User Guide

Cybersecurity for Danfoss Drives

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

Explore our solutions
drives.danfoss.com

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 is able to support the security level intended for different parts/zones in the system.

Frequency converters (also called drives or VFD) are considered as a component in the entire cybersecurity system. Drives in scope for this document: FC 102, FC 103, FC 202, FC 301, FC 302, and FCD 302, in this document referred to as FC drives.

As product supplier, Danfoss FC drives drives are certified to be used in the system based on:

- IEC 62443-4-1: Secure development and production of the components.
- IEC 62443-4-2: Description of the product and certified security level, 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 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.

Danfoss FC drives in scope are certified to SL-1.

Recommendations to implement systems on higher security levels can be found in the section: Chapter 8 Security Configuration Guidelines.

A list for the IEC62443-4-2 Mitigation plan can be found in Chapter 5 Security Mitigation Plan IEC 62443-4-2.

1.2 Terms and Abbreviations

AOC – Application Oriented Controller: software component that is responsible for user interface, I/O handling, data storage, and event management.

Bootloader – a small program placed at the MCU boot memory of the drive. The bootloader contains instructions on how to prepare memory for main program execution, and it performs the 1st security checks before the follow-up application is executed.

CC – a control card of the Danfoss VLT® Series Frequency Converter units. A printed circuit board that houses the microcontroller units for AOC and MOC, external flash, and memory chips and pin connectors for I/O, power supply, and connectivity with the rest of the drive.

Drive – Danfoss VLT® Series Frequency Converter unit, consisting of 1 or more power card(s) and control card, and any other mounted terminals or additional hardware options and accessories.

DTM – Danfoss Test Monitor: dedicated application installed during the production process to test and calibrate the hardware and is later used for firmware updates. Also referred to as “boot mode monitor” or “test monitor”.

EDU – Enhanced Drive Updater feature for updating the communication options via Ethernet.

Firmware – application software in the form of a binary flash image. The firmware usually contains software for both AOC and MOC, but could additionally include update images for other components or applications like DTM, options and LCPs. Firmware update package is bundled up inside an encoded OSE file, containing one or more binary images to flash, instructions how to verify the intended target and how to apply the update.

Hash – A fixed size binary value obtained as an output from cryptographic operation of a given input. Hashes are called secure if they are one directional: knowing the output does not help constructing the input value, yet same input always returns same output. Hashes are used in digital signatures, message authentication, and in ensuring data integrity and authenticity.

LCP – Local Control Panel: a terminal unit connected to the RS-485 port. The LCP is mounted directly on the device or via cable to the wall next to the drive. Used for human-user interaction and monitoring.

MOC – Motor Oriented Controller: software component that is dedicated to direct motor control, digital signal processing, and filtering.

SCF – Security Configuration File: a binary security file describing access control rules for Danfoss VLT® series frequency converters, defining all the user accounts, each account access privileges, and contains password hashes for those accounts.

PIN – Personal Identification Number, usually a 4-digit, or longer, secret number that the user makes up or is assigned to. PIN both identifies and authenticates any person in a system who knows the number.

PLC – Programmable Logic Controller is an industrial computer that has been ruggedized and adapted for the control of manufacturing processes. The PLC uses built-in ports, such as USB, Ethernet, RS-232, RS-485, or RS-422 to communicate with external devices (sensors, actuators) and systems (SCADA, user interface, engineer workstations).

PUD – Power Unit Data is a collection of data that lists the frequency converter output’s minimum, maximum, and nominal currents and voltages, temperature limits for transducers, fan speeds, and other data that is hardware and device specific. It varies depending on the supported output power and supply voltage range.

1.3 Extended Requirements

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

In this document, a list of issuers with extended requirements can be found in Chapter 6 Extended Requirements.

1.4 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
BC529529075529, document version 01	Preliminary release	x.x.x

2 Safety

2.1 Safety Precautions

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

3 Security Measures

Incorporating security measures to address potential misuse or tampering with the product functionality.

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 certified with TüV on maturity level 3.
- The technical requirements for secure components are implemented and certified by TüV for security level 1.
- Analyze functions 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 related 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, the 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 cybersecurity.

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.

4.3 Security Context

Danfoss FC series drives can be used as a low-level embedded device in an industrial automation control system, operating at the process control level or as a standalone all-in-one application providing all the same capabilities of a system from data acquisition, process, and supervisory control in a household or small-business settings. Balancing the targeted security level, confidentiality, availability and integrity requirements against usability, ease of maintenance and scalability of the security countermeasures will always remain a challenge for these kinds of devices. The similar inherited shortcomings plague the standardized communication protocols used in the field. The proposed approach from Danfoss is not to force hard security controls by default but to provide a flexible approach defining different access control rules, means to monitor them and only essential cybersecurity functions, focusing on risks that cannot be mitigated easily outside of the device.

Security in Danfoss FC drives is anchored to 3 cornerstones to fulfill the Security Level 1 requirements raised by the IEC/ISA 62443-4-2 standard:

1. Authentic software received from Danfoss
2. Customizable access control rules in the form of Security Configuration File (SCF) to fulfill the mitigation plan set by asset owner's risk assessment.
3. In-device integrity check of the installed firmware and device configuration.

Details of each anchor:

Software authenticity

Danfoss shares software updates and releases through authorized service partners. FC Series drives are unable to verify any Danfoss digital signatures on software release packages. If those packages are going to be signed in the future, the signature verification must happen outside of the device using common IT tools capable of handling public key certificates. The same applies also for the PC tools used to update and commission the FC drives in the field. PC tools can only verify the compatibility between the hardware and firmware but not the authenticity of the software.

Be vary of any e-mail attachments, links to cloud storage, or mass storage device claiming to contain an official firmware release or latest security patch to the VLT® drives. If in doubt, contact the claimed sender, your Danfoss service contact, or customer representative to confirm the authenticity of the firmware package.

Access control rules described in the security Configuration File

The security configuration file (SCF) contains access rules and passwords to access the FC drive. The user can specify a number of roles and associate appropriate rights and passwords to each role. The SCF itself does not contain any secrets like encryption keys, default passwords, certificates, or credentials.

Access rules are applied to human-user interfaces (LCP and connected PC-SW tools) and limit the access/visibility of the parameters and restrict what actions a given user can take. There are no built-in user roles (like "admin" or root) in the software. A user role is defined in SCF through the access right given. For different applications, configuration and installed environments having a non-fixed role description provides flexibility and versatility to meet the access control requirements of any complex system and its risk assessment.

Parameter access can be described for a single parameter, for a range of parameters or for an entire interface (called *paramDefaultAccess*) limiting the access to *Read-Only*, providing *No Access* or full access by allowing *Read and Write*.

Having few and straightforward access rules for defined accounts, especially for anonymous user accounts (user accounts that do not require authentication), improves the performance of the drive.

Device integrity

FC series drives can detect changes in firmware that are caused by malicious code, physical damage, or wear that can happen during the lifetime of a device either in storage or in active use. The integrity of the application firmware can be checked before every execution Chapter 11 General Parameter Setup.

Once configured, the integrity check of the flashed firmware happens at an early stage. The bootloader calculates the hash value of application code and compares against a pre-stored value. If those values match, the normal application execution continues. If the integrity check fails, it is indicated with an LED flashing pattern on the drive.

NOTICE

If the integrity check failed during booting into DTM, the CC must be replaced as it can be recovered only in lab condition.

Table 2: Flashing pattern of Control Card LEDs and their Meaning

Flashing pattern of control card LEDs	Meaning
Cycling LEDs: GREEN -> YELLOW -> RED	Integrity check is currently in progress, as firmware integrity validation is enabled. The integrity check typically takes 2–3 s for the AOC, but it may appear to be skipped when booting into the DTM because the application size is much smaller.
Flashing RED LED	Integrity check has failed. The firmware has been changed without updating the stored hash value or the stored hash value is missing (legacy software case). A power cycle is needed to start the recovery process (execute DTM).
RED, YELLOW, and GREEN LEDs flash at the same time.	The drive is in the DTM mode, meaning that normal communication and control over fieldbus or via LCP is not possible. Communication with a drive can be established via serial line.

Table 2: Flashing pattern of Control Card LEDs and their Meaning - (continued)

Flashing pattern of control card LEDs	Meaning
Flashing GREEN LED with high duty cycle.	MOC firmware is being updated (normal execution routine after software update). The drive is past the boot time integrity check and should execute as normally.
RED and YELLOW LEDs flash at the same time.	Other unspecified internal error when initializing integrity hash calculation.

4.4 Security Limitations and Known Vulnerabilities

Every security control has its own limitations and inherit vulnerabilities that must be understood and if needed mitigated on a system level with additional countermeasures or policies.

Limitation of security configuration file (SCF)

Access control, user authentication, and user management are all AOC features and are achieved with the correct usage and configuration of the SCF. Security configuration itself is a binary file that can be created with a separate PC tool (Security Admin tool). The input for the Security Admin tool is a YML formatted configuration file describing the user accounts, user passwords, and user permissions, and access to parameters user can read or write. The security admin tool will also validate the YML configuration for any formatting error or conflicts before creating the binary security file that can be uploaded to the device.

NOTICE

The specific user: Security Configuration (YML file) containing user passwords in plain text should be stored and handled as confidential information that, if exposed, could compromise system security.

Without the SCF there are no access restrictions to parameter access, the audit, and parameter logs are creating a trace as normally, the drive is also capable to perform the boot-time integrity check but enabling or disabling this check can be disabled by anyone.

Some parameters that are needed to identify the device are always visible regardless of the settings described in SCF. The complete list of these parameters can be found in chapter 12.2 Parameters with Exception in Access Control.

Missing security controls in test monitor

NOTICE

A drive in boot mode (running DTM) has no security controls. All memory interfaces, including EEPROM and internal and external flash, storage content can be modified – erased, rewritten, or dumped. There are no security checks in DTM mode.

NOTICE

DTM supports connections only on the serial ports (USB, RS-232 (LCP port) or RS-485) using Danfoss proprietary protocol. Any of the hardware communication options are not supported in DTM mode.

Physical security

The FC drive is not protected against physical attacks. Actions that require close proximity and are executed only via LCP fall to the same physical security context. Performing factory reset or 3-finger reset to reset the drive parameter values to default, are not controlled by security configuration. These reset actions can be performed by anyone during a drive power-up sequence with the use of a mounted LCP.

Exceptions in parameter access rules

The existing and standardized fieldbus protocols do not have a concept of session handling and privilege escalation. Session control and access rules (in SCF) are built around the concept of a parameterized data model in the drive. This does not map well with some fieldbus protocols that use signals or objects instead. Security cannot be imported into existing industrial protocols or applied around them without breaking conformance to these communication protocols.

NOTICE

Parameter access rules DO NOT apply to fieldbus communication:

- Serial protocols (like PROFIBUS, Modbus, BACnet, DeviceNet, CANopen, and LonWorks)
- EtherNet-based protocols (like PROFINET, EtherCAT, EtherNet/IP, BACnet/IP, and Modbus TCP)

The concept of sessions is only for human users using either LCP or PC tools (using FC or FC/MC protocol). HMI devices and RTU (remote terminal units) are seen as a fieldbus device, like PLCs which do not support authentication or access control.

NOTICE

Protecting parameter access over Ethernet based fieldbus must be managed on the network level by configuring firewall access control lists and packet inspection.

EDU and other Ethernet services

All of the basic Ethernet services like FTP, SNMP, and HTTP server, can be enabled/disabled from parameters 1280–1289. The parameter ***12-89 Transparent Socket Channel Port*** controls both the Ethernet TSC and EDU features. When the parameter is set to value 0, both TSC and EDU are disabled. When the parameter is set to any non-zero value, the TSC feature remains active, while EDU is disabled, unless the default value 4000 is used.

NOTICE

When the FTP, HTTP, SMTP, and SNMP services are not required, keeping them enabled unnecessarily increases the network exposure of the drive. These services leave interfaces open, such as file transfer, the web interface for parameter commissioning, mail-related information, and device management data.

Limited security logging capacity

In case of a security or safety incident, logged information helps the investigation team to find out who did what and when. Due to hardware limitations, almost all logs (except service and parameter logs) in the drive are implemented in a circular buffer, meaning at some point, the oldest log entries are overwritten. Thus, it is important to monitor the logs and, in case of an incident, to copy the logs and store them in a persistent medium outside the device.

NOTICE

Last Changed Parameters, Firemode/Emergency mode has capacity for the last 10 entries.

Alarm/Warning log has capacity for the last 30 entries.

The audit log has capacity for the last 100 entries.

Service code activation is not tied to user session

Service codes are legacy features of firmware to activate some special features of an application that are normally not active. These features could be different modes of operation for example, boot mode, clearing logs or changing identification data stored in EEPROM (like type product label info). The aim is to assist debugging and testing or restoring the operational condition of the unit after warranty-affecting maintenance or spare part replacement.

There are 2 kinds of service codes:

- Permanent service codes which are in effect after restart.
- Temporary service codes which are cleared after resetting parameter ***14-29 Service Code*** or restarting the drive.

Temporary service codes are activated by entering a fixed numeric value in hex notation to parameter ***14-29 Service Code***. To deactivate the service code by performing a power cycle or entering an invalid and non-default value (default value being zero) like 1 to parameter ***14-29 Service Code***. Permanent service codes need both actions to activate/deactivate: setting the value of parameter ***14-29 Service Code*** and doing an additional power cycle.

NOTICE

The service codes are not bound to an active user session and are in effect even when the user session is terminated.

The service codes are grouped into 4 categories; each category requires a special named permission to active the code (see chapter 12.3 Special Named Permissions for User Accounts in SCF). Having write access to parameter ***14-29 Service Code*** does not automatically grant access to activate any service code, on the other hand, having a named policy grants write access even if specific write access to parameter ***14-29 Service Code*** is not given.

