendments: • For SP0 to SP2, this requirement applies for communication via untrusted networks and wireless networks.	–	YES^H	M4, M6
Section 4.4.9 Session integrity			
See IEC-62443-3-3 SR 3.8 The system shall protect the integrity of sessions. Invalid session IDs shall be rejected. Amendments: • For SP0 to SP2, this requirement applies for communication with or via untrusted networks.	–	YES^H	M6
See IEC-62443-3-3 SR 3.8 RE1 The system shall invalidate session IDs after logout or other session termination (Including browser sessions). Amendments: • For SP1 to SP2, this requirement applies for communication with or via untrusted networks.	–	YES^H	M6
Section 4.5.2 Information confidentiality			

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

DNV rules for classification ships edition July/2023 extended requirements (*H*)	IEC SL1[1]	DNV SP1	Mitigation at system level recommended DNV
See IEC-62443-3-3 SR 4.1 RE1 The system shall be able to protect the confidentiality of information at rest or in transit on untrusted networks Amendments: • For SP1 to SP2, this requirement applies for wireless networks.	–	YES[H]	M1, M4, M6
Section 4.6.2 Network segmentation			
See IEC-62443-3-3 SR 5.1 RE1 For requirements to physical network segmentation, see 4.6.1 General This subsection describes requirements for security zones and conduits. The following principles for the design of security zones apply: • OT systems and IT systems shall be physically segmented into different zones. • Navigational and radio communication systems shall be in a separate zone. • Systems providing required safety functions shall be in separate zone(s). • Wireless devices shall be grouped in zones separated from wired devices.	✓	YES[H]	M4, M6, M7
Section 4.6.3 Zone boundary protection			
See IEC-62443-3-3 SR 5.2 RE1 Communication traversing zone boundaries shall be controlled according to the principle of *deny by default, allow exceptions*.	–	YES[H]	This behavior cannot be controlled in the drive. It must be handled by other system components with valid protection functions.
See IEC-62443-3-3 SR 5.2 RE2 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"). Amendments: • Use of data diodes / Unidirectional communication may be accepted.	–	YES[H]	This behavior cannot be controlled in the drive. It must be handled by other system components with valid protection functions.

[1] *SL1: Protect the integrity of the IACS against casual or coincidental manipulation.*

7 Device Specifications

7.1 Overview

The Danfoss Premium frequency converter series consist of 3 main series:

HVAC : FC-102/FC-103, Power range 0.37 kW to 1.4 MW

AQUA : FC-202, Power range 0.37 kW to 1.4 MW

Automation : FC-301/FC-302, Power range 0.25 kW to 1.2 MW

The frame sizes range A-B-C-D-E-F can be delivered in IP20, IP21, IP54, IP55, and IP66

In all drives, a firmware is downloaded during production to operate the functions in the drive. Due to the different use of the drives HVAC, AQUA, or Automation, each series has its own firmware version.

For each series, the firmware version is the same in all power sizes.

Operating, changing settings, or updating firmware to the drive can be done by different methods: LCP (local control panel), commissioning software (VLT® Motion Control Tool MCT 10) or via different fieldbus options.

The interface layout is the same independently of the size of the drive:

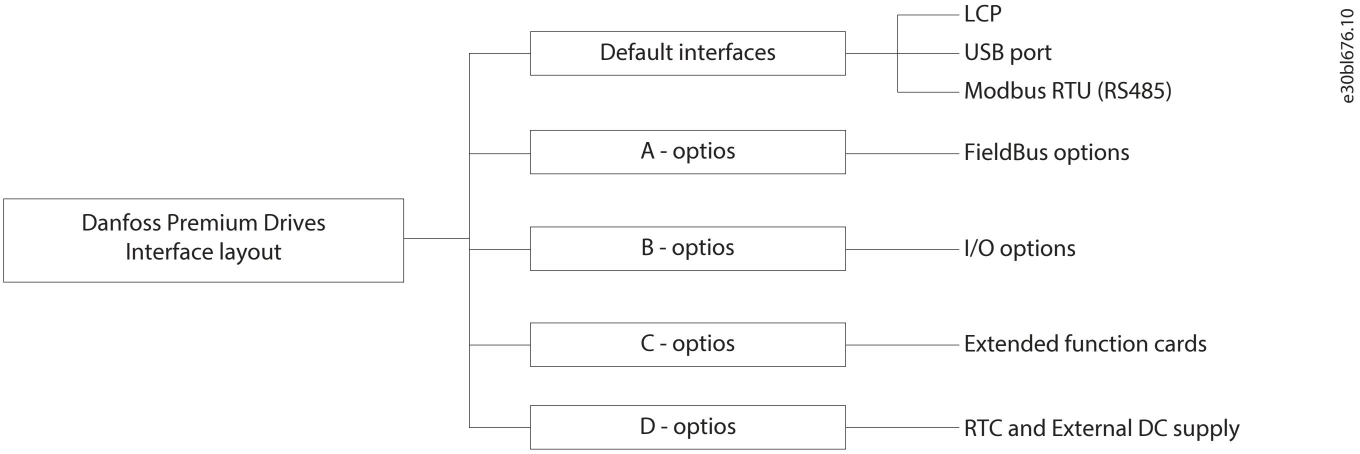


Figure 1: Danfoss Premium Drives Interface Layout

7.2 Default interfaces

7.2.1 LCP

7.2.1.1 Overview

Local Control Panel. It is possible to connect three types of 3 panels:

