User guide

Cybersecurity

VACON® NX



Explore our solutions
drives.danfoss.com

VACON®

Contents

1 Introduction

1.1 Purpose of the Guide 7
1.2 Scope 7
1.3 Terms and Abbreviations 8
1.4 Extended Requirements 9
1.5 Document Version 9

2 Safety

2.1 Safety Symbols 10
2.2 General Safety Considerations 10
2.3 Qualified Personnel for Working with Cybersecurity 11

3 Security Measures and Management

3.1 Overview 12
3.2 Product Defense-in-Depth Strategy 12
3.3 Security Context 12
3.3.1 VACON® NX Applications and Industries 12
3.3.2 Interfaces of VACON® NX Products 14
3.3.3 Intended Environment 14
3.4 Interfaces 15
3.5 Tools and Software for VACON® NX Products 16
3.6 Software and Firmware Updates 17

4 Security Features and Verification of Functionality

4.1 Identification of Security Capabilities 18
4.2 Security Parameters of VACON®NX Drives 18
4.3 Secure Boot 19
4.3.1 Secure Boot Overview 19
4.3.2 Secure Boot Recovery 19
4.4 Connectivity 19
4.5 User Management 20
4.5.1 User Access and Configuration Management 20
4.5.2 Setting-up Admin Password via VACON® NCDrive 20
4.5.3 Setting-up Admin Password via Keypad 21

4.5.4 Changing Admin Password via VACON® NCDrive 23
4.5.5 Changing Admin Password via Keypad 24
4.5.6 Password Requirements 26
4.5.7 Login via VACON® NCDrive 26
4.5.8 Login via Keypad 26
4.5.9 Logout via VACON® NCDrive 27
4.5.10 Logout via Keypad 28
4.5.11 Cooldown Period After Repeated Failed Logins 28
4.5.12 System Use Notification 29
4.5.13 Configuring Anonymous Access Rights and Keypad Settings 30
4.6 Session Timeout 31
4.7 Audit Logging 31
4.8 Disable Option Board Slots 34
4.9 Physical Tamper Resistance and Detection 34
4.10 Denial of Service Protection 34
4.11 Control System Backup and Recovery 34
4.11.1 Control System Backup and Recovery Management 34
4.11.2 Backup via VACON® NCDrive 35
4.11.3 Backup via Keypad 35
4.11.4 Automated Backup via VACON® NCDrive 35
4.11.5 Automated Backup via Keypad 36
4.11.6 Restore Backups via VACON® NCDrive 38
4.11.7 Restore Backups via Keypad 38
4.12 Device Component Inventory (Service Info) 39
4.13 Update VACON® NX Firmware 41

5 Security Configuration Guidelines

5.1 Overview 43
5.2 General Principles 43
5.2.1 General Security Principles 43
5.2.2 Restrict Physical Access 43
5.2.3 Restrict Network Access 43
5.2.4 Reduce the Attack Surface 44
5.2.4.1 Reducing System Attack Surface 44
5.2.4.2 Disabling PC-Tool Connectivity from OPTEA/OPTE9 Cards 45

Danfoss Drives Oy © 2026.11

5.2.4.3 Disabling SNMP Functionality 46
5.2.5 Set up User Management and Access Control 46
5.2.6 Perform Regular Maintenance 47
5.3 Security Limitations and Non-Mitigated Threats 47

6 Decommissioning

6.1 Disposal of the Drive 52
6.2 Erase User Customized Application 52
6.3 Secure Reset Function 52
6.4 Clear Data Stored in the Keypad 53
6.5 Backups 54
6.6 Remaining Data After Various Resets 54

7 Appendix

7.1 Achieved Security Level Capabilities for Component Requirements 55
7.2 Fault Codes Related to Cybersecurity Features 56

Danfoss Drives Oy © 2026.11

1 Introduction

1.1 Purpose of the Guide

The purpose of this guide is to provide comprehensive guidance and understanding of cybersecurity measures and best practices adopted by VACON® NX products from Danfoss.

As a Product Supplier, Danfoss provides information on VACON® NX products to be used in the industry based on:

- IEC 62443-4-1: Development and manufacturing of products.
- IEC 62443-4-2: Cybersecurity features of the products and approved Security Level Capability.

The components selected for the system must be able to fulfill the requirements of the intended/Targeted Security level (SL-T). SL-T 0 is the lowest and SL-T 4 is the highest level.

The VACON® NX products distinguish between Local and Remote operation:

- Local operation is defined as the user interacting in physical proximity with the VACON® NX product. This could be the Keypad or PC software tools.
- Remote operation is defined as an external controller, for example, a PLC interacting with the VACON® NX product via a fieldbus or other external interface.

The Security Level Capability of VACON® NX is SL-C 1, and the secure development process is certified by TÜV to meet Maturity Level 3.

1.2 Scope

This guide applies to all VACON® NX products mentioned in the following list. While not all these products are drives, the term “drive” is used throughout this guide for simplicity to refer to all applicable products.