Here are the listed 3 of 4 groups of service codes, the 4th group is used by Danfoss internal testing.

Table 3: Service codes

Codes for end users	Codes for Danfoss service engineers	Codes covered by ALLOW.UPDATE_FIRMWARE
Requires policy SERVICECODES.USER	Requires policy SERVICECODES.DANFOSS_SERVICE	
• Demo Mode Activate[1] • Demo Mode Deactivate[1] • Change Serial Number • Change typecode • 3-finger reset via p.14-22 • Disable fan in 24 V mode • Select Profibus ident number • Blow fan • Custom fan control • Change typecode in CUE203 • Disable fan • Stop dependencies • Disturbance Rejection Control • Activate dependencies • Run fans in 24 V mode	• Reset Parameter log • Reset Fault Log • Firemode Reset Log	• Boot mode • Restart drive

[1] *Permanent service codes*

The exact service code values are not publicly listed.

5 Security Mitigation Plan IEC 62443-4-2

5.1 Overview

The following products are certified to IEC62443-4-2 SL-1: FC 102, FC 103, FC 202, FC 301, FC 302, FCD 302. In this section there are recommendations for mitigations to achieve higher security on system level.

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 4: 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 5: 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 protecting the drives in enclosures or rooms with access control. The enclosure or room can have access control by a 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 Chapter 10 Commissioning.
M2	**Remove the 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 LCP 103 is not recommended 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 and wireless connectivity.
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 engineering tools used.

Table 5: 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 strictly limited and well-monitored portion of a certain network or control system. For recommendations to achieve security level SL-1, see Chapter 10 Commissioning.
M7	**Use 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

IEC62443-4-2 FRs, CRs, and REs	SL1[1] Certification coverage	SL-2 Mitigation at system level	SL-3 Mitigation at system level	SL-4 Mitigation at system level
FR 1 - Identification and authentication control (IAC) - Chapter 5				
CR 1.1 - Human-user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication	–	M3	M3	M3
RE (2) Multifactor authentication for all interfaces	–	–	M3	M3
CR 1.2 -Software process and device identification and authentic action	–	X	–	–
RE (1) Unique identification and authentication	–	–	X	–
CR 1.3 - Account management	✓	✓	✓	✓
CR 1.4 - Identifier management	✓	✓	✓	✓
CR 1.5 - Authenticator management	✓	✓	✓	✓
RE (1) Hardware security for authenticators	–	–	X	–
NDR 1.6 Wireless access management	✓	M4 Support for wireless discontinued. Change the default password for WLCP (parameter***30-92 Password***) even if not used.	M4 Support for wireless discontinued. Change the default password for WLCP (parameter***30-92 Password***) even if not used.	M4 Support for wireless discontinued. Change the default password for WLCP (parameter***30-92 Password***) even if not used.
RE (1) Unique identification and authentication	–	X	–	–
CR 1.7 - Strength of password-based authentication	✓	✓	✓	✓
RE (1) Password generation and lifetime restrictions for human users	–	–	X	–

IEC62443-4-2 FRs, CRs, and REs	SL1[1] Certification coverage	SL-2 Mitigation at system level	SL-3 Mitigation at system level	SL-4 Mitigation at system level
RE (2) Password lifetime restrictions for all users (human, software process, or device)	–	–	–	X
CR 1.8 - Public key infrastructure certificates	–	X	–	–
CR 1.9 - Strength of public key-based authentication	–	X	–	–
RE (1) Hardware security for public key-based authentication	–	–	X	–
CR 1.10 - Authenticator feedback	✓	✓	✓	✓
CR 1.11 - Unsuccessful login attempts	✓	✓	✓	✓
CR 1.12 - System use notification	✓	✓	✓	✓
NDR 1.13 - Access via untrusted networks	✓	M6	M6	M6
RE (1) Explicit access request approval	–	–	X	–
CR 1.14 - Strength of symmetric key-based authentication	–	X	–	–
RE (1) Hardware security for symmetric key-based authentication	–	–	X	–
FR 2 - Use control (UC) - Chapter 6				
CR 2.1 Authorization enforcement	✓	✓	✓	✓
RE (1) Authorization enforcement for all users (humans, software processes, and devices)	–	X	–	–
RE (2) Permission mapping to roles	–	✓	–	–
RE (3) Supervisor override	–	–	✓	–
RE (4) Dual approval	–	–	–	X
CR 2.2 -Wireless use control	M4 Support for wireless discontinued. Change the default password for WLCP (parameter*30-92 Password*) even if not used.	M4 Support for wireless discontinued. Change the default password for WLCP (parameter*30-92 Password*) even if not used.	M4 Support for wireless discontinued. Change the default password for WLCP (parameter*30-92 Password*) even if not used.	M4 Support for wireless discontinued. Change the default password for WLCP (parameter*30-92 Password*) even if not used.
CR 2.3 - Use control for portable and mobile devices	✓	The product does not use mobile code.	The product does not use mobile code.	The product does not use mobile code.
EDR 2.4 Mobile code	✓	The product does not use mobile code.	The product does not use mobile code.	The product does not use mobile code.
RE (1) Mobile code authenticity check	–	X	–	–

IEC62443-4-2 FRs, CRs, and REs	SL1[(1)] Certification coverage	SL-2 Mitigation at system level	SL-3 Mitigation at system level	SL-4 Mitigation at system level
CR 2.5 Session lock	✓	✓	✓	✓
CR 2.6 Remote session termination	–	✓	–	–
CR 2.7 Concurrent session control	–	–	✓	–
CR 2.8 Auditable events	✓	✓	✓	✓
CR 2.9 - Audit storage capacity	✓	✓	✓	✓
RE (1) Warn when audit record storage capacity threshold reached	–	–	X	–
CR 2.10 - Response to audit processing failures	✓	✓	✓	✓
CR 2.11 - Timestamps	✓	✓	✓	✓
RE (1) Time synchronization	–	X	–	–
RE (2) Protection of time source integrity	–	–	–	X
CR 2.12 - Non-repudiation	✓	✓	✓	✓
RE (1) Non-repudiation for all users	–	–	–	X
EDR 2.13 Use of physical diagnostic and test interfaces	–	X	–	–
RE (1) Active monitoring	–	–	X	–
FR 3 – System integrity (SI) - Chapter 7				
CR 3.1 - Communication integrity	✓	✓	✓	✓
RE (1) Communication authentication	–	X	–	–
EDR 3.2 Protection from malicious code	✓	✓	✓	✓
CR 3.3 - Security functionality verification	✓	✓	✓	✓
RE (1) Security functionality verification during normal operation	–	–	–	X
CR 3.4 - Software and information integrity	✓	✓	✓	✓
RE (1) Authenticity of software and information	–	X	–	–
RE (2) Automated notification of integrity violations	–	–	X	–
CR 3.5 - Input validation	✓	✓	✓	✓
CR 3.6 - Deterministic output	✓	✓	✓	✓
CR 3.7 - Error handling	✓	✓	✓	✓
CR 3.8 - Session integrity	–	X	–	–
CR 3.9 - Protection of audit information	–	X	–	–

IEC62443-4-2 FRs, CRs, and REs	SL1(1) Certification coverage	SL-2 Mitigation at system level	SL-3 Mitigation at system level	SL-4 Mitigation at system level
RE (1) Audit records on write-once media	–	–	–	X
EDR 3.10 Support for updates	✓	✓	✓	✓
RE (1) Update authenticity and integrity	–	X	–	–
EDR 3.11 - Physical tamper resistance and detection	–	X	–	–
RE (1) Notification of a tampering attempt	–	–	X	–
EDR 3.12 - Provisioning product supplier roots of trust	–	X	–	–
EDR 3.13 - Provisioning asset owner roots of trust	–	X	–	–
EDR 3.14 Integrity of the boot process	✓	✓	✓	✓
RE (1) Authenticity of the boot process	–	X	–	–
FR 4 – Data confidentiality (DC) - Chapter 8				
CR 4.1 - Information confidentiality	✓	✓	✓	✓
CR 4.2 - Information persistence	–	X	–	–
RE (1) Erase of shared memory resources	–	–	X	–
RE (2) Erase verification	–	–	X	–
CR 4.3 - Use of cryptography	✓	✓	✓	✓
FR 5 – Restricted data flow (RDF) - Chapter 9				
CR 5.1 - Network segmentation	✓	✓	✓	✓
NDR 5.2 Zone boundary protection	–	–	–	–
RE (1) Deny all, permit by exception	–	X	–	–
RE (2) Island mode	–	–	X	–
RE (3) Fail close	–	–	X	–
NDR 5.3 - General purpose, person-to-person communication restrictions	–	–	–	–
FR 6 – Timely response to events (TRE) - Chapter 10				
CR 6.1 - Audit log accessibility	✓	✓	✓	✓
RE (1) Programmatic access to audit logs	–	–	X	–
CR 6.2 - Continuous monitoring	–	X	–	–
FR 7 – Resource availability (RA) - Chapter 11				

IEC62443-4-2 FRs, CRs, and REs	SL1[1] Certification coverage	SL-2 Mitigation at system level	SL-3 Mitigation at system level	SL-4 Mitigation at system level
CR 7.1 - Denial of service protection	✓	✓	✓	✓
RE(1) Manage communication load from component	–	X	–	–
CR 7.2 - Resource management	✓	✓	✓	✓
CR 7.3 - Control system backup	✓	✓	✓	✓
RE (1) Backup integrity verification	–	X	–	–
CR 7.4 - Control system recovery and reconstitution	✓	✓	✓	✓
CR 7.5 - Emergency power	–	–	–	–
CR 7.6 - Network and security configuration settings	✓	✓	✓	✓
RE (1) Machine-readable reporting of current security settings	–	–	X	–
CR 7.7 - Least functionality	✓	✓	✓	✓
CR 7.8 - Control system component inventory	–	X	–	–

[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 be 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:

- 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.
- 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.
- 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/FCD 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, 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:

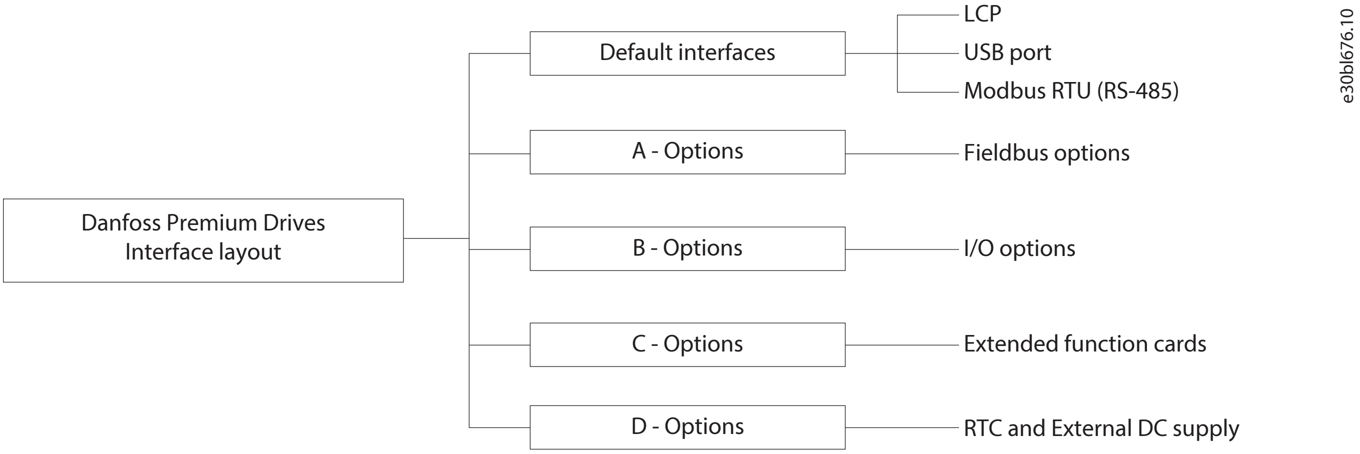


Figure 1: Danfoss Premium Drives Interface Layout

7.2 Default interfaces

7.2.1 LCP

7.2.1.1 Overview

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

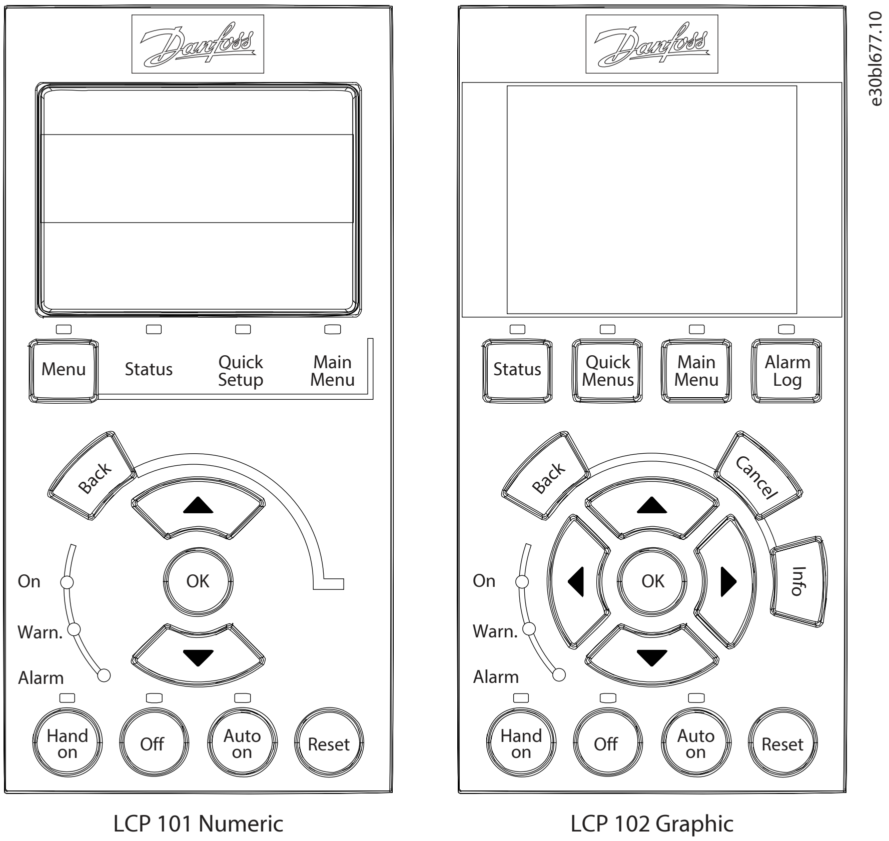


Figure 2: Local Control Panel (LCP) Type

The LCPs 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.