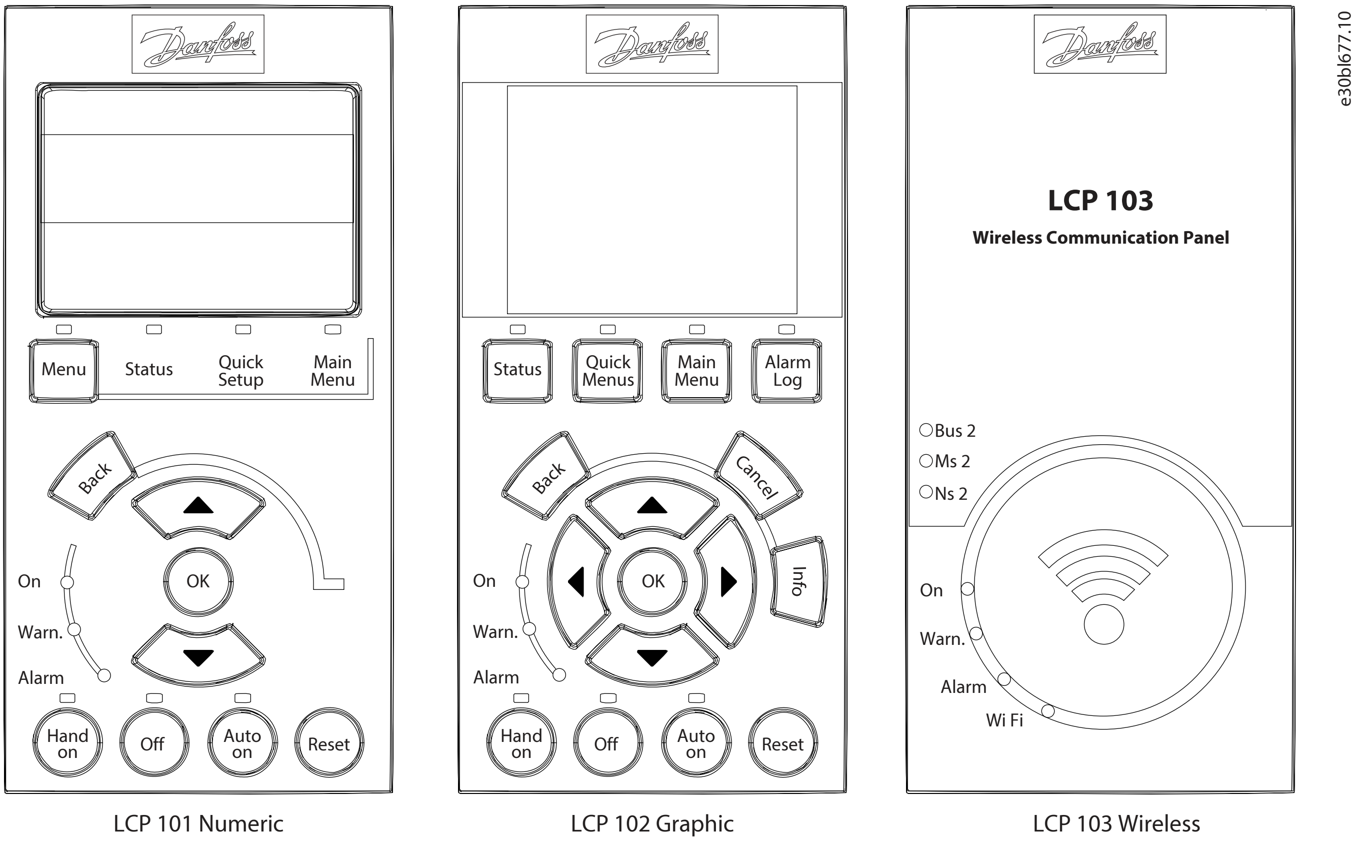


Figure 2: Local Control Panel (LCP) Type

The LCP 101/102 allow local operating and parameterizing of the drive.

The LCP 103 requires the app MyDrive® Connect – an app which can be downloaded to iOS- and android-based smart devices.

All the LPCs are removable from the drive. The LCP is used on all drives sizes across series.