The following product variants are in the scope of this guide:

- VACON® NXP liquid-cooled
- VACON® NXP air-cooled
- VACON® NXP AFE/Grid Converter
- VACON® NXP DC/DC Converter
- VACON® NXP Common DC Bus
    - VACON® NX Inverter (INU)
    - VACON® NXP DCGuard
    - VACON® NX brake chopper module (BCU)
    - VACON® Non-regenerative front-end (NFE)

Available options include basic and safety I/O options, digital I/O extensions, encoder/resolver interface as well as temperature and voltage measurement options. These options are included in the drives as option boards.

The following option boards are in the scope of this guide:

- OPTA series
- OPTB series
- OPTD series
- OPTE series

Only option boards OPTE9, OPTEA, and OPTEC include such firmware which has any relationship for the cybersecurity functionalities of VACON® NX drives.

Table 1 shows the minimum firmware versions for VACON® NX products which are in the scope of this guide. Cybersecurity features were introduced in these versions, and thus older versions do not include the features and functionalities described in this guide.

Table 1: Minimum Firmware Versions Required for Security Capabilities

NX component	Minimum firmware version	Minimum boot version
Control board	NXP00002V212	53.2.x
OPT-E9	FW0196V015	2.6.0
OPT-EA	FW0241V013	2.6.0
OPT-EC	FW0128V006	2.6.0

Verify the latest firmware version from the Danfoss website when updating the drive. More instructions can be found in 3.6 Software and Firmware Updates.

1.3 Terms and Abbreviations

Table 2: Terms and Abbreviations

Term/ Abbreviation	Description
AFE	Active Front End
BOM	Bill of Materials
CCA	Change Control Authority
CCB	Change Control Board
CM	Configuration Management, Change Management
CS	Cybersecurity
DD/DDS	Danfoss Drives
DPD	Danfoss Power Electronics and Drives
EMS	Electronics Manufacturing Services
ERP	Enterprise Resource Planning
FI	Finland
GC	Grid Converter
HW	Hardware
ID	Identification
LCD	Liquid-cooled Drive
LOC	Local
PCR	Product Change Record
PDM	Product Development Management
PLM	Product Lifecycle Management
PO	Product Owner
PRS	Product Requirement Specification
PTO/PTI	Power Take Out/Power Take In
QR	Quality Release
R&D	Research and Development (organization)
RBAC	Role-based access control
REM	Remote

Danfoss Drives Oy © 2026.11

Table 2: Terms and Abbreviations - (continued)

Term/ Abbreviation	Description
RQR	Request for Quality Release
SBOM	Software Bill of Materials
SC (S/C)	Supply Chain (aka Production or Manufacturing)
SOP	Standard Operating Procedure
S-PDS	System Product Design Specification
SPT	Software Platform Team
SQM	Supplier Quality Manager
SVV	Security Verification and Validation
SW	Software
T-PDS	Technical Product Design Specification

1.4 Extended Requirements

The IEC 62443 is the basis for industrial automation cybersecurity. If an issuer of certificates or approvals extends the requirements beyond this standard, the system integrator must consider these additional requirements when preparing their cybersecurity documentation.

1.5 Document Version

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

The original language of this guide is English.

Table 3: Document and Software Versions

Version	Remarks
BC563869736695, document version 01	First release

2 Safety

2.1 Safety Symbols

The following symbols are used in Danfoss documentation and products.

DANGER

Indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING

Indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION

Indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

NOTICE

Indicates information considered important, but not hazard-related (for example, messages relating to property damage).

	ISO warning symbol for hot surfaces and burn hazard
	ISO warning symbol for high voltage and electric shock
	ISO action symbol for referring to the instructions

2.2 General Safety Considerations

When installing or operating the drive, pay attention to the safety information given in the instructions. For more information about safety guidelines for installation, see the product-specific safety guide that is included in the drive shipment. For more information about safety guidelines for operating the drive, see the product-specific guides.

WARNING



RISK OF ELECTRIC SHOCK

The STO safety function does not provide electrical safety. The STO function itself is not sufficient to implement the Emergency-Off function as defined by IEC 60204-1:2018. Using the STO function to implement Emergency-Off may lead to death or personal injury.

- Emergency-Off requires measures of electrical isolation, for example, by switching off mains via an extra contactor.

Danfoss Drives Oy © 2026.11

NOTICE

COMMISSIONING TEST

After installing the safety functions, perform a commissioning test.

A successful commissioning test is required after the initial installation, and after each change to the installation or application involving functional safety.

If the commissioning test fails, safe operation cannot be guaranteed.

2.3 Qualified Personnel for Working with Cybersecurity

Only qualified personnel are allowed to install, configure, commission, maintain, and service cybersecurity-related functions and settings. Qualified personnel are individuals who have sufficient knowledge of industrial automation, networks, and cybersecurity to understand how their actions can affect the security of the system.