NOTICE

LCP 103 is under phase out and no longer sold from Danfoss and hence not part of cybersecurity certification.

All the LCPs are removable from the drive. The LCP is used on all drive 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

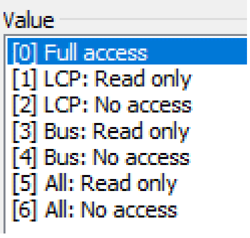
7.2.1.2 ID 060 Main menu Password

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. A list of all options can be found below.



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

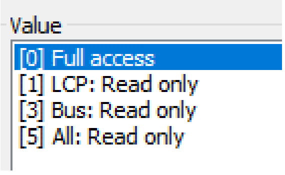
e30bl725.10

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

e30bl726.10

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:

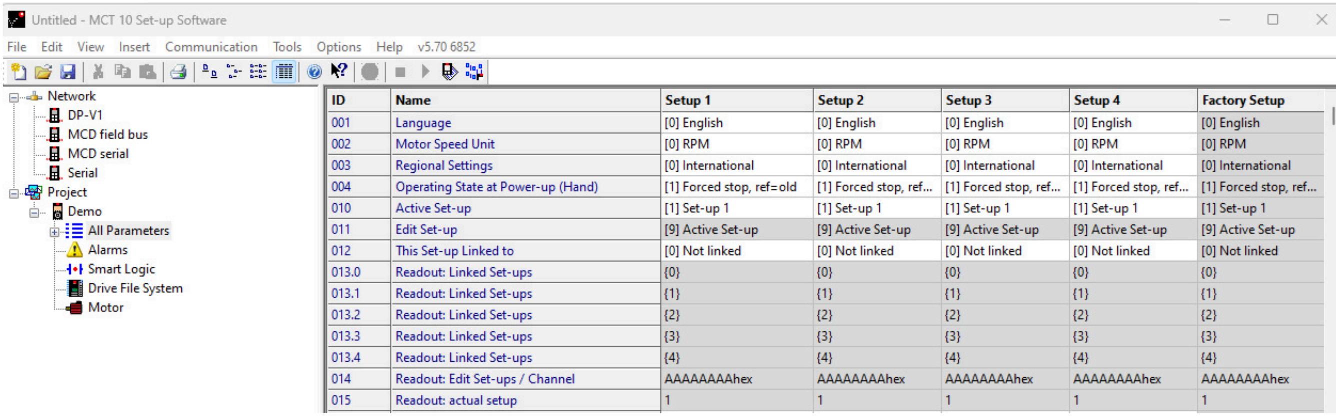
- VLT® Motion Control Tool MCT 10 via the USB port
- Modbus RTU (RS-485)
- Fieldbus (A-option)

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

e30bl727.10

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

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

Connection to the drive can be controlled by parameter ***0-67 Buss Password Access*** as mentioned above.

7.2.3 Modbus RTU (RS-485)

The Modbus RTU protocol is based on the built-in RS-485 (EIA-485) interface on the FC Drive series control card. RS-485 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 2-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.

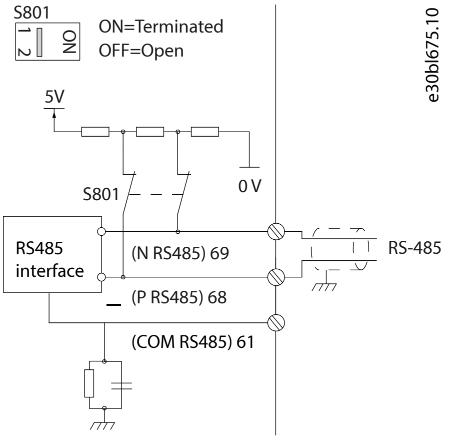


Figure 3: Connection Terminals 68–69

One or more frequency converters can be connected to a control (or master) using the RS-485 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 1 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.

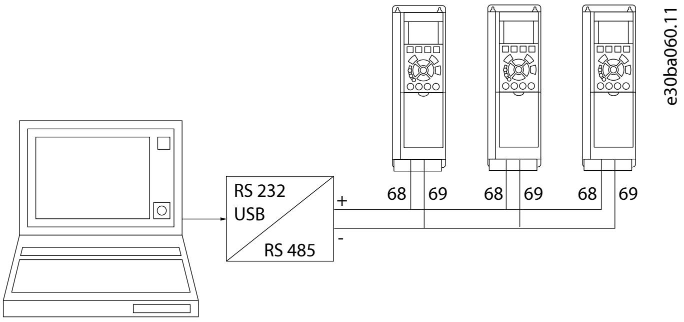


Figure 4: RS-485 Application Connected to 3 FC-Drives

Since the interface is open, consult recommendations to achieve security level SL-1 in section Chapter 8 Security Configuration Guidelines.

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).

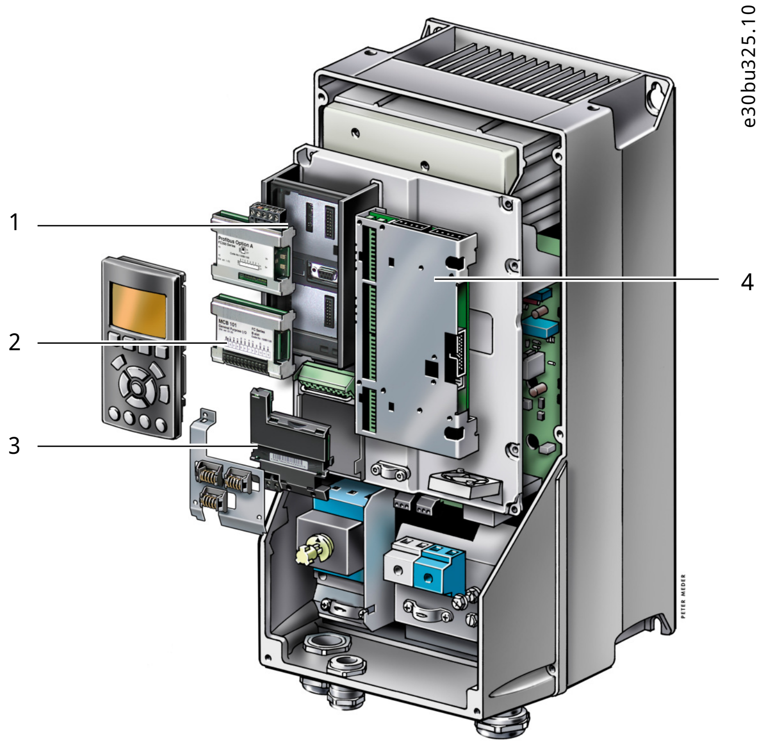


Figure 5: Option Slots on a VLT® FC Series Drive (Example Compact Enclosure)

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 Overview)
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	FCD 302	Maximum SL level
VLT® PROFIBUS DP MCA 101	S	A	X	X	X	X	X	X	SL-1
VLT® DeviceNet MCA 104	S	A	X	–	X	X	X	X	SL-1
VLT® CANopen MCA 105	S	A	–	–	–	X	X	X	SL-1
VLT® BACNet MCA 109	S	A	X	–	–	–	–	–	SL-1
VLT® PROFIBUS Converter MCA 113 (VLT® 3000 to VLT® FC302)	S	A	–	–	–	X	X	X	SL-1
VLT® PROFIBUS Converter MCA 114 (VLT® 5000 to VLT® FC302)	S	A	–	–	–	X	X	X	SL-1

Table 7: A-option - (continued)

Option name	Type[1]	Slot	FC 102	FC 103	FC 202	FC 301	FC 302	FCD 302	Maximum SL level
VLT® PROFINET MCA 120	E	A	X	X	X	X	X	X	SL-1
VLT® EtherNet/IP MCA 121	E	A	X	X	X	X	X	X	SL-1
VLT® Modbus TCP MCA 122	E	A	X	X	X	X	X	X	SL-1
VLT® EtherNet POWERLINK MCA 123	E	A	–	–	–	X	X	X	SL-1
VLT® EtherCAT MCA 124	E	A	–	–	–	X	X	X	SL-1
VLT® BACNet/IP MCA 125	E	A	X	–	X	–	–	–	SL-1
VLT® Devicenet Converter MCA 194	S	A	–	–	–	–	X	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 chapter 8 Security Configuration Guidelines.

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 Overview

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:

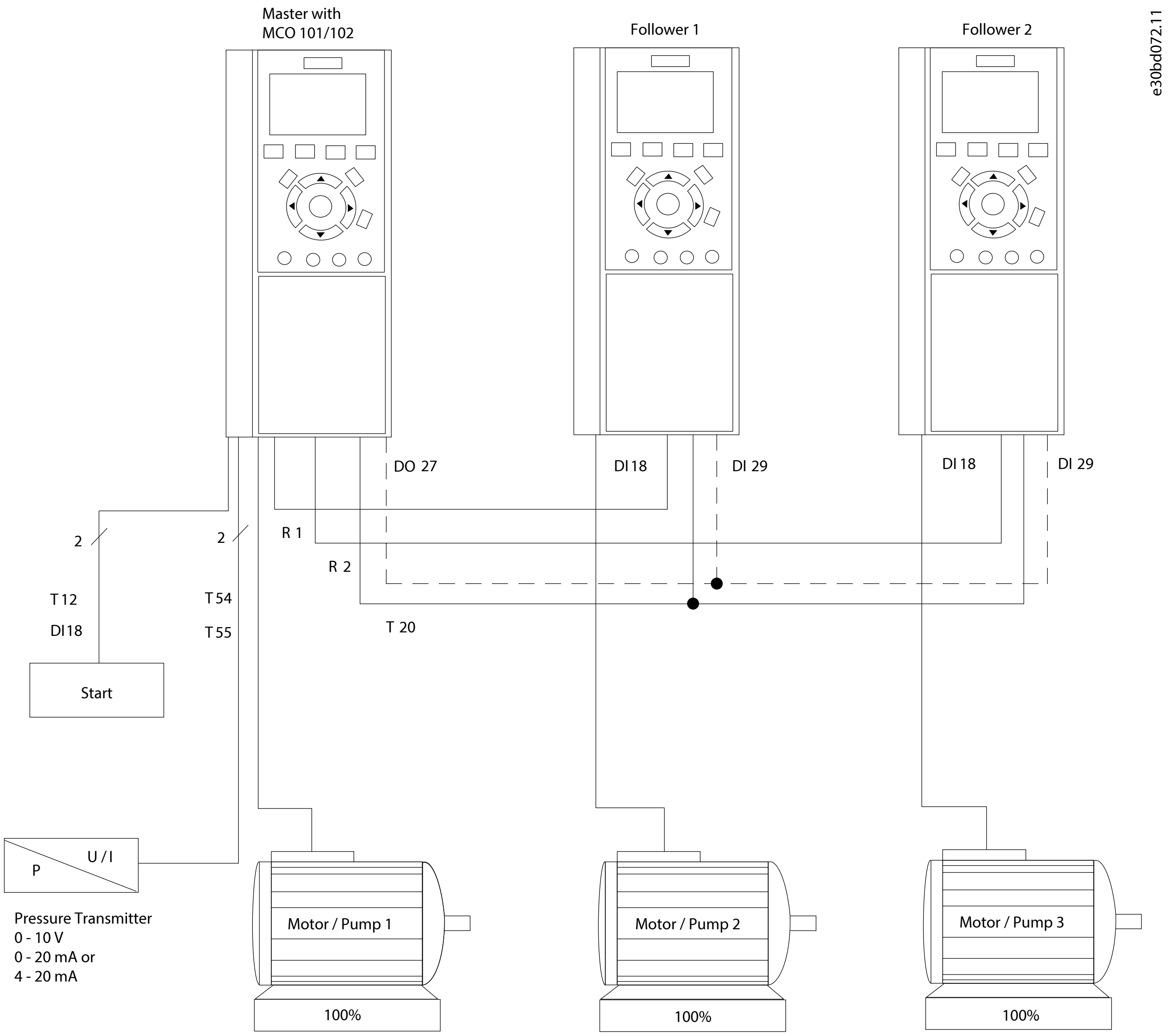


Figure 6: MCO 101/102 Cascade Controllers

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 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, 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 following described principles, the system integrator must 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 a locking mechanism where special tools, special keys, or access codes are needed for accessing. Only qualified personnel have the means to get access.

The Danfoss FC Product

Depending on the frame size of the drive 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 security.

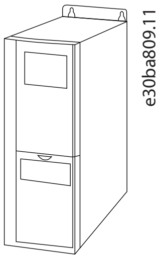


Figure 7: Example of an IP20 Drive

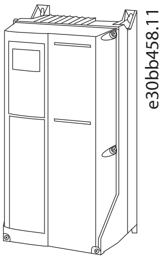


Figure 8: Example of an IP55/IP66 Drive

9 Installation

9.1 Limiting Attack Surface

Hardening the drives configuration (both connected hardware options and parameter settings) to limit attack surface: disable any services, inputs, outputs/relays, buttons, and ports that are not used.