It is possible to activate password protection with different options:

ID	Name
060	Main Menu Password
061	Access to Main Menu w/o Password
065	Quick Menu Password
066	Access to Quick Menu w/o Password
067	Bus Password Access

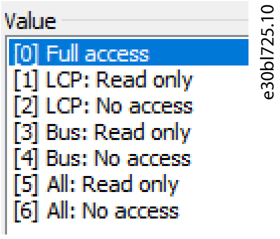
7.2.1.2 **ID 060 Main menu Password**

Define the password for access to the Main Menu via the [*Main Menu*] key. If ***parameter 0-61 Access to Main Menu w/o Password*** is set to *[0] Full access*, this parameter is ignored.

Password range: -9999 to 9999

7.2.1.3 ID 061 Access to Main Menu w/o Password

Select *[0] Full access* to disable the password defined in ***parameter 0-60 Main Menu Password***. Select *[1] Read only* to avoid unauthorized editing of Main Menu parameters. Select *[2] No access* to avoid unauthorized viewing and editing of Main Menu parameters. Below a list of all options can be found.



Value

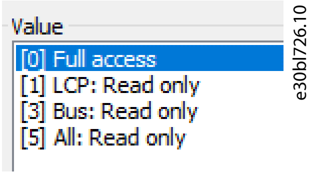
[0] Full access
[1] LCP: Read only
[2] LCP: No access
[3] Bus: Read only
[4] Bus: No access
[5] All: Read only
[6] All: No access

7.2.1.4 ID 065 Quick Menu Password

Define the password for access to the Quick Menu via the *[Quick Menu]* key. If ***parameter 0-66 Access to Quick Menu w/o Password*** is set to *[0] Full access*, this parameter is ignored.

7.2.1.5 ID 066 Access to Quick Menu w/o Password

Select *[0] Full access* to disable the password defined in ***parameter 0-65 Quick Menu Password***. Select *[1] Read only* to avoid unauthorized editing of Quick Menu parameters.



Value

[0] Full access
[1] LCP: Read only
[3] Bus: Read only
[5] All: Read only

7.2.1.6 ID 067 Bus Password Access

To unlock the drive remotely, enter the password defined in ***parameter 0-60 Main Menu Password***.

The different remote channels which allow to unlock:

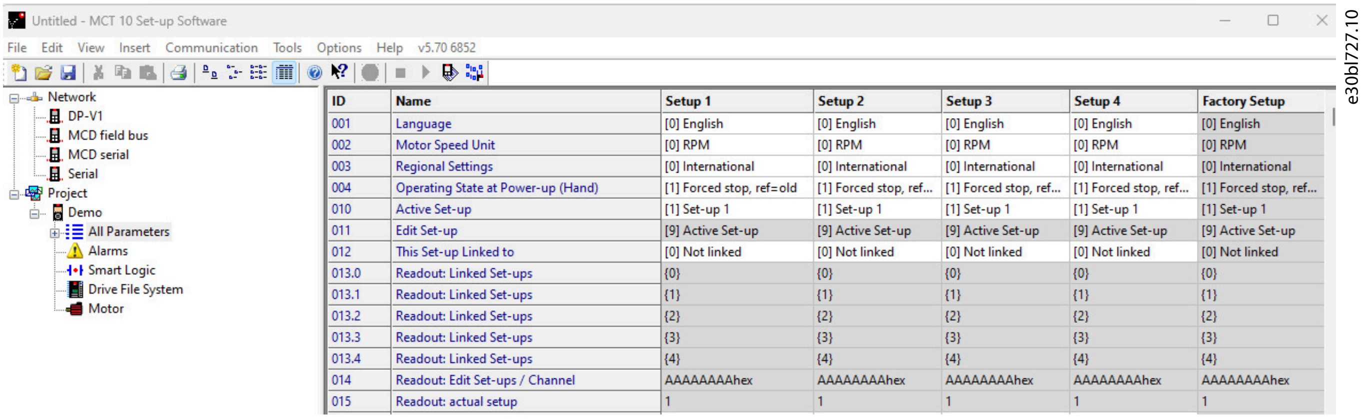
- VLT® Motion Control Tool MCT 10 via the USB port
- Modbus RTU (RS85)
- Fieldbus (A-option)

When a valid password is entered, this unlocks the drive for 30 minutes.

When unlocked, access is possible via the above mentioned remote connections and the local LCP.

7.2.2 USB Port

This port is used for connecting the VLT® Motion Control Tool MCT 10 Configuration Software.