Qualified personnel

Requirements:

- The personnel must be familiar with applicable cybersecurity requirements and industry standards, including IEC 62443.
- The personnel must have read and understood the cybersecurity information provided in this guide.
- The personnel must understand how user accounts, passwords, network connections, and remote access can affect system security.
- The personnel must be aware of the risks associated with connecting industrial equipment to company networks, enterprise systems, or the Internet.
- The personnel must be able to apply basic cybersecurity measures appropriate for the installation.

Machine builders, system integrators, and asset owners

Responsibility:

- Assessing cybersecurity risks for the application and installation.
- Defining the required security level for the system.
- Implementing appropriate network segmentation, access control, and protection measures.
- Maintaining the cybersecurity of the installation throughout its lifecycle, including software updates, backups, monitoring, and incident management.

Cybersecurity is not provided by a single product alone. The overall security of the system depends on secure design, proper configuration, and ongoing maintenance of the complete installation.

3 Security Measures and Management

3.1 Overview

A security management process according to IEC 62443-4-1 and ISO 27001 forms the basis for the implementation of industrial cybersecurity.

This section explains how cybersecurity is addressed in VACON® NX drives. It provides a foundational overview of the product's security approach, beginning with the defense-in-depth strategy and expanding to examine the cybersecurity context from multiple perspectives.

3.2 Product Defense-in-Depth Strategy

The defense-in-depth strategy for VACON® NX includes:

- Defining the intended use and operating environment
- Identifying threats and mitigations
- Implementing countermeasures
- Documenting residual risk
- Ensuring efficient incident management

IEC 62443-4-1 defines the secure development lifecycle, while IEC 62443-4-2 defines the cybersecurity capabilities implemented in the products.

The customer is a vital part of this defense strategy and must monitor updates and notifications from Danfoss to ensure that security-related updates and patches are installed in a timely manner.

To report a security incident, contact Danfoss:

- Email: security@danfoss.com
- Website: https://www.danfoss.com/en/service-and-support/coordinated-vulnerability-disclosure/report-a-vulnerability

3.3 Security Context

3.3.1 VACON® NX Applications and Industries

The VACON® NX drives are primarily intended for marine propulsion and machinery, as well as power conversion, and generation applications.

From a cybersecurity perspective, the product is intended for applications with limited cybersecurity risk and exposure. It provides basic cybersecurity capabilities but is not designed to meet higher security levels under the IEC 62443-4-2 Component Requirements. For critical applications requiring more advanced security features and higher levels of security, the Danfoss iC7 platform is the preferred solution.

The product is expected to be deployed at the lower levels of the automation hierarchy. As a result, multiple layers of defense typically exist between potential attackers and the product, reducing the likelihood of direct access via network-based attacks.

Environments and industries where VACON® NX drives are used:

- Marine and offshore
- Food and beverage
- Water and wastewater
- HVAC/Building automation
- Refrigeration
- Chemical

Danfoss Drives Oy © 2026.11

- Mining and minerals
- Cranes, hoists, elevators, and escalators
- Metal, pulp and paper, cement, oil, and gas
- Power and energy

The VACON® NX drives offer the development of electrification, power, and propulsion solutions, including AC and DC networks and conversions between VACON® NX drives with Marine and Hybrid applications.

- Hybrid propulsion
  - Battery energy storage
  - DC grids
  - AC grids
  - Main power generation
    - Hybrid shaft generator
    - Shore power supply
- Diesel-electric propulsion
- Thrusters
- Steering gears
- Winches
- Cranes
- Fans and HVAC systems
- Process pumping
- Cooling water systems
- Separators
- Refrigeration compressors