Do not connect hardware options, cables, or jumper plugs for which the application need is not understood and documented. The system is expected to run the software version for the planned tasks, ensure only the necessary ports and connection points are open or accessible.

Make sure the labeled information on the physical hardware option matches with the information recognized by the drive. Use the recommended option software version from v8.xx.

When using the programmable motor control options (VLT® Motion Control options: MCO 305, MCO 302, or MCO 301) the loaded customer application must be verified before commissioning the device.

NOTICE

LCP is required to perform a factory reset (erasing the parameter settings and removing loaded SCF).

In case the unit is commissioned without the LCP, and privileged accounts' access credentials are lost or altered, the ownership can be re-established by mounting a graphical or numerical LCP and pressing and holding the factory reset key combination on the LCP during drive power-up (see Figure 19).

10 Commissioning

10.1 Pre-commissioning

Before configuring the device to achieve the targeted security level by ISA/IEC 62443, the OEM or system integrator must verify that the component at hand (the drive hardware and installed software) is SL1 capable. As different components of the device are released and updated at different times, multiple checks are needed to verify the devices capability security level. Table 9 contains a parameter list and their expected values.

NOTICE

If any of these parameters is missing (a parameter could be hidden for LCP or PC tools but readable over fieldbus) or the expected value is missing or wrong – the installed hardware or software does not meet the minimum requirements to be an SL1 capable device.

Table 9: Component Parameters and their Expected Values

Component	Parameter number	Expected readout value
Control Card HW is capable to support security certified firmware.	***15-98***	Drive ident string contains value; **K=2** at index values from 30 to 33. Example: F=1; D=FC-302; B=FC-302; L=FC-302; **K=2**; SC=1
Control Card firmware is capable to execute SL1 level features (like providing access control via SCF)	***15-98***	Drive ident string contains the value of; **SC=1**somewhere after index 33 Example: F=1; D=FC-202; B=FC-202; L=FC-202; K=2; UP=1; **SC=1**
Bootloader SW version	***15-94.3***	3.0 or newer
Testmonitor SW version	***15-94.4***	4.30 or newer (mark II CC) 5.30 or newer (mark II H7 CC)

10.2 Parameter Commissioning

The following parameters settings must be considered, and their settings adjusted according to the application's security needs. See Chapter 11 General Parameter Setup of this document and *the drive-specific operating guide* of the drive to learn more about the listed parameters and their choices.

Table 10: Parameters Settings and Security Recommendations

Parameter number	Factory default	Security recommendations
0-40 to ***0-45 LCP Keypad settings***	LCP keys are *[1] Enabled*	Set to *[0] Disabled* or to 1 of the selections that requires user authorization, for example, *[2] Password* or *[4] Hand On/Off with Password* or *[8] Password without OFF*
0-91 Integrity check at startup	*[0] No Check*	If delay in startup is acceptable, this parameter should be set to ***[1] After firmware update*** or ***[2] Always*** to check the integrity of the firmware after software update or after every startup.
0-93 Security Session Timeout	300 s	Set for how many seconds a session of a logged-in user is kept open after a period of inactivity.

Table 10: Parameters Settings and Security Recommendations - (continued)

Parameter number	Factory default	Security recommendations
0-94 Maximum Login Attempts	5 failed login attempts before interface is flagged as under "password-guessing" attack.	Set the allowed number of login attempts before applying rate-limit, thus blocking access to every user.
Group ***5-** Digital In/Out***	Some of the digital inputs are by default set to signal start, coast, jog, or reversing.	Always set digital inputs that are not in use to ***[0] No Operation***
Analog Input Live Zero Function parameters ***6-00*** to ***6-02***	Live Zero is enabled by default for all analog inputs, but the Live Zero function, and the delay for applying the function are not set by default.	Go over all the analog input terminals in use. Consider what is the required action when the signal is cut and for which terminals a Live Zero function should be enabled.
Control Word Timeout Parameters ***8-00*** to ***8-06***	Control Word Timeout is disabled by default. Drive will operate according to the last received control word.	Define the needed action and activation delay when control word is not received from a fieldbus device.
Parameter group ***12-8* Ethernet Services***	By default, FTP, HTTP, and SMTP services are disabled, but SNMP service is enabled and parameter ***12-89 Transparent Socket Channel Port*** default value controls both the Ethernet TSC and EDU features.	After commissioning is completed and PC tool access is no longer required, it is strongly recommended to disable all unused Ethernet services. Specifically, set Parameter ***12-89 Transparent Socket Channel Port*** to 0 to disable both TSC and EDU functionality.
14-89 Option Detection	Depending on application the default behavior is ***[0] Protect Option Configuration changes*** or ***[1] Enable Option Change***.	For secure environments, it is recommended to protect access to parameter ***14-89 Option Detection***and set the parameter value to ***[0]***.

10.3 PC Tool (MCT 10) Commissioning

10.3.1 PC Tool Installation

To commission cybersecurity products (drives), a corresponding/updated version of MCT 10 is required.

Install the following PC tools:

- MCT 10 (Recommended version: v.6.10 Build 7348 or later)
- SecurityAdminTool (Recommended version v. 1.0 or later)

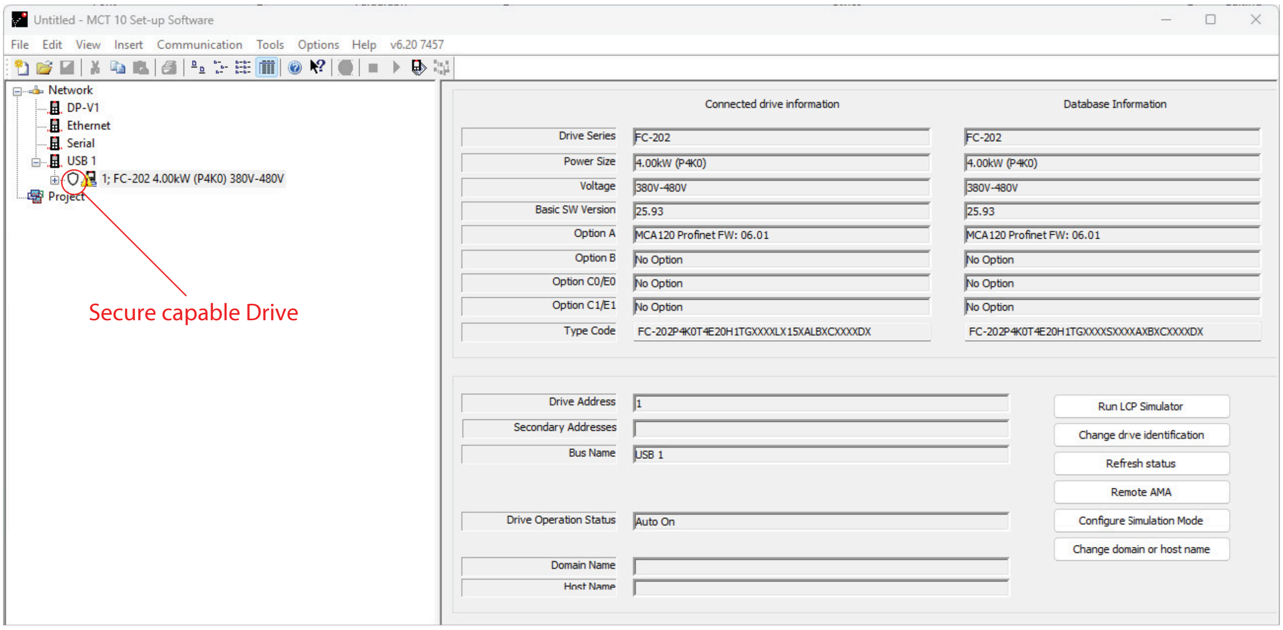
10.3.2 Security Configuration File (SCF) Handling

Basic steps:

1. Make or edit a security configuration file (SCF)
2. Download the SCF to the drive

How to:

Connect a drive to MCT 10 and verify that the drive is connected as *Secure Capable*.

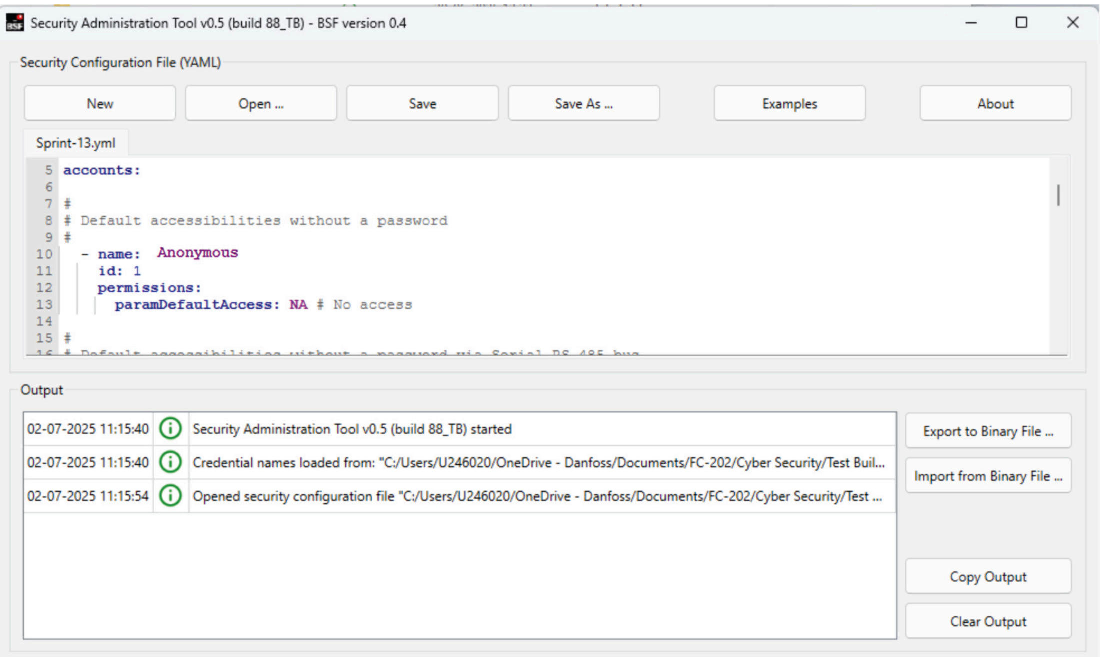

Untitled - MCT 10 Set-up Software
File Edit View Insert Communication Tools Options Help v6.20 7457
Network
DP-V1
Ethernet
Serial
USB 1
1; FC-202 4.00kW (P4K0) 380V-480V
Project
Secure capable Drive
Run LCP Simulator
Change drve identification
Refresh status
Remote AMA
Configure Simulation Mode
Change domain or host name
e30bm787.10

	Connected drive information	Database Information
Drive Series	FC-202	FC-202
Power Size	4.00kW (P4K0)	4.00kW (P4K0)
Voltage	380V-480V	380V-480V
Basic SW Version	25.93	25.93
Option A	MCA120 Profinet FW: 06.01	MCA120 Profinet FW: 06.01
Option B	No Option	No Option
Option C0/E0	No Option	No Option
Option C1/E1	No Option	No Option
Type Code	FC-202P4K0T4E20H1TGXXXXLX15XALBXCXXXXDX	FC-202P4K0T4E20H1TGXXXXSXXXXAXBXCXXXXDX

Drive Address	1
Secondary Addresses	
Bus Name	USB 1
Drive Operation Status	Auto On
Domain Name	
Host Name	

Figure 9: Drive is Connected as Secure Capable

Start the SecurityAdminTool.

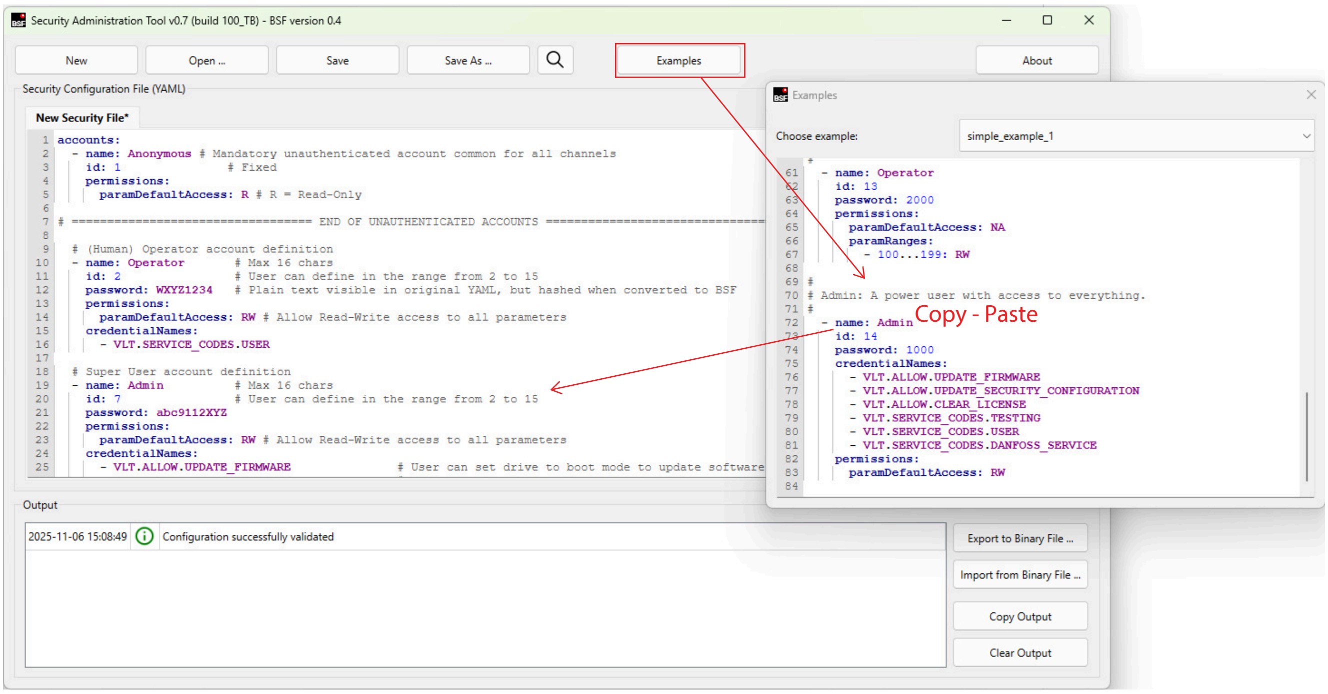

Security Administration Tool v0.5 (build 88_TB) - BSF version 0.4
Security Configuration File (YAML)
New
Open ...
Save
Save As ...
Examples
About
Sprint-13.yml
Output
Export to Binary File ...
Import from Binary File ...
Copy Output
Clear Output
e30bm788.10

```
accounts:

#
# Default accessibilities without a password
#
  - name:  Anonymous
    id: 1
    permissions:
      paramDefaultAccess: NA # No access

#
# Default accessibilities without a password via Serial RS-485 bus
```

```
02-07-2025 11:15:40  Security Administration Tool v0.5 (build 88_TB) started
02-07-2025 11:15:40  Credential names loaded from: "C:/Users/U246020/OneDrive - Danfoss/Documents/FC-202/Cyber Security/Test Buil...
02-07-2025 11:15:54  Opened security configuration file "C:/Users/U246020/OneDrive - Danfoss/Documents/FC-202/Cyber Security/Test ...
```

Figure 10: SecurityAdminTool

Make or open an SCF or copy-paste an existing one.