ID	Name	Setup 1	Setup 2	Setup 3	Setup 4	Factory Setup
001	Language	[0] English	[0] English	[0] English	[0] English	[0] English
002	Motor Speed Unit	[0] RPM	[0] RPM	[0] RPM	[0] RPM	[0] RPM
003	Regional Settings	[0] International	[0] International	[0] International	[0] International	[0] International
004	Operating State at Power-up (Hand)	[1] Forced stop, ref=old	[1] Forced stop, ref...	[1] Forced stop, ref...	[1] Forced stop, ref...	[1] Forced stop, ref...
010	Active Set-up	[1] Set-up 1	[1] Set-up 1	[1] Set-up 1	[1] Set-up 1	[1] Set-up 1
011	Edit Set-up	[9] Active Set-up	[9] Active Set-up	[9] Active Set-up	[9] Active Set-up	[9] Active Set-up
012	This Set-up Linked to	[0] Not linked	[0] Not linked	[0] Not linked	[0] Not linked	[0] Not linked
013.0	Readout: Linked Set-ups	{0}	{0}	{0}	{0}	{0}
013.1	Readout: Linked Set-ups	{1}	{1}	{1}	{1}	{1}
013.2	Readout: Linked Set-ups	{2}	{2}	{2}	{2}	{2}
013.3	Readout: Linked Set-ups	{3}	{3}	{3}	{3}	{3}
013.4	Readout: Linked Set-ups	{4}	{4}	{4}	{4}	{4}
014	Readout: Edit Set-ups / Channel	AAAAAAAAhex	AAAAAAAAhex	AAAAAAAAhex	AAAAAAAAhex	AAAAAAAAhex
015	Readout: actual setup	1	1	1	1	1

To use the VLT® Motion Control Tool MCT 10, application must be installed on a PC with the minimum system requirements:

- 4 GB of available space on the hard drive.
- MCT 10 runs on Windows™ 10 32/64-bit edition.

Connection to the drive can be controlled by ***parameter ID 67 Buss Password Access*** as mentioned above.

7.2.3 Modbus RTU (RS485)

The Modbus RTU protocol is based on the built-in RS485 (EIA-485) interface on the FC Drive series control card. RS485 is a 2 wire bus interface that allows multi-drop network topology, that is, nodes can be connected as a bus (daisy chain), or via drop cables from a common trunk line. Danfoss uses the two-wire system where the communication between master and follower is half duplex, that is, it cannot transmit and receive at the same time. Connection terminals 68-69 are as shown in Figure 3.

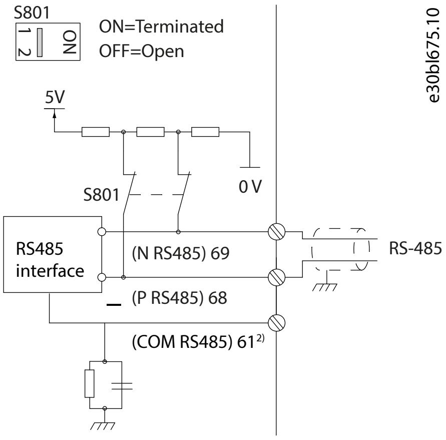


Figure 3: Connection terminals 68-69

One or more frequency converters can be connected to a control (or master) using the RS485 standardized interface.

Terminal 68 is connected to the P signal (TX+, RX+), while terminal 69 is connected to the N signal (TX-, RX-). If more than one frequency converter is connected to a master, use parallel connections. In Figure 4, a configuration is shown which can be used for commissioning more FC drives using the VLT® Motion Control Tool MCT 10 Software.

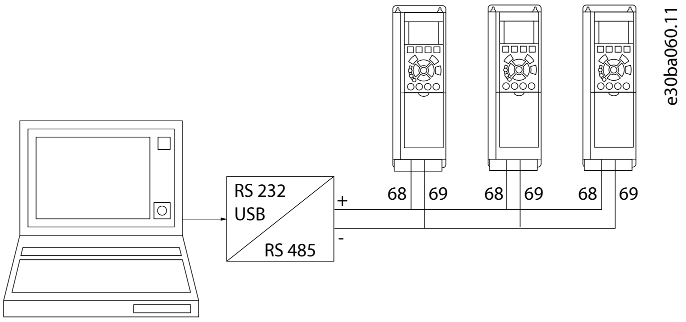


Figure 4: RS485 Application Connected to 3 FC-Drives

Since the interface is open, consult recommendations to achieve security level SL-1 in section 8.2.1 Local Access and 8.2.2 Remote Access.

7.2.4 ABCD-options

7.2.4.1 VLT® FC Series Options Concept

Options are used to add extra features to the drive. That allows tailoring the drive to the specific need and application.

The drives have 4 option slots (A, B, C, and D).