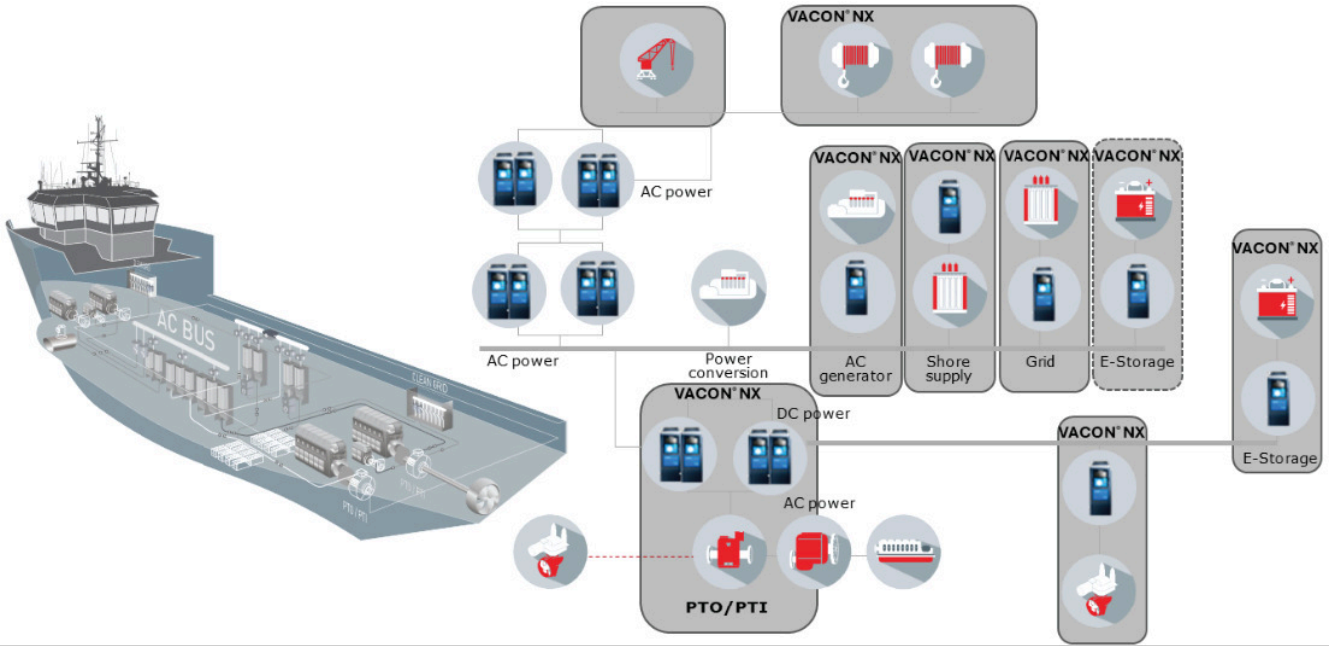


Figure 1: Uses of VACON® NX-Marine and VACON® NX-Hybrid Modules in Representative Example Application

3.3.2 Interfaces of VACON® NX Products

Figure 2 shows the VACON® NX products interfaces and categories. The integrator must consider all relevant interfaces when performing a system-level risk assessment. Some interfaces are internal and not intended to be exposed outside of the enclosure.