Security Administration Tool v0.7 (build 100_TB) - BSF version 0.4

```
accounts:
  - name: Anonymous # Mandatory unauthenticated account common for all channels
    id: 1              # Fixed
    permissions:
      paramDefaultAccess: R # R = Read-Only

# ================================== END OF UNAUTHENTICATED ACCOUNTS ==================================

  # (Human) Operator account definition
  - name: Operator        # Max 16 chars
    id: 2                 # User can define in the range from 2 to 15
    password: WXYZ1234    # Plain text visible in original YAML, but hashed when converted to BSF
    permissions:
      paramDefaultAccess: RW # Allow Read-Write access to all parameters
    credentialNames:
      - VLT.SERVICE_CODES.USER

  # Super User account definition
  - name: Admin           # Max 16 chars
    id: 7                 # User can define in the range from 2 to 15
    password: abc9112XYZ
    permissions:
      paramDefaultAccess: RW # Allow Read-Write access to all parameters
    credentialNames:
      - VLT.ALLOW.UPDATE_FIRMWARE              # User can set drive to boot mode to update software
```

Output

```
2025-11-06 15:08:49  Configuration successfully validated
```

Examples

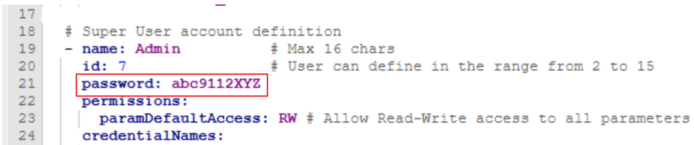
Choose example: simple_example_1

```
#
  - name: Operator
    id: 13
    password: 2000
    permissions:
      paramDefaultAccess: NA
      paramRanges:
        - 100...199: RW

#
# Admin: A power user with access to everything.
#
  - name: Admin
    id: 14
    password: 1000
    credentialNames:
      - VLT.ALLOW.UPDATE_FIRMWARE
      - VLT.ALLOW.UPDATE_SECURITY_CONFIGURATION
      - VLT.ALLOW.CLEAR_LICENSE
      - VLT.SERVICE_CODES.TESTING
      - VLT.SERVICE_CODES.USER
      - VLT.SERVICE_CODES.DANFOSS_SERVICE
    permissions:
      paramDefaultAccess: RW
```

e30bm789.10

Figure 11: Security Configuration File (SCF)

Change the password. Changing the password is mandatory/recommended if an example configuration is used.

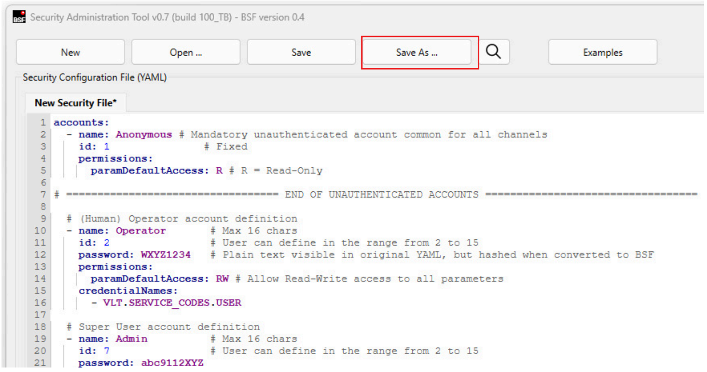


```
  # Super User account definition
  - name: Admin           # Max 16 chars
    id: 7                 # User can define in the range from 2 to 15
    password: abc9112XYZ
    permissions:
      paramDefaultAccess: RW # Allow Read-Write access to all parameters
    credentialNames:
```

e30bm790.10

Figure 12: Changing Password

Save the configuration file as .yml (optional).



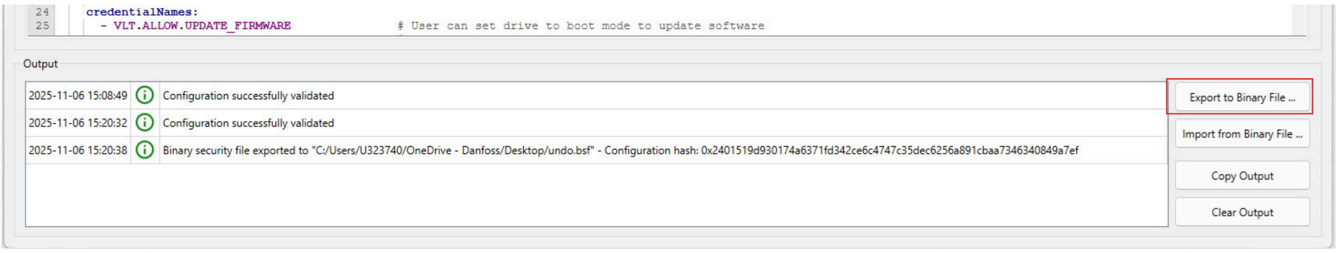
Security Administration Tool v0.7 (build 100_TB) - BSF version 0.4

```
accounts:
  - name: Anonymous # Mandatory unauthenticated account common for all channels
    id: 1              # Fixed
    permissions:
      paramDefaultAccess: R # R = Read-Only

# ================================== END OF UNAUTHENTICATED ACCOUNTS ==================================

  # (Human) Operator account definition
  - name: Operator        # Max 16 chars
    id: 2                 # User can define in the range from 2 to 15
    password: WXYZ1234    # Plain text visible in original YAML, but hashed when converted to BSF
    permissions:
      paramDefaultAccess: RW # Allow Read-Write access to all parameters
    credentialNames:
      - VLT.SERVICE_CODES.USER

  # Super User account definition
  - name: Admin           # Max 16 chars
    id: 7                 # User can define in the range from 2 to 15
    password: abc9112XYZ
```

e30bm791.10

Figure 13: Save as .yml

Save the configuration file as a binary (for writing to the drive).



```
    credentialNames:
      - VLT.ALLOW.UPDATE_FIRMWARE              # User can set drive to boot mode to update software
```

Output

```
2025-11-06 15:08:49  Configuration successfully validated
2025-11-06 15:20:32  Configuration successfully validated
2025-11-06 15:20:38  Binary security file exported to "C:/Users/U323740/OneDrive - Danfoss/Desktop/undo.bsf" - Configuration hash: 0x2401519d930174a6371fd342ce6c4747c35dec6256a891cbaa7346340849a7ef
```

e30bm792.10

Figure 14: Export as Binary

Write SCF to the drive.

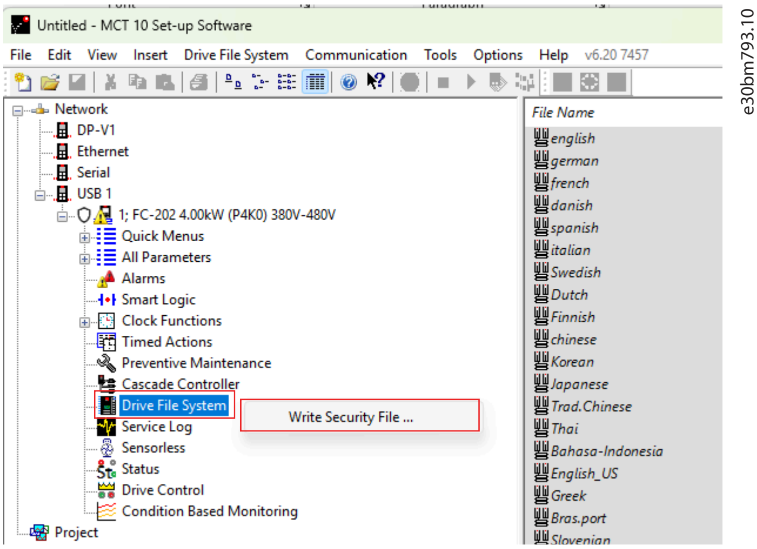
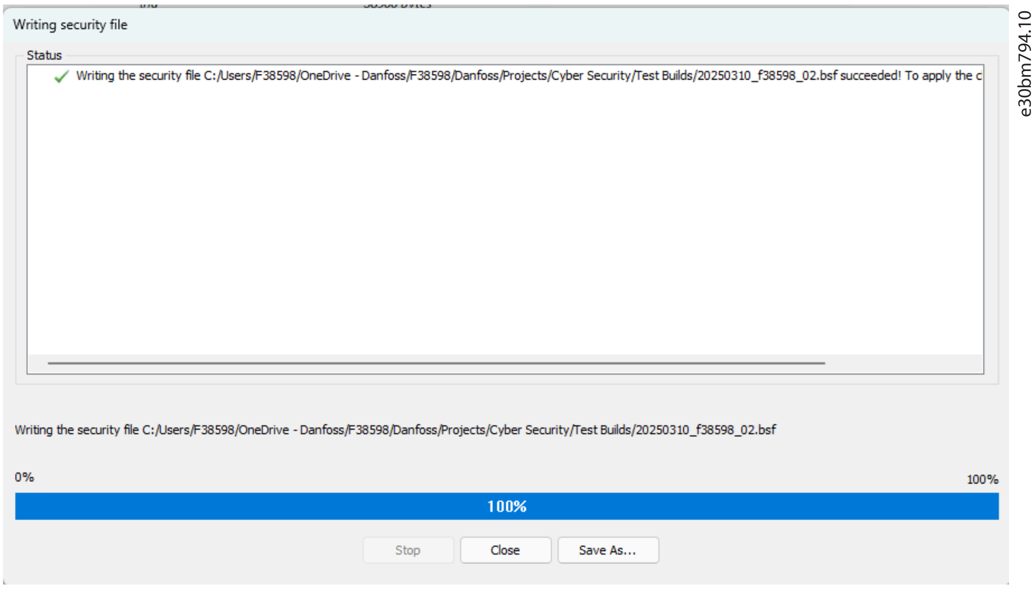


Figure 15: Write SCF to Drive

Select the SCF (.bsf extension) to download and write to the drive.


Writing security file

Status

✓ Writing the security file C:/Users/F38598/OneDrive - Danfoss/F38598/Danfoss/Projects/Cyber Security/Test Builds/20250310_f38598_02.bsf succeeded! To apply the c

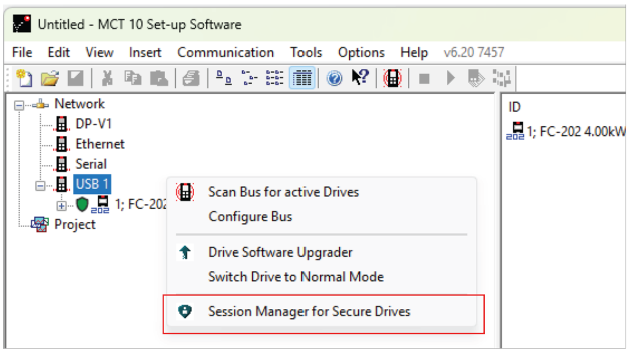
Writing the security file C:/Users/F38598/OneDrive - Danfoss/F38598/Danfoss/Projects/Cyber Security/Test Builds/20250310_f38598_02.bsf

Figure 16: Select the SCF

The drive will use this security configuration after a power cycle.

10.3.3 Session Handling

Open *Session Manager for Secure Drives* in MCT 10.


Untitled - MCT 10 Set-up Software
File Edit View Insert Communication Tools Options Help v6.20 7457
Network
DP-V1
Ethernet
Serial
USB 1
1; FC-202
Project
ID
1; FC-202 4.00kW
Scan Bus for active Drives
Configure Bus
Drive Software Upgrader
Switch Drive to Normal Mode
Session Manager for Secure Drives
e30bm795.10

10.4 Operation

10.4.1 Overview

User session management for the VLT® drives has some limitations that does not follow common IT approaches:

- **There can be only 1 active user session per physical access channel**: (LCP, USB, RS-485, Ethernet).
- If 1 user is authorized on a channel, all other human users using the same physical channel will share the session. If different access rights are required, terminate the active user session and start a new login procedure.
- **There are no privileged accounts:** every account (except anonymous accounts) can terminate an active user session with valid login credentials.