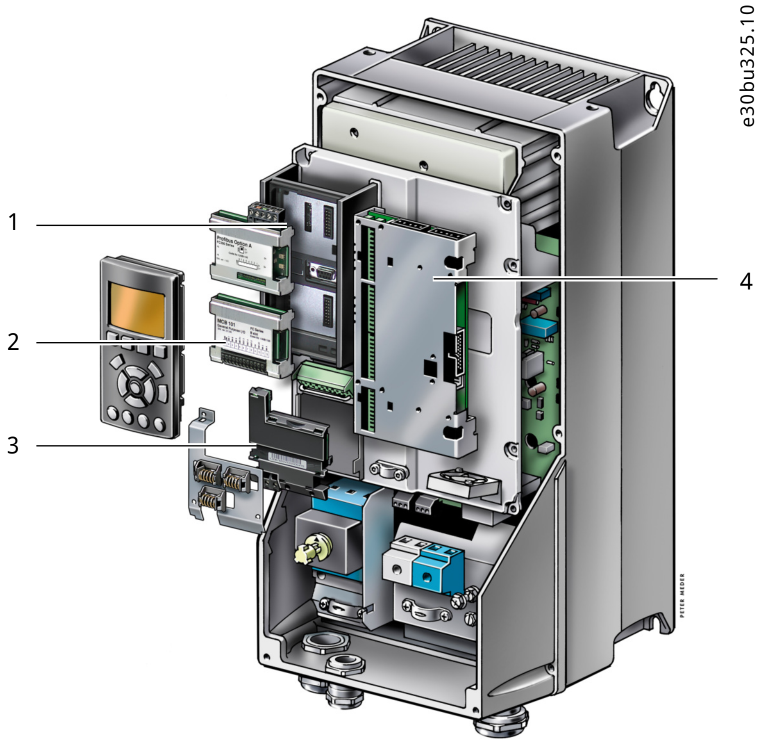


Figure 5: Option Slots on a VLT® FC Series Drive (Example Compact Enclosure)

1	A option	**2**	B option
3	D option	**4**	C option

Interface	Functions to be installed
A-option	VLT® Fieldbus Options (See 7.2.4.2 A-option)
B-option	VLT® Functional Extensions: I/O extensions, Encoder signals and more.
C-option	VLT® Functional Extensions: Programmable function cards (See 7.2.4.4.1 C-option)
D-option	VLT® 24 V DC External supply and Real Time Clock (RTC)

7.2.4.2 A-option

For the Danfoss Drives products a number of fieldbus options can be installed:

Table 7: A-option

Option name	Type[1]	Slot	FC 102	FC 103	FC 202	FC 301	FC 302	Maximum SL level
VLT® PROFIBUS DP MCA 101	S	A	X	X	X	X	X	SL-1
VLT® DeviceNet MCA 104	S	A	X	–	X	X	X	SL-1
VLT® CANopen MCA 105	S	A	–	–	–	X	X	SL-1
VLT® AK-LonWorks MCA 107 for ADAP kool®	S	A	–	X	–	–	–	SL-1
VLT® LonWorks MCA 108	S	A	X	–	–	–	–	SL-1
VLT® BACNet MCA 109	S	A	X	X	–	–	–	SL-1
VLT® PROFIBUS Converter MCA 113 (VLT® 3000 to VLT® FC302)	S	A	–	–	–	–	X	SL-1
VLT® PROFIBUS Converter MCA 114 (VLT® 5000 to VLT® FC302)	S	A	–	–	–	–	X	SL-1
VLT® PROFINET MCA 120	E	A	X	X	X	–	X	SL-1
VLT® Ether Net/IP MCA 121	E	A	X	–	X	X	X	SL-1
VLT® Modbus TCP MCA 122	E	A	X	–	X	–	X	SL-1
VLT® POWERLINK MCA 123	E	A	–	–	–	–	X	SL-1
VLT® Ether Net/IP MCA 124	E	A	–	–	–	–	X	SL-1
VLT® BACNet/IP MCA 125	E	A	X	–	–	–	–	SL-1
VLT® Device Net Converter MCA 194	S	A	–	–	–	–	X	SL-1

[1] *S: Serial, E: Ethernet*

For all of the above communication cards, access to the drive can be controlled by the ***parameter 0-67 Bus Password Access***.

For recommendations to achieve security level SL-1, see section 8.2.1 Local Access and 8.2.2 Remote Access.

7.2.4.3 B-option

These options have no communication exchange. The channel is used for digital signals either from I/O extensions or encoder signals for motor or position control.

7.2.4.4 C-option

7.2.4.4.1 C-option

For the FC-drives a number of cards which can extend the functionality of the drive:

Table 8: C-option

Option name		FC 102	FC 103	FC 202	FC 301	FC 302
VLT® Extended Cascade Controller MCO 101	B	–	–	X	–	–
VLT® Advanced Cascade Controller MCO 102	C	–	–	X	–	–
VLT® Motion Control Option MCO 305	C	–	–	–	X	X
VLT® Synchronizing Controller MCO 350	C	–	–	–	–	X
VLT® position Controller MCO 351	C	–	–	–	–	X

7.2.4.4.2 MCO 101 and MCO 102

The MCO 101 and MCO 102 are controlled from parameters in the firmware. They have digital I/O signals and relays to control motors:

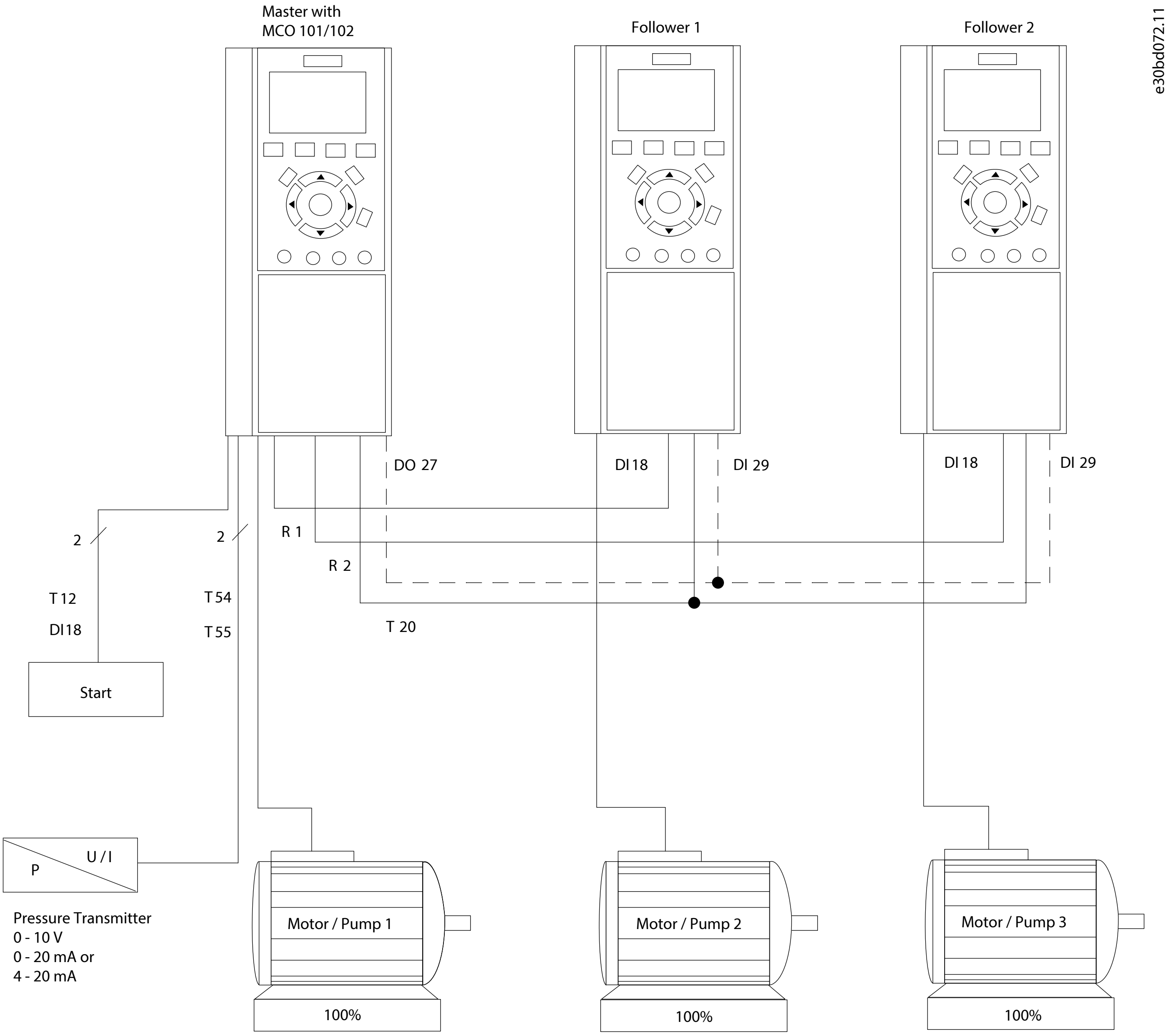


Figure 6: MCO 101/102 Cascade Controllers

7.2.4.4.3 **MCO 305, 350, and 351**

For programming the MCO 305, 350, and 351 the VLT® Motion Control Tool MCT 10 is used. The APOSS programming function used to program the extended functions is an integrated part of the MCT 10 Software.

Projects can be programmed offline or by means of Networking online.

- Online: When MCT 10 has a connection established to the drive, APOSS uses the drive connection that MCT 10 has already established.
- Offline: All the features that allow to switch drives, connect to multiple drives, or to read current parameters are enabled.

When APOSS is started by MCT 10, then APOSS connects to only a single drive. Hence, all the features that allow APOSS to switch drives or connect to multiple drives are disabled.

7.2.4.5 **D-option**

The D-options have no communication exchange.

Possible functionality to add is a 24 V DC external supply and Real Time Clock (RTC)

8 Security Configuration Guidelines

8.1 Introduction to Recommendations

There are different possibilities to prevent access to local or remote, to change settings, and to view data or settings in the FC-drive. From the below described principles, it is up to the system integrator to decide which principles give 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 fulfill SL-1.