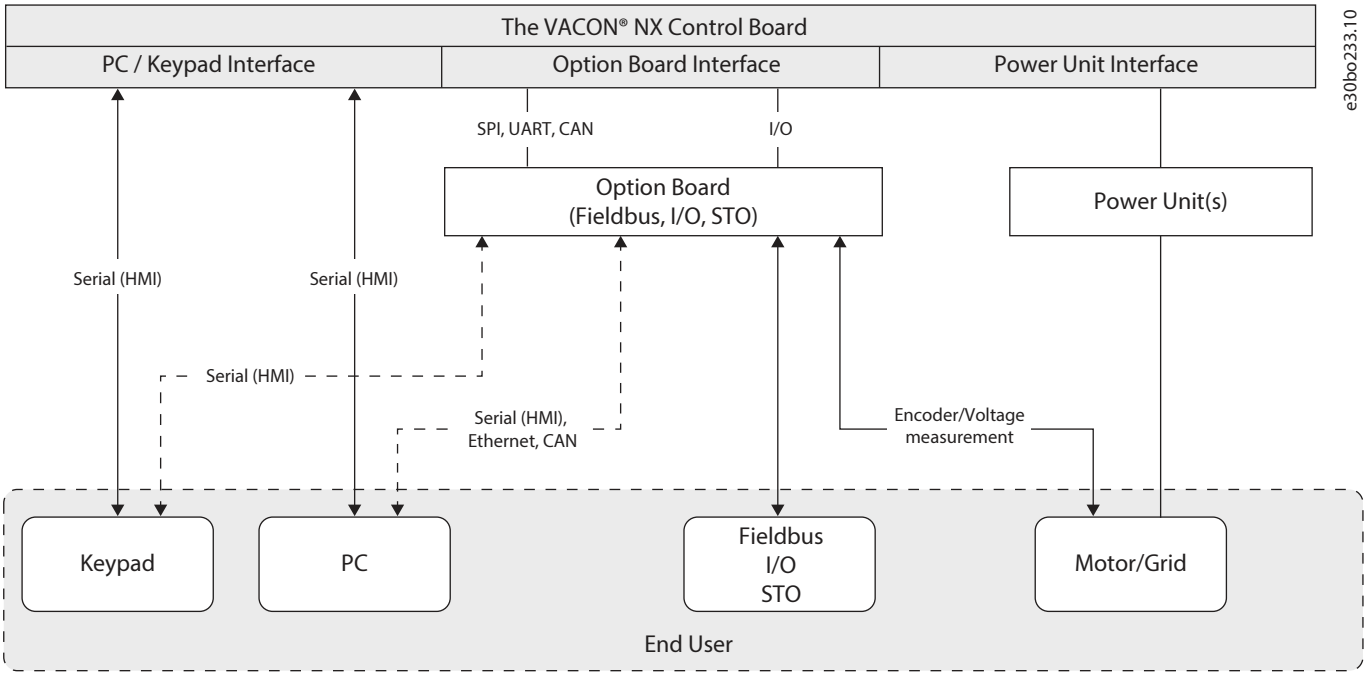


Figure 2: Interfaces of the VACON® NX Products

3.3.3 Intended Environment

- The VACON® NX products are intended to be installed in an enclosure within an access-controlled area that provides physical security accessible only to authorized and trained personnel. See Figure 3.
- Equipment that is connected to local interfaces, instrumentation, and control interface is contained within a secured area.
- Do not connect VACON® NX directly to untrusted networks.
- Internal and module-to-module interfaces remain protected inside an enclosure.
- Unauthorized physical access to the control panel of the device must be prevented.
- External communication and remote interfaces, for example, Ethernet or fieldbus may cross security boundaries or connect to wider networks. As a result:
  - Monitor and filter network traffic or protect it by external cybersecurity measures.
  - The VACON® NX products must not be used as a boundary device or conduit, according to IEC 62443-1-1.
- The connections to the cooling and power interfaces providing coolant to the drives and the grid power may cross security boundaries. These interfaces do not transfer data. It is the responsibility of the asset owner to protect these connections and ensure the availability and correct functioning of the external systems.

Danfoss Drives Oy © 2026.11

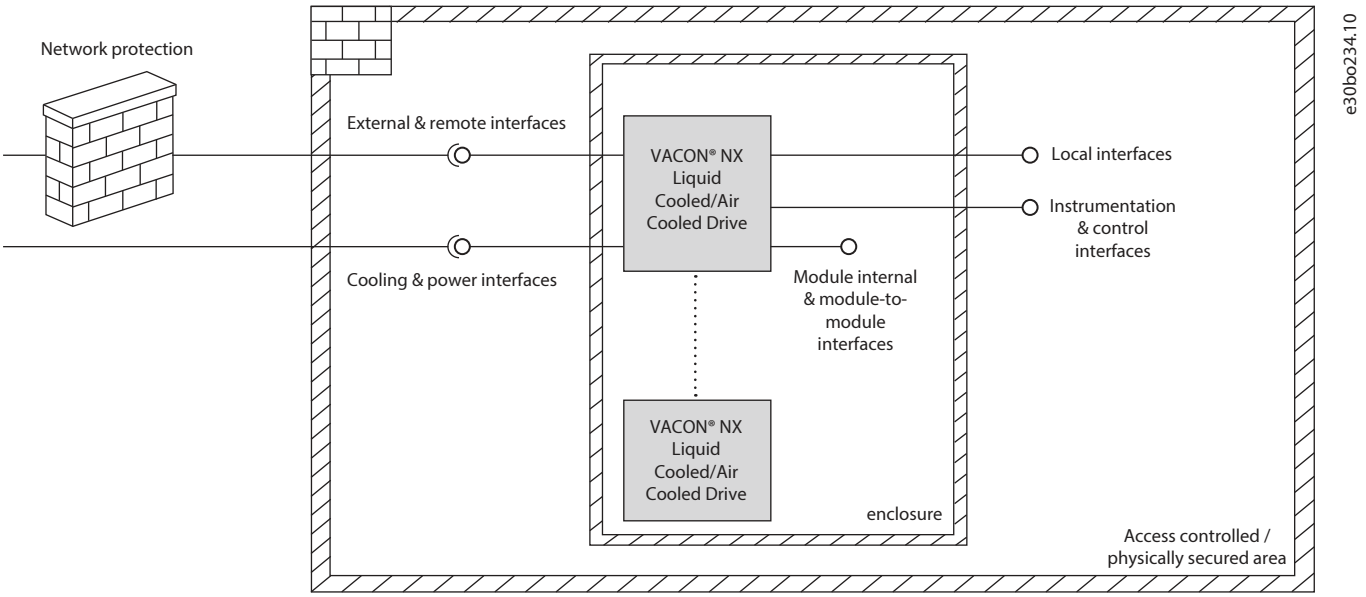


Figure 3: Generalization of Supported Applications

3.4 Interfaces

All VACON® NX platform drives feature a uniform implementation of control board interfaces.