Anonymous account rights are not applied to every other account: depending on the SCF, it is possible that the user has more visibility and permissions as an anonymous user compared to as an authenticated user.

10.4.2 Security Status Monitoring

Enabling the start-up integrity check via parameter ***0-91 Integrity Check at Startup*** is not enough to ensure secure operations. Integrity check only confirms that the data has not been tampered with, lost, or degraded; it does not verify authenticity. If these integrity checks are not cryptographically signed, the human user must verify that the software versions, file names, and hash checksums match the expected values stored or calculated outside the drive.

In addition, there are encoded strings like device type code that can be used to monitor any changes in the hardware and software feature configuration that can be verified against documentation, backups, or product label information stored outside the drive.

Table 11: Components and Verification Steps

Component	Readout parameters *<readout formatting example>*	Verification steps
Control Card Firmware (both AOC and MOC)	**92.0** Firmware Checksum SHA256, for example, *"da323580f0994e794b768d…"*	Compare the value published by drive against the value published by Danfoss for the given software version.
	15-43 AOC Software version major.minor: for example, *"7.71"* **15-94.0** Product variant for example, "*FC302_IMC*" or "*FC202*" etc. **15-94.1** software platform version: major.minor.patch+<buildID> for example, *"24.5.60+4555874"* **15-94.2** MOC (DSP) version: major.minor.patch +<buildID>, for example, *"24.5.4+4555212"*	Reported metadata about the Firmware: (version major, minor, patch, build number) matches with the documented metadata from the last software up-date done during production or maintenance.
Ordered AOC Software Features	**15-44** Ordered Typecode String "*… N1M0T4E00P2TGC7XX**S009**XAXBX..*"	Compare the S-code or L-code value published by the drive match with the product label information.

Table 11: Components and Verification Steps - (continued)

Component	Readout parameters *<readout formatting example>*	Verification steps
Activated AOC Software Features and installed hardware options	**15-45** Actual Typecode String *"…E20H1TGXXXX**LX11XAXBXCXXXXDX**"*	Compare the end of the actual type code string against the last documented configuration of installed hardware options and licensed software features.
Power Card Firmware	**15-50** software ID Power Card: for example, *"SW:02.04 EE:04.81"* For high-power units that contain more than one inverter: **43-02.**[1]Component software ID, for example, *"SW:01.37 EE:04.99"*	Reported software version ("software:<major>.<minor>") and reported PUD version in EEPROM ("EE:<major>.<minor>") matches with the product label information or information documented during last maintenance.
Bootloader software version	**15-94.3** bootloader version: major.minor:, for example, *"3.0"*	Compare the values published by drive against the value published by Danfoss for the given software version.
DTM software version	**15-94.4** test monitor version: major.minor:, for example, *"4.30"* **92.3**Firmware Checksum SHA256, for example,*"a4257bbcd51d9f7dca9474…"*	Compare the values published by drive against the value published by Danfoss for the given software version.
Security Configuration File (SCF)	**15-54.4** Security Config Filename **92.1** Security Configuration Checksum (SHA256), for example,*"50c3aea338ff1266fe57…"*	Verify that the applied security file matches the documented or intended one by comparing the SCF filename and configuration hash against the intended file created by Security Admin.
Option Firmware	**1560.**[1] Option Mounted **1561.**[1] Option software Version	Verify that mounted option configurations and their software versions match with information on the options labels or with information documented during the last maintenance.
Drive File System	**15-54.0** Splash Screen Filename **15-54.1** SAS Wizard Filename **15-54.2** CSIV Filename **15-54.3** Envelope Filename **15-54.4** Security Config Filename	Verify that the drive filesystem does not contain any files not required for operation. Some files like translations and Smart Application Startup Wizard are contained within the firmware update package. Others (configuration files) are added post-production during or after commissioning (sensorless, SCF, CSIV and so on). The full list of files stored in *Drive File System* can be readout via PC-tool.

1) Parameters for Multiple options

10.4.3 Security Configuration Update Status Monitoring

If a user is authorized to update an SCF, the integrity of the uploaded file is checked before the file is approved. A drive power cycle is required to apply the new SCF (integrity check passed) or to clear the slot (if integrity check failed). When the SCF update process is done via remote interface, the status of the integrity check can be monitored by observing the parameter ***16-99 Extended Status Word 3*** bit 6 and bit 7 to plan the follow-up actions.

Bit 6 shows new Security Configuration File Integrity Check progress (0000 0040 hex) – "not done"/done.

Bit 7 shows new Security Configuration Integrity Check status (0000 0080 hex) – failed/passed.

Table 12: Extended Status Word 3 and Combined Bit Value Meanings

Extended status word 3		Combined bit value meanings
Bit 6	Bit 7	
0	0	There is no request to update the SCF. The drive has a free slot in flash to store a new SCF.
0	1	New SCF received. The integrity check for the SCF is in progress. When bit 6 goes to high state it is safe to do a power cycle to complete the SCF update process.
1	0	The integrity check for the received SCF is done however the integrity check failed meaning the file transferred was incomplete or file content was altered during file transfer. Power cycle the drive to try updating SCF again.
1	1	The integrity check for the received SCF is done with ”passed” result. Power cycle the drive to apply the new transferred SCF and remove the old file.

11 General Parameter Setup

11.1 Configuration

The Cybersecurity feature introduces the following new device parameters or choices.

0-50 LCP Copy

The LCP-based backup and restore process of the drive has new choices to make a local copy of the security settings (both parameters and *Security Configuration File (SCF)*) to the LCP.

NOTICE

> Every account with write access to parameter ***0-50 LCP Copy*** can make a backup, but only an authorized account having the named credential to "UPDATE SECURITY CONFIGURATION" can replace an existing security configuration on an already secured drive.

Changes in the LCP Copy functionality are as follows:

- ***[0] No copy***
- ***[1] All to LCP*** – does not include Security Configuration File.
- ***[2] All from LCP*** – does not include Security Configuration File.
- ***[10] Delete LCP copy data***
- ***[11] Security to LCP*** - copies only Security Configuration File to LCP
- ***[12] Security from LCP*** - updates Security Configuration File from LCP (if the user has permissions to update).
- ***[13] Security&Params to LCP***– backs up the SCF and all the application parameter to LCP.
- ***[14] Security&Params from LCP*** – copies the SCF and all the application parameter from LCP.

0-90 - reserved parameter for future cybersecurity features

0-91 Integrity Check at Powerup

This parameter controls the behavior of boot-time integrity check of installed software. The boot loader can check the integrity of the application firmware before loading and executing (both AOC and DTM). If integrity check fails for AOC, the boot process is halted. On the next power-up, the drive will try to execute Danfoss Testmonitor instead. Danfoss Testmonitor mode can be used to flash another software. However, if the integrity check fails also for Danfoss Testmonitor, the control card cannot be recovered in the field and must be replaced.

The Integrity of SCF is checked always on every power-up and on every update of the SCF. If this parameter is set to ***[2] Always***, the integrity of the SCF is checked before loading the SCF.

NOTICE

> Make sure that this parameter is set to ***[0] No Check*** before flashing an older frozen software version that does not support cybersecurity.

- ***[0] No Check*** – No boot-time integrity check of firmware. SCF check will happen anyway (factory default).
- ***[1] After Firmware Update*** – The integrity of firmware is only checked once on next power-up after software update.
- ***[2] Always*** – Software and SCF integrity is checked at every powerup. Depending on the size of the software and SCF the integrity check could delay the start-up time up to 3-4 s.

0-92 Checksum (SHA256)

Readout parameter for integrity hash values (256-bit value produced by SHA-2 algorithm represented as 64 hexadecimal symbols). Each index of this parameter shows a calculated hash of an installed application firmware or stored file that is a fundamental corner stone maintaining the integrity and security of the device.

Index values correspond to following components:

- [0] Checksum of the installed Application Oriented Controller (AOC) software.
- [1] Checksum of the Security Configuration File (SCF), 0 if the security file is not uploaded to the drive or it is not in use/invalid.
- [2] Reserved for power cards.
- [3] Checksum of the installed Danfoss Testmonitor software.
- [4] Reserved for A-option FW.
- [5] Reserved for B-option FW.
- [6] Reserved for C-option FW.

0-93 Session Timeout (in seconds)

Set for how many seconds a session of a logged-in user is kept active after a period of inactivity. Inactivity is measured differently for different access ports. For the LCP, a user is defined as inactive if no keys are pressed. Serial or network communication is inactive if no requests are sent to the drive.

0-94 Maximum Login Attempts

Number of failed login attempts allowed on a given interface before a rate-limited cool-down is activated on that interface. When an interface is in cool-down for the 1st time, no user sessions can be started on the "locked" access port for 30 s. Subsequent authentication failures on that channel will increase the cool-down time geometrically until reaching the ceiling limit of approximately 8 minutes. for setting the maximum cool-down value, use parameter ***0-93 Maximum cool-down***. During the cool-down time, all user log-on actions will always fail. This is a measure to protect the drive from brute force attacks utilizing the unit's own hardware. To prevent a denial of service attack, a cool-down can be ended prematurely on a given interface if an authorized person logs in on another channel and changes the value in parameter ***0-94 Maximum Login Attempts***. Changing parameter 0-94 value resets all the cool-down timers for all interfaces.

Factory default is 5 failed attempts before cool-down is activated. If the cool-down behavior is not acceptable, set the parameter value to the maximum value of 255.

0-95 Warning LED blinking – controls the warning LED behaviour during alarms.

0-96, 0-97 - reserved parameters for future cybersecurity features

The last 2 parameters in parameter group ***0-9* Security Settings*** are hidden from users, but they are always accessible regardless of the used SCF settings. They are used to implement parameter-based-session handling, providing the possibility to elevate user permissions on given access channel, query active user status, and resolve conflicts.

0-98 Session Response

Read-only string parameter that shows the last response to user input. See Chapter 12 Technical Specifications for more information about different responses.

0-99 User Input

Parameter that expects user input as a formatted string. See Chapter 12 Technical Specifications for more information about input formats.

11.2 Audit Log

The audit log can be monitored and read out from parameter group ***43-6* Audit Log***. One audit log entry contains event type, user account, access channel, and timestamp (either by storing operating hours value or current date and time if it is set). The audit log capacity is 100 log entries, following entries overwrite the oldest entries.

NOTICE

Timestamps have a second resolution. If the date and time are set, the operating hours value is not stored in audit log to save the log space. Other logs, such as Alarm Log, that store both can be used to create a reference point between operating hours values and set date and time.

NOTICE

The drive does not provide service for automatically transferring logs to an external server. If long-term log storage is needed, the data needs to be read out (via fieldbus or PC tools) and stored.

Table 13: Audit Log

ID	Event	Stored in log
1	Factory reset event	Yes
2	Password set (a user changed a password, for example, from LCP)	Yes
3	Drive set into boot mode	Yes
4	Security configuration downloaded to drive (new SCF is downloaded or existing one is updated)	Yes
5	Security configuration applied	Yes
7	Successful login	Yes
8	Failed login (maximum number of retries reached)	Yes
9	Audit log buffer overrun. Audit log registers more than 99 new events and is not able to store them all.	Yes
10	Session timeout (LCP/MCT10) - not logged to save log-space	No
11	Backup of security configuration - not logged to save log-space	No

12 Technical Specifications

12.1 Parameter-based Session Control

Parameters ***0-99 Session Request/Input***(input parameter) and ***0-98 Session Response/Feedback*** (output parameter) implement a simple open-text protocol to handle human-user sessions on a secure drive. Here are the listed technical specifications, which requests the drive can handle, and what is expected responses to these requests.

Table 14: Parameter Value and Usage

Parameter	Type	Value	Usage
0-98 Session Response/ Feedback	Command string read-Only	"Protocol version: ...", "Logging in", "Access ...", "User: ..."	Feedback to PC-tool, logged in user credentials, feedback info, error codes, and so on.
0-99 Session Request/Input	Command string	string of 4 chars without ':' - a request ":<password>" - PIN authentication "<username>:<password>" - authentication request for given username	This parameter is used to send requests to drive.

Table 15: Supported Requests and Responses

Version	Input	Response	Comment
1.0	:<password>	"Logging in" -> "Access Granted" or "Access Denied" ->"Error 409: Conflict"	PIN authentication requests
1.0	<username>:<password>	"Logging in" -> "Access Granted" or "Access Denied" ->"Error 409: Conflict"	user&pass authentication requests
1.0	FINS	"491: Request Pending" -> "Finished"	FINISH SESSION - request needs a follow-up authentication request.
1.0	VERS	"Protocol version: %d.%d"	REQUEST_PROTOCOL_VERSION - shows that major.minorversion of the protocol drive is using.
1.0	WHO?	"User: %s; ID: %u; Role: %s"	REQUEST_WHOAMI - shows who has logged in on the same channel.

To end own/other's session send: "FINS" request to parameter ***0-99 Session Request/Input*** followed by another write sending valid authentication credentials (session owner's or other's)

Table 16: Response Format

Response	Comment
"information"	Informative message, does not require follow-up actions
"< 3-digit-number>: information"	Non-error state, follow-up action is needed
"Error < 3-digit-number>: information"	Error condition, request denied

Table 17: Error Codes

Error	Meaning
"Error 401: Unauthorized"	Request requires prior user authentication.
"Error 405: Method Not Allowed"	Request specified in the line is understood, but not allowed (not supported).

Table 17: Error Codes - (continued)

Error	Meaning
"Error 409: Conflict"	Another user is logged in.
"Error 606: Not Acceptable"	Unsupported channel is used for session creation.