The Danfoss FC-Product

Depending on the drives frame size and protection class, different methods (IP20, IP21, IP54, IP55, IP66) can be used. IP20 is to be installed in an enclosure. IP21, IP54, IP55, and IP66 are intended to be mounted on a wall or standing on the floor inside or outside of buildings.

The easier access to the Drive, the more protection is needed to ensure a security level.

8.1 Introduction to Recommendations and Figure 8 are examples of IP20 and IP55/IP66 drives.

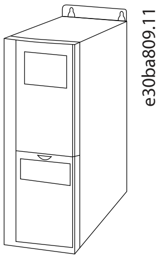


Figure 7: FC-Drive: IP20

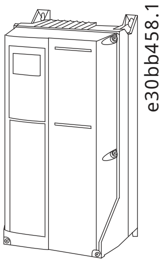


Figure 8: FC-Drive: IP55

8.2 Recommendations for Drives in Protection Class IP20

8.2.1 Local Access

Protection methods

- The FC-drives of protection class IP20 are intended for installation in a lockable enclosure or room. The lock for the enclosure/room must provide sufficient protection against access by unauthorized persons.
- Removing the LCP from the FC-drives under normal operation. If unintended access should happen, removing the LCP will prevent access to the drive, for example, 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.
- Make the access control active by selecting ***Parameter 0-61 Access to Main Menu w/o Password*** to ***[6] all: No access***. To change settings, the password must be entered. For controlling access via the fieldbus options, set ***Parameter 0-66 Access to Quick Menu w/o Password*** to ***[5] All: read only***. This will also prevent access via USB and Modbus RTU (RS485). The owner of the installation is responsible for protecting the password and if needed, change it during suspicion of the password being compromised.
- Entering the correct password in ***Parameter 0-67 Bus Password Access*** will also open up for local access. To prevent access, remove the LCP from the drive, even if it is installed in locked environments, to prevent local access in case of remote operation.
- As WiFi access to components is often seen as a threat for industrial installations, Danfoss recommends not to use the LCP 103 as described earlier.

8.2.2 Remote Access

The remote access can be made via an A-options or Modbus RTU (RS485). Usually, the control system has access control and will compensate for having the main password activated for normal operation.

Due to the design method of the FC-drive password, when not having the main password activated the possibility to prevent local access on the bus cannot be prevented. Since the option is between *all no access*, *LCP no access* or *bus no access*. It is recommended to select the read-only option or have an opening sequence programmed from the control system changing the possibilities depending on the situation.

Password A	Password B	Function / Password request		
Parameter 0-61	Parameter 0-66	Main Menu	Quick Menu	
Access to Main Menu w/o password	Access to Quick Menu w/o password	All Parameters	My Personal Menu	All others
Full access	Full access	Full access	Full access	Full access
Full access	Read only	Full access	Full access	Full access
Read only	Full access	Read only / A	Full access	Full access
Read only	Read only	Read only / A	Read only / A or B	Read only / A or B
No access	Full access	No access / A	Full access	Not Available
No access	Read only	No access / A	Read only / A or B	Not Available

These recommendations are still valid

- Make the access control active by selecting ***Parameter 0-61 Access to Main Menu w/o Password*** to ***[6] all: No access***. Enter a password for this installation. Also, set ***Parameter 0-66 Access to Quick Menu w/o Password*** to ***[5] All: read only***. The owner of the installation is responsible for protecting the password and if needed, change it during suspicion of the password being compromised.

- Entering the correct password in ***Parameter 0-67 Bus Password Access*** will also open up for local access. To prevent access by removing the LCP from the drive even if it is installed in locked environments, to prevent local access in case of remote operation.

Connection to Trusted/untrusted networks

- IEC 62433-3-3 mentioned in SR 1.13 – access via untrusted networks, that the control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks. Only connecting to trusted networks will ensure that the measure for access is under control. For the FC-drive, this will protect against unintentional access to fulfill security level SL-1. The local access to the drive interfaces like LPC, USB, or Modbus will fulfill the SL-1 by following the M1 mitigation list mentioned in section 5.3 Codes for Mitigation to be Achieved with Other Means.

8.3 Recommendations for Drives in Protection Class IP21/IP54/IP55/IP66

8.3.1 Local Access

The FC-drives of protection class IP55/66 are as IP20 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 prevention is not possible, the following prevention methods can be recommended:

- Removing the LCP from the FC-drives under normal operation. If unintended access should happen, removing the LCP will prevent access to, for example, 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.
- For having access to USB port and Modbus RTU (RS485), the front cover must be removed using tools. This will complicates access at certain levels but not fully prevent access. But for security level SL-1, this is seen as fulfilling the requirements.
- As WiFi access to components is often seen as a threat for industrial installations, Danfoss recommends not to use the LCP 103 as described earlier.