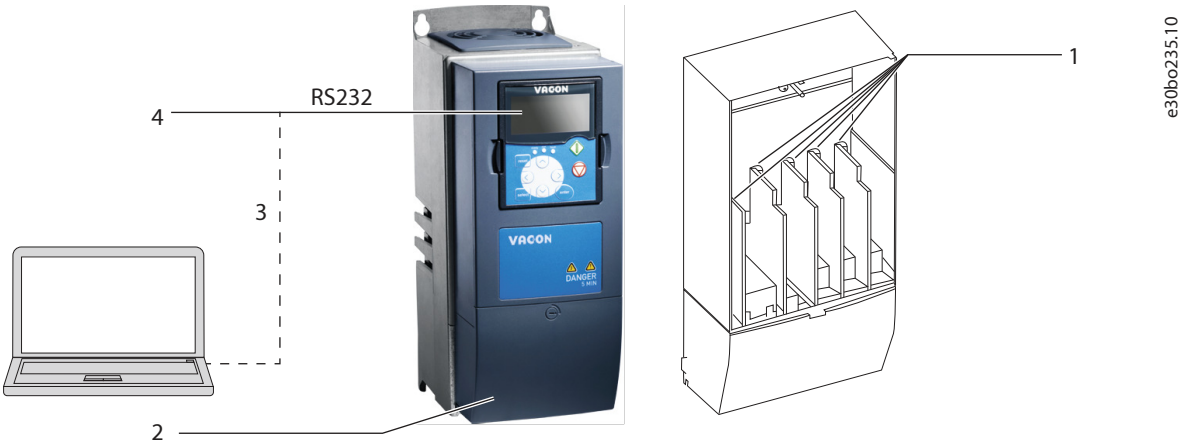


Figure 4: VACON® NX Interface Diagram

1	Option board slots A-E	2	Power connector
3	RS232 to USB	4	Control panel (detachable)

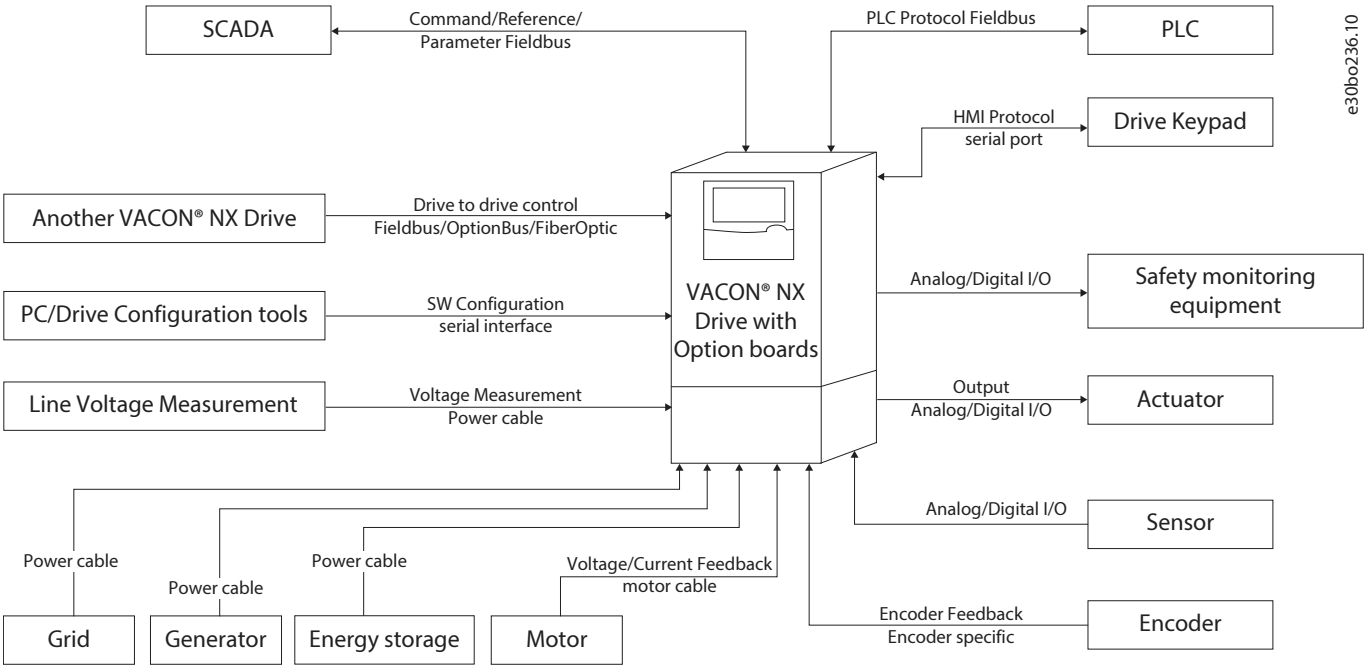


Figure 5: Generalized Connectivity of VACON® NX Drive

The control unit of a VACON® NX drive acts as the central hub for connectivity and system integration. It provides multiple interfaces that enable communication, control, and monitoring of the drive:

- Ethernet interfaces for fieldbus communication and integration with software tools, SCADA systems, and other industrial applications.
- Serial port connector for connecting a keypad/PC tool.
- Analog and digital inputs/outputs, together with a 24 V supply, for instrumentation and control purposes.
- Internal OptionBus, used to connect option boards directly to the control unit.

When using OPTD boards, multiple drives can be connected in a line via fiber optic connections. This enables reliable communication between multiple drives within the system.

The Internal and local interfaces include the local communication interfaces to other Danfoss products (Options/OptionBus/Keypad/Serial Port). The external and remote interfaces include the Ethernet and Fieldbus interfaces to customer systems, so that the communication may potentially span security boundaries. Lastly, instrumentation and control interfaces include the local 24 V supply, analog and digital I/O, encoder/resolver interface, grid voltage measurement via OPTD7 option board as well as motor interface.

3.5 Tools and Software for VACON® NX Products

Following tools and software are used to commission, manage, and operate VACON® NX drives.