12.2 Parameters with Exception in Access Control

Table 18: Parameters with Exception in Access Control

Parameter number or file	Bus	Mandatory accessibility	Purpose
10	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
11	Serial, USB, Fieldbus	READ/WRITE	Enables reading from different setups
12	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
15	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
34	Serial, USB, Fieldbus	READ-ONLY	System use notification text
60	Serial, USB, Fieldbus	ERROR CODE 133	For copying in MCT 10 the drive from *Network* to *Project*
67	Serial, USB, Fieldbus	READ/WRITE	Legacy bus password parameter
68	Serial, USB, Fieldbus	READ/WRITE	To enter the password for safety option
98	Serial, USB, Fieldbus	READ-ONLY	Session control
99	Serial, USB, Fieldbus	READ/WRITE	Session control
810	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
813	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
814	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
830	Serial	READ/WRITE (only for MCT 10)	For switching the protocol from FC to FCMC
1201	Fieldbus	READ/WRITE (only for MCT 10)	EDU uses for drive identification
1208	Fieldbus	READ/WRITE (only for MCT 10)	EDU uses for drive identification
1209	Fieldbus	READ/WRITE (only for MCT 10)	EDU uses for drive identification
1500	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1530	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1531	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1532	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1533	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1540	Serial, USB, Fieldbus	READ-ONLY	For identification
1541	Serial, USB, Fieldbus	READ-ONLY	For identification
	Serial, USB, Fieldbus	READ-ONLY	For identification
1542	Serial, USB, Fieldbus	READ-ONLY	For identification
1543	Serial, USB, Fieldbus	READ-ONLY	For identification

Table 18: Parameters with Exception in Access Control - (continued)

Parameter number or file	Bus	Mandatory accessibility	Purpose
1544	Serial, USB, Fieldbus	READ-ONLY	For identification
1545	Serial, USB, Fieldbus	READ-ONLY	For identification
1546	Serial, USB, Fieldbus	READ-ONLY	For identification
1547	Serial, USB, Fieldbus	READ-ONLY	For identification
1549	Serial, USB, Fieldbus	READ-ONLY	For identification
1550	Serial, USB, Fieldbus	READ-ONLY	For identification
1551	Serial, USB, Fieldbus	READ-ONLY	For identification
1553	Serial, USB, Fieldbus	READ-ONLY	For identification
1560–1564	Serial, USB, Fieldbus	READ-ONLY	For identification
1570	Serial, USB, Fieldbus	READ-ONLY	For identification
1571	Serial, USB, Fieldbus	READ-ONLY	For identification
1572	Serial, USB, Fieldbus	READ-ONLY	For identification
1573	Serial, USB, Fieldbus	READ-ONLY	For identification
1574	Serial, USB, Fieldbus	READ-ONLY	For identification
1575	Serial, USB, Fieldbus	READ-ONLY	For identification
1576	Serial, USB, Fieldbus	READ-ONLY	For identification
1577	Serial, USB, Fieldbus	READ-ONLY	For identification
1594	Serial, USB, Fieldbus	READ-ONLY	For identification
1598	Serial, USB, Fieldbus	READ-ONLY	For identification
1599	Serial, USB, Fieldbus	READ-ONLY	For identification
1600	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1602	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1603	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1660	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1666	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1671	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1690–1699	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1855	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1856	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
1999	Serial, USB, Fieldbus	READ-ONLY	For identification
4040	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4041	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4042	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4043	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4044	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4045	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status

Table 18: Parameters with Exception in Access Control - (continued)

Parameter number or file	Bus	Mandatory accessibility	Purpose
4046	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4330	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4331	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4332	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4333	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4338	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4339	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4340	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4341	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4342	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4343	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4344	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4345	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4346	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4347	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4348	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
4349	Serial, USB, Fieldbus	READ-ONLY	For reading the drive status
File 0, which is the directory listing, must include at least the PUD file in the list.	Serial, USB, Fieldbus	READ-ONLY	For downloading the proper PUD file
PUD file	Serial, USB, Fieldbus	READ-ONLY	For downloading the proper PUD file

12.3 Special Named Permissions for User Accounts in SCF

Table 19: Special Named Permissions for User Accounts in SCF

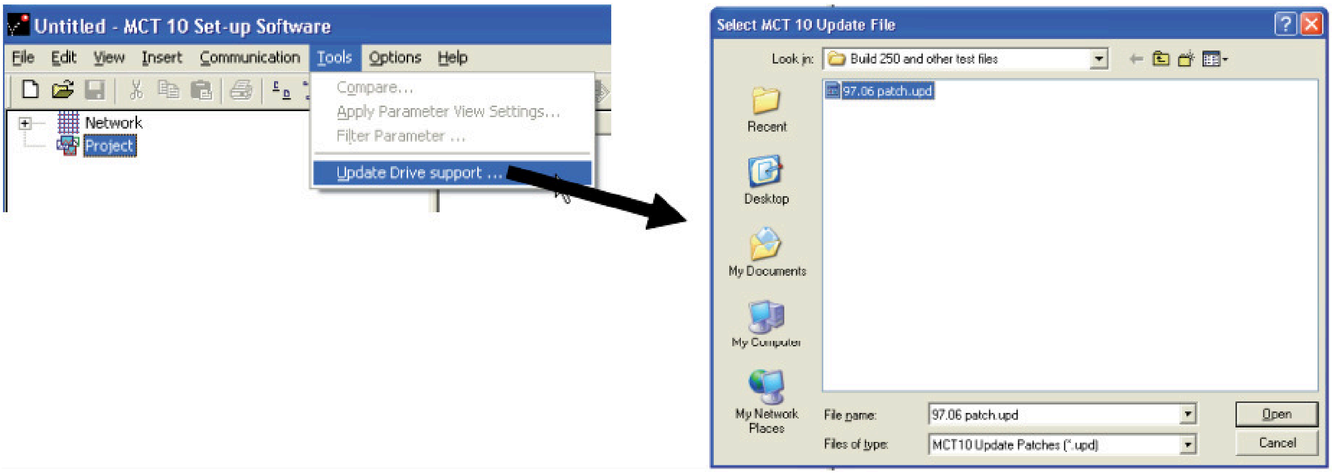
Named permission	Explanation of the given permission
VLT.ALLOW.UPDATE_FIRMWARE	The drive can be set to boot mode to: • Update the AOC/option software • Change the drive filesystem content
VLT.ALLOW.UPDATE_SECURITY_CONFIGURATION	It is possible to upload a new security configuration if one is already present.
VLT.ALLOW.CLEAR_LICENSE	It is possible to clear licensed software features.
VLT.SERVICE_CODES.USER	Customer service codes are allowed.
VLT.SERVICE_CODES.DANFOSS_SERVICE	Allows both customer and Danfoss maintenance service codes.
VLT.SERVICE_CODES.TESTING	DANFOSS INTERNAL USAGE: All service codes are allowed.
VLT.USER.COPY_ACCESSRIGHTS_FROM.<AccountName>	For this account, use the same access rules as for the named account.

13 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 MCT 10 software.

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


Untitled - MCT 10 Set-up Software
File Edit View Insert Communication Tools Options Help
Network
Project
Compare…
Apply Parameter View Settings…
Filter Parameter …
Update Drive support …
Select MCT 10 Update File
Look in: Build 250 and other test files
97.06 patch.upd
Recent
Desktop
My Documents
My Computer
My Network Places
File name: 97.06 patch.upd
Files of type: MCT10 Update Patches (*.upd)
Open
Cancel

e30bl728.10

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

14 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 *VLT® 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 *VLT® 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.

15 Appendix

15.1 Graphical Local Control Panel (GLCP)

15.1.1 Overview

Press [*Status*] + [*Alarm Log*] to activate the GLCP login menu.

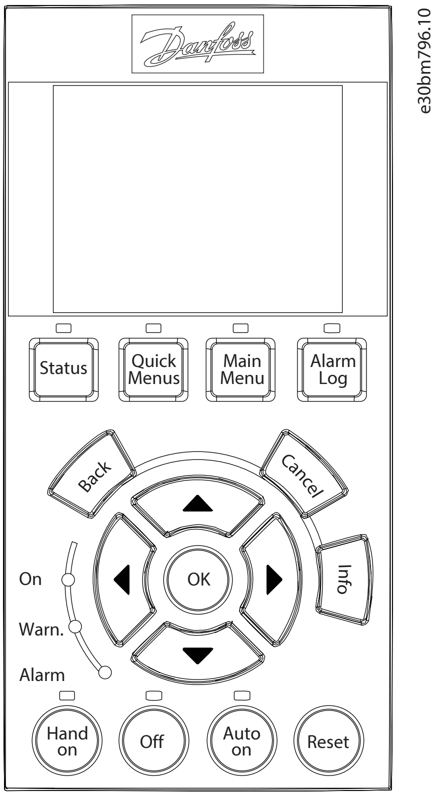


Figure 17: Graphic Local Control Panel (GLCP)

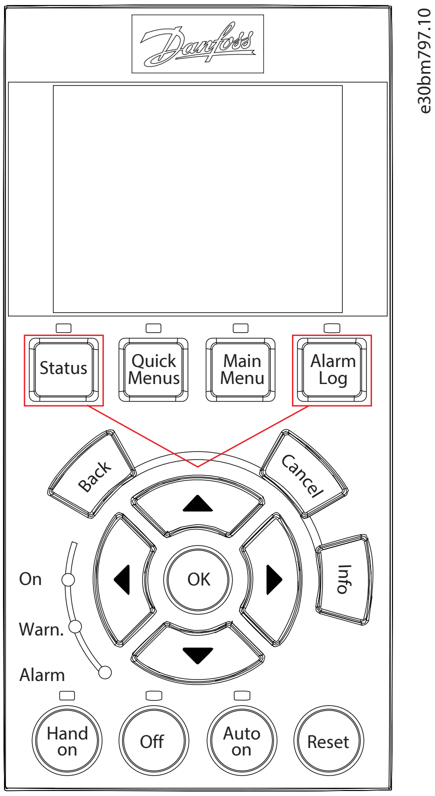


Figure 18: Enter Password

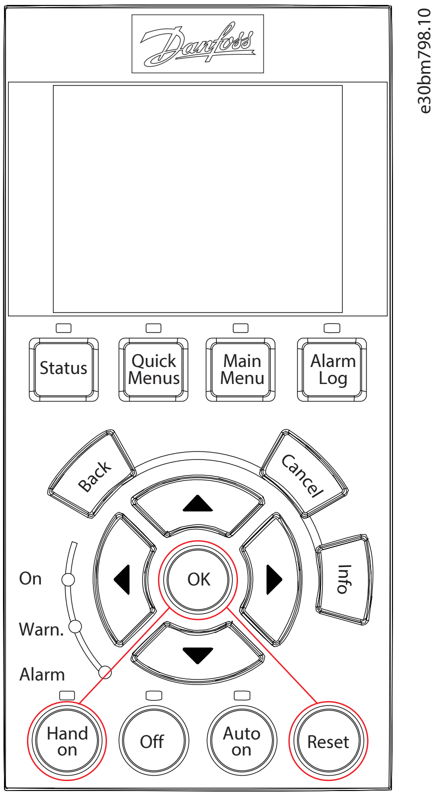
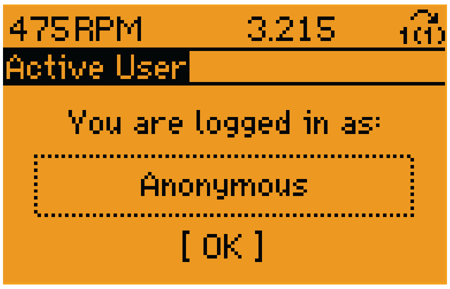


Figure 19: Factory Reset

15.1.2 Usage

Press [*Status*] and [*Alarm Log*] buttons, see Figure 18, you are shown which user is logged in from the LCP:


475 RPM 3.215

Active User

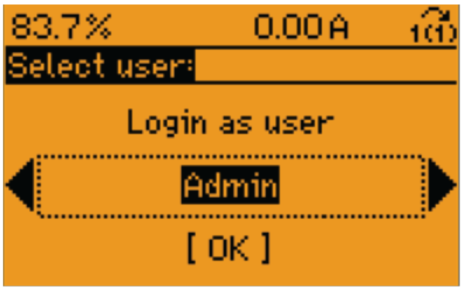
You are logged in as:

Anonymous

[OK]

Figure 20: Anonymous Login

It is only possible to press OK on this screen. On the next screen, an anonymous user can log in as another user. Use [◀] and [▶] to select between users. Press [*OK*] to select a user.


83.7% 0.00 A

Select user:

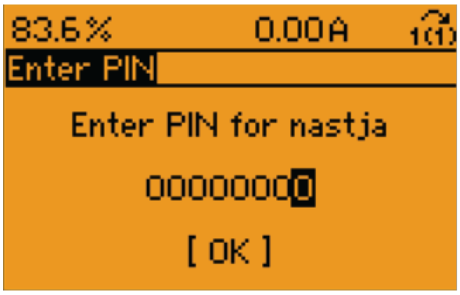
Login as user

Admin

[OK]

Figure 21: Admin Login

Enter the PIN for the selected user. On entering the correct PIN, login is successful.