8.3.2 Remote Access

Same recommendations as for IP20 (See section 8.2.2 Remote Access)

8.4 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 FC 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:

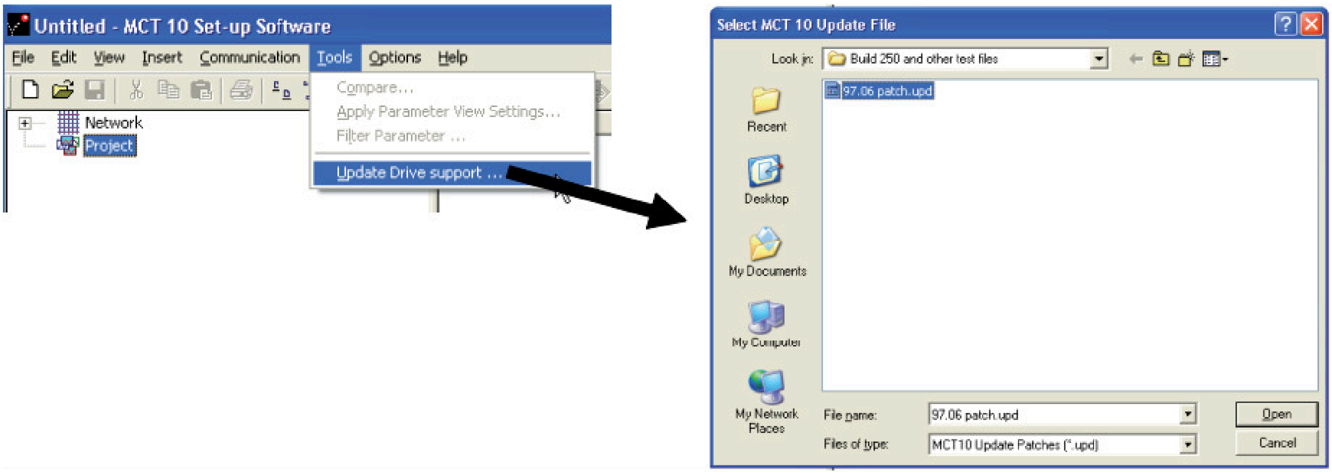
- Do not assign passwords that can be easily guessed, for example, simple number combinations like 1111 or 1234
- Assign, if possible, passwords with the required maximum length. This makes it more complicated to gain access unintentionally.

9 Software and Firmware Updates

The FC-drives firmware can be updated by using the VLT® Motion Control Tool MCT 10 configuration software.

The MCT 10 software can be updated regardless of the firmware version of the The MCT 10 software.

The latest version can be downloaded from www.danfoss.com (direct link: AC drive firmware | Danfoss)



Look in: Build 250 and other test files

File name: 97.06 patch.upd

Files of type: MCT10 Update Patches (*.upd)

e30bl728.10

More detailed instructions on updating the firmware can be found in the VLT® Motion Control Tool MCT 10 applications *Help*.

10 Supplier Documentation

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

- The design guide provides specifications and information to be used when including the FC-drive in an application.
- The operating guide provides detailed information for the installation and start-up of the drive.
- The programming guide provides greater detail on how to work with parameters. It also contains application examples.
- The condition-based monitoring programming guide provides information on working with condition-based monitoring (CBM) parameters on the VLT® FC series AC drives.
- The safe torque off operating guide describes how to use Danfoss VLT® drives in functional safety applications. This manual is supplied with the drive when the safe torque off option is present.
- The VLT® Brake Resistor MCE 101 design guide describes how to select the optimal brake resistor.
- The VLT® Advanced Harmonic Filters AHF 005/AHF 010 design guide describes harmonics, various mitigation methods, and the operation principle of the advanced harmonic filter. This guide also describes how to select the correct advanced harmonics filter for a particular application.
- The Output Filter design guide explains why it is necessary to use output filters for certain applications and how to select the optimal dU/dt sine-wave filter, all-mode filters, and common mode filters.
- supplemental publications, drawings, EPLAN macros, and manuals are available at www.danfoss.com

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

Any information, including, but not limited to information on selection of product, its application or use, product design, weight, dimensions, capacity or any other technical data in product manuals, catalog descriptions, advertisements, etc. and whether made available in writing, orally, electronically, online or via download, shall be considered informative, and is only binding if and to the extent, explicit reference is made in a quotation or order confirmation. Danfoss cannot accept any responsibility for possible errors in catalogs, brochures, videos and other material. Danfoss reserves the right to alter its products without notice. This also applies to products ordered but not delivered provided that such alterations can be made without changes to form, fit or function of the product. All trademarks in this material are property of Danfoss A/S or Danfoss group companies. Danfoss and the Danfoss logo are trademarks of Danfoss A/S. All rights reserved.