- VACON® NCDrive
  - Tool for managing VACON® NX drives
  - Configuration
  - Monitoring
  - Security/audit logs
- VACON® NCLoad
  - Updating software packages in VACON® NX drives
- VACON® NCIPConfig
  - Configuring network related parameters for Ethernet option boards via the Ethernet connection
    - Board IP address and relevant parameters

Danfoss Drives Oy © 2026.11

    - PROFINET name of station
- VACON® Safe
    - Write a safety configuration to the safety board
- VACON® Loader
    - Used to update the software of specific option boards (OPTE, Advanced Safety Options)

3.6 Software and Firmware Updates

Keeping software up to date is one of the most effective ways to protect systems from known vulnerabilities and cyber threats. It is highly recommended to follow Danfoss security advisories and other provided and available information related to the latest firmware and software versions.

Find the latest firmware versions from: https://www.danfoss.com/en/service-and-support/downloads/dds/ac-drive-firmware/#tab-overview

Procedure to verify the downloaded packages:

1. Download the latest firmware packages directly from the Danfoss website to ensure accuracy.
2. Open PowerShell.exe
3. Replace the file path with the correct path. Write `Get-FileHash c:\nx\NXP00002V212.vcn` and press *Enter*
4. Compare the generated hash of the `.vcn` package against the hash value provided in the downloaded ZIP file to confirm integrity.

4 Security Features and Verification of Functionality

4.1 Identification of Security Capabilities

The following sections introduce the security features of the VACON® NX and how to verify that a feature is active and performing as expected.

To ensure that the firmware is certified to IEC 62443-4-2 Capability Security Level 1 (SL-C 1), identify the current version. See 1.2 Scope for information about correct firmware versions.

4.2 Security Parameters of VACON®NX Drives

When the security features of VACON® NX are enabled by setting the Administrator password, the following parameters can be modified. Detailed descriptions of the parameters functionality are provided in subsequent sections.

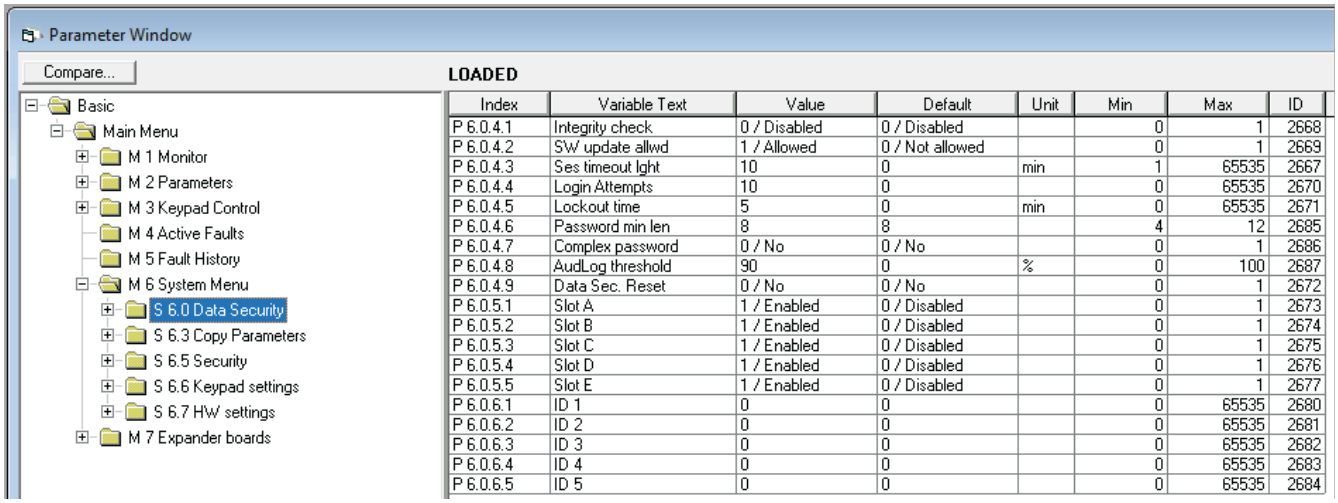


Figure 6: Security Parameters of a VACON® NX Drive

Table 4: Security Parameters of VACON® NX Drive

Parameter	Description	Refer section
P 6.0.4.1 Integrity check	If the boot integrity check is enabled	4.3.1 Secure Boot Overview
P 6.0.4.2 SW update allwd	Allow drive software to be updated	4.13 Update VACON® NX Firmware
P 6.0.4.3 Ses timeout lght	Delay until user is logged off (minutes)	4.6 Session Timeout
P 6.0.4.4 Login Attempts	How many unsuccessful login attempts are allowed before the cooldown process is triggered	4.5.11 Cooldown Period After Repeated Failed Logins
P 6.0.4.5 Lockout time	Time for cooldown period (seconds)	4.5.11 Cooldown Period After Repeated Failed Logins
P 6.0.4.6 Password min len	Minimum length of the password	4.5.6 Password Requirements
P 6.0.4.7 Complex password	Enable password complexity	4.5.6 Password Requirements
P 6.0.4.8 AudLog threshold	An alert is generated when the audit log usage exceeds the threshold	4.7 Audit Logging
P 6.0.4.9 Data Sec. Reset	Secure reset for drive	6.3 Secure Reset Function
P 6.0.5.1 Slot A to ***P 6.0.5.9 Slot E***	Status of the physical slots for option boards. Slots can be enabled/disabled via these parameters.	4.8 Disable Option Board Slots
P 6.0.6.1 ID 1 to ***P 6.0.6.5 ID 5***	The parameters which the Anonymous user is allowed to configure via Keypad.	4.5.13 Configuring Anonymous Access Rights and Keypad Settings

Danfoss Drives Oy © 2026.11

4.3 Secure Boot

4.3.1 Secure Boot Overview

On every power-up, the system verifies the integrity of the firmware, application, and all associated data. This verification occurs in a staged sequence where each stage validates the integrity of the next before the execution continues.