83.6% 0.00 A

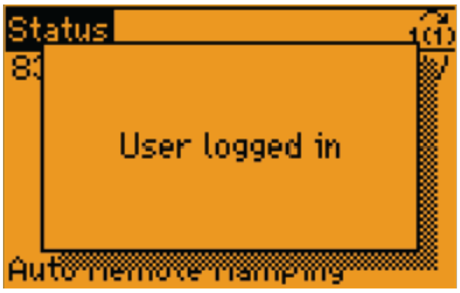
Enter PIN

Enter PIN for nastja

00000000

[OK]

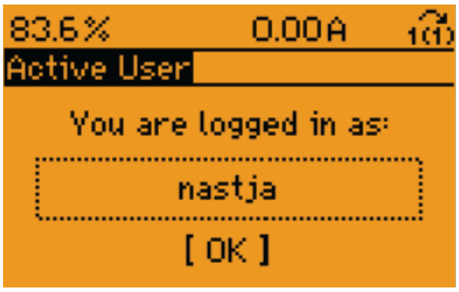
Figure 22: Enter the PIN for the Selected User


Status

User logged in

Figure 23: User Logged in Pop-up

To see the active user, press [*Status*] and [*Alarm Log*] again, see Figure 18.



83.6% 0.00A 1(1)

Active User

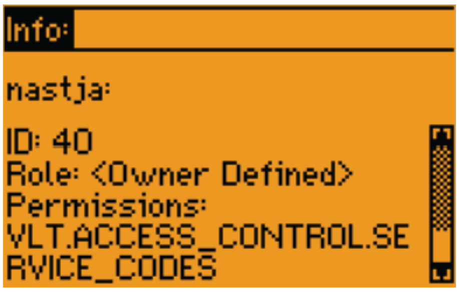
You are logged in as:

nastja

[OK]

Figure 24: Active User Name

Press [*Info*] to see more information about the active user.



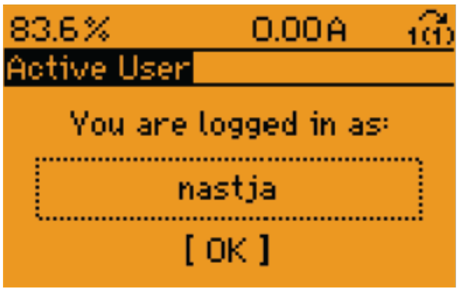
Info:

nastja:

ID: 40
Role: <Owner Defined>
Permissions:
VLT.ACCESS_CONTROL.SE
RVICE_CODES

Figure 25: Information About Active User

Press [*Info*] again to close this view and return to the active user login screen.



83.6% 0.00A 1(1)

Active User

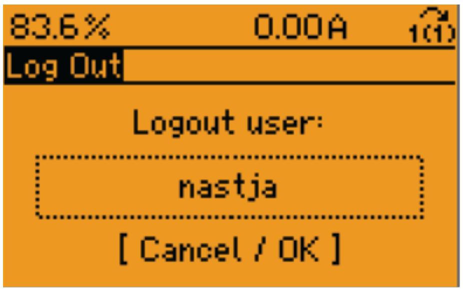
You are logged in as:

nastja

[OK]

Figure 26: Active User Name

Press [*OK*] to get to the logout screen.



83.6% 0.00A 1(1)

Log Out

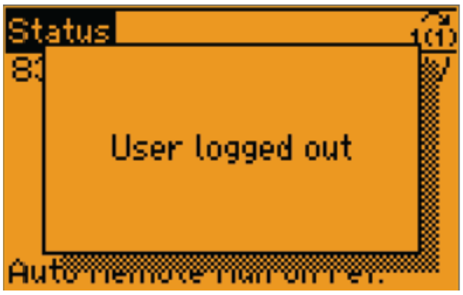
Logout user:

nastja

[Cancel / OK]

Figure 27: Option to Log Out

Press [*OK*] to log out.



Status 1(1)

User logged out

Auto

Figure 28: User Logged out Pop-up

It is now possible to log in as another user. It is not possible to log in multiple users from the LCP at the same time.

15.2 Numeric Local Control Panel (NLCP)

15.2.1 Overview of the Numerical Control Panel

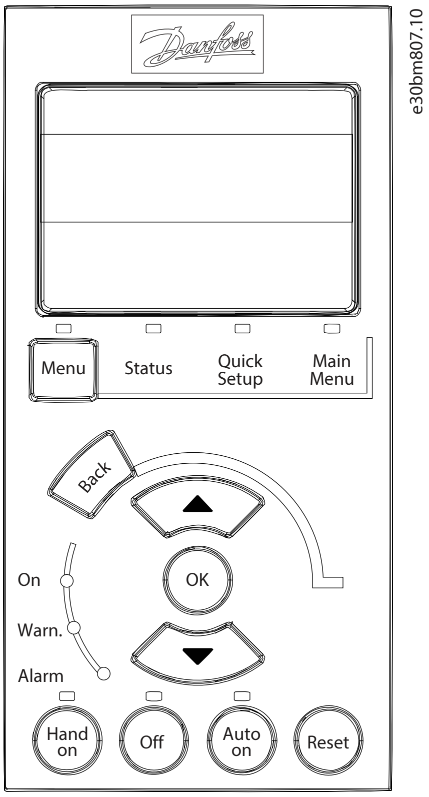


Figure 29: Numeric Local Control Panel (NLCP)

Password keys = [*Menu*]-[*OK*]-[▼]

Limitations: no ASCII/characters, only cursor [▲]/[▼], missing keys (info/quick menu/and so on).

The user must be identified via the user ID (the security file calls it “id”).

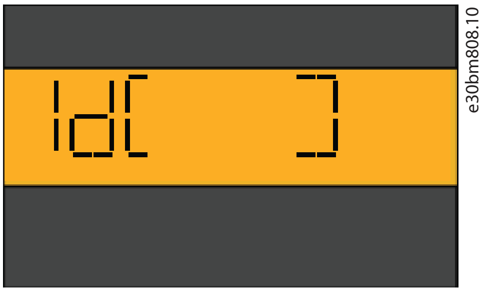


Figure 30: User Id

Use the [▲]/[▼] to select the user. Click [*OK*] to activate the user.

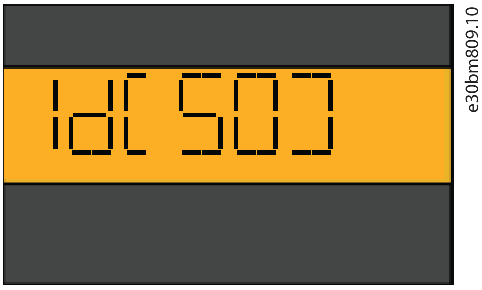
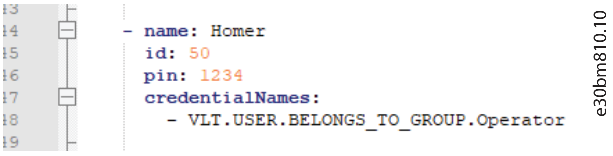


Figure 31: Example User 50

50 is user "Homer" in this example:



```
  - name: Homer
    id: 50
    pin: 1234
    credentialNames:
      - VLT.USER.BELONGS_TO_GROUP.Operator
```

Figure 32: Example User 50

Click [*OK*] to activate PIN dialog.

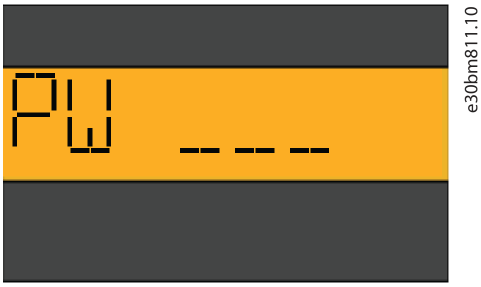


Figure 33: PIN dialog

[▲]/[▼] selects the active 1st digit. Another [*OK*] selects the next digit.

When editing, the reaction time of the display may be a little slow. To avoid typos, be thorough when editing.

As the pin has 8 digits, the dialog changes to the 2nd pin screen after the 4th digit has been entered.

If the pin consists of only 4 digits, the first 4 digits must be entered as "0".

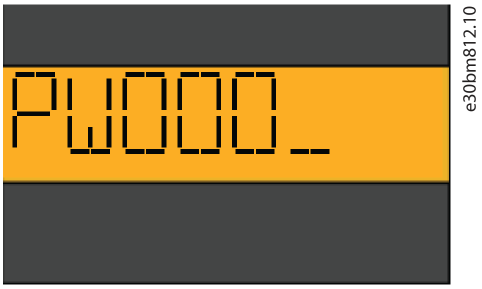


Figure 34: 1st Screen with 4 Digits for PIN

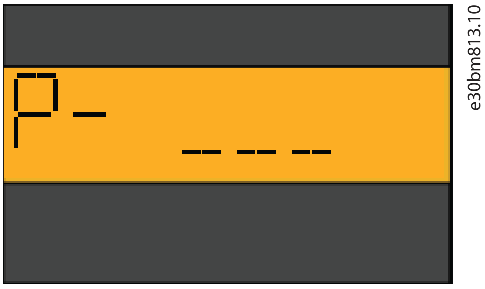


Figure 35: 2nd Screen for PIN

The “-“ indicates the 2nd screen.

NOTICE

It is not possible to revert to the 1st screen. If needed, start from the beginning.

On entering the 8th digit, the drive shows *done*, if the PIN is correct. In case of a wrong PIN, the drive shows *fail*.

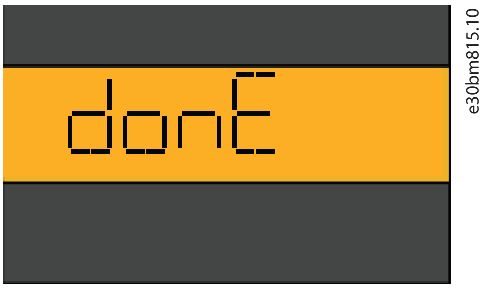


Figure 36: Login Message

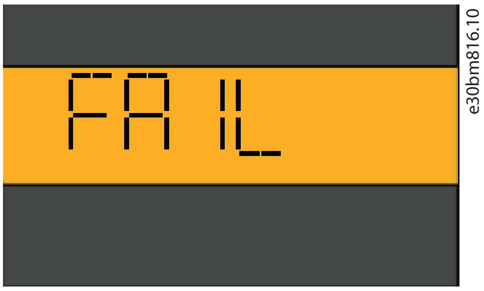


Figure 37: Fail Message

To log out, enter the PW menu again ([*Menu*]-[*OK*]-[▼]) and select ID [***00***].

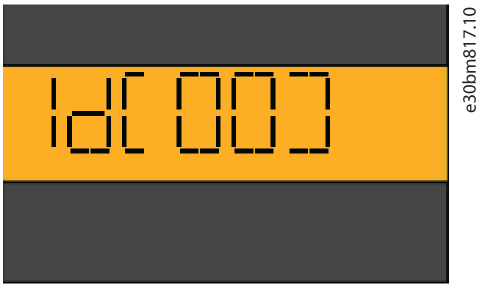


Figure 38: Logout Id

On successful logout, the drive displays *bye*message.

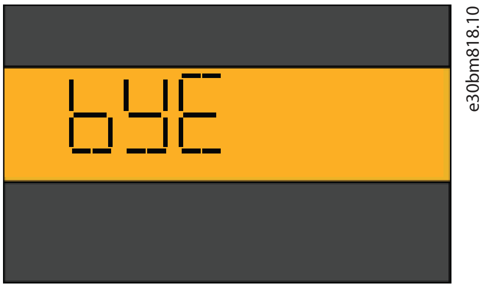


Figure 39: Logout Message

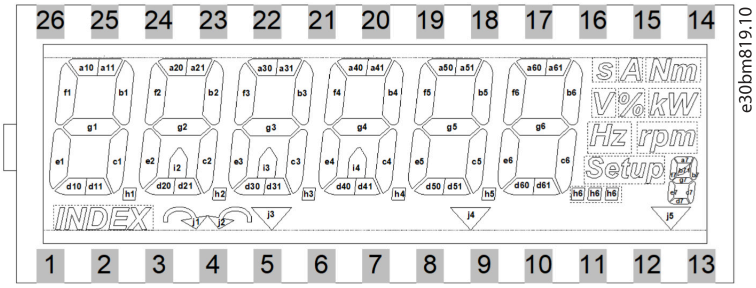


Figure 40: Display

15.2.2 System Use Notification Text (Parameter 00-34)

Local user interfaces provide the capability to display a system use notification message before authenticating. The message is configurable by authorized personnel.

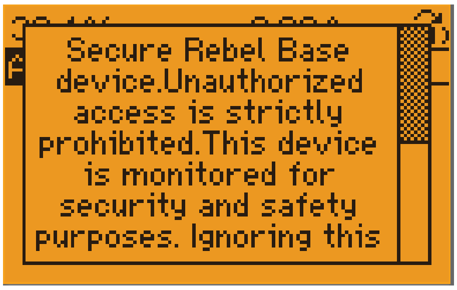
Example:

Secure <ASSET_OWNER_NAME> device. Unauthorized access is strictly prohibited. This device is monitored for security and safety purposes.

Ignoring this warning and proceeding without the necessary permissions may result in severe legal penalties. Access to this device/ operation is only for authorized personnel who possess the necessary credentials.

- The text is displayed in a pop-up when a user logs in via LCP.
- Use the LCP to edit the text. However this is challenging.
- The length for editing via LCP is limited to 50 characters.
- The longer text up to 240 characters can be added via MCT 10.
- Only logged-in users are permitted to change the parameter. Access control rules must be in place to enforce this and prevent unauthorized modifications.
- The parameter can also be changed via fieldbus (if fieldbus allows this parameter type).
- The user must verify that the characters are displayed correctly on LCP.

- The text must be set by the user, by default the parameter is empty.
- The text is not available on NLCP.
- If the user has not set this text, no message/popup will appear.
- The popup can be closed with the *[OK]*or *[cancel]* button.



Secure Rebel Base device.Unauthorized access is strictly prohibited.This device is monitored for security and safety purposes. Ignoring this

Figure 41: Example Popup

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.