The secure boot with integrity protection can fail for various reasons. For instance, the firmware may be corrupted, tampered with, or partially unreadable due to flash memory wear or damage. If validation fails at any stage, or if the firmware cannot be started for any other reason, the control unit aborts the normal startup sequence and transitions into BOOT RECOVERY mode, provided that the control unit has a sufficiently recent firmware version (see 4.13 Update VACON® NX Firmware).

With older boot versions, a similar automatic transition to *BOOT RECOVERY* mode is not available. When the drive does not boot and the keypad display is either empty or shows only running lines, new firmware can be uploaded via VACON® NCLoad.

When a faster boot time of the drive is more critical than verifying the firmware integrity, it is possible to disable the boot time integrity check by setting the parameter ***P 6.0.4.1 Integrity check*** to *0/False*.

> IMPORTANT: This action disables the security control for verifying boot integrity and thus firmware integrity is not verified anymore. Danfoss recommends regularly rebooting the drive with the boot integrity check enabled to verify that the integrity of the drive firmware/software has not been compromised.

To configure:

- Login to VACON® NCDrive or keypad with Admin credentials.
- Go to the parameter group *System Menu > S 6.0 Data Security* set parameter ***P 6.0.4.1 Integrity check*** to correct value.

4.3.2 Secure Boot Recovery

In *BOOT RECOVERY* mode, new firmware can be installed onto the drive. The requirements for the firmware version depend on the drive configuration. In some cases, only firmware versions that include the cybersecurity functionalities (see 4.13 Update VACON® NX Firmware) are accepted. In other configurations, it is also possible to install older firmware versions.

The correct firmware version can be checked from the text shown in the keypad

- *RECOVERY*: Older firmware version can be installed.
- *RECOVERY CS*: Only a cybersecurity enabled firmware version can be installed. This mode is displayed when the Admin password has been set or an integrity check is enabled.

When the drive is in *BOOT RECOVERY* mode, a new firmware version can be installed normally using VACON® NCLoad. In this mode, the parameter ***P 6.0.4.2 SW update allwd*** has no effect.

4.4 Connectivity

VACON® NX drives include multiple different protocols and interfaces to allow communication with other systems and devices. These protocols do not include any modern encryption mechanisms due to historical reasons and the legacy of the VACON® NX product family.

The following list goes through various protocol types found in VACON® NX products.

- Serial communication: Typically, point-to-point communication. Since serial protocols do not support security, the cables should be secured physically to prevent eavesdropping or intrusion.
- Ethernet communication: Various fieldbuses are supported via the OPTE boards. The fieldbuses do not support secure communication and are intended only to be used on trusted local networks. If remote connectivity is required, secure technologies such as a VPN should be used. Depending on the risk assessment, it can be necessary to use additional network monitoring devices, firewalls, packet inspection, and so on, to monitor the insecure fieldbus communication on the network.

4.5 User Management

4.5.1 User Access and Configuration Management

VACON® NX supports user management using 2 predefined user accounts: Admin and Anonymous. Each user is assigned specific permissions and access capabilities. The Anonymous user account is applied when the user has not authenticated or logged in. The Admin user requires a login operation. Use the Anonymous account for normal operations and to edit specific parameters of the drive configuration, such as the control place. An anonymous user can change the keypad frequency reference, when the control place is set appropriately.

By default, there are no access restrictions, and the user accounts are not active. When a password is set for the predefined Admin user, the restrictions in Table 5 are enforced.

The maximum number of concurrent sessions depends on the available hardware configuration of the drive. There is one session per interface, which means that the keypad and VACON® NCDrive share the session if they are using the same interface for connectivity.

IMPORTANT: There is no resource locking mechanism on parameters or configurations. The fieldbus and multiple users can all have write access to the same parameters and are responsible for coordinating their changes. Write operations happen through a message bus/queue which means that the latest operation gets applied, if the same parameter is changed from different sessions.

Table 5: Users and Access Permissions

User	Purpose	Permissions
Anonymous	Limited access role with read-only permission	• Read parameter values • Read monitoring values • Use pre-defined basic functions • Can edit up to 5 parameters. The Admin configures the list of parameters. • Can stop the drive from the keypad unless an application disables the functionality.
Admin	Provides full access	• Access to all parameters, monitoring, and functions • Change parameters • Reset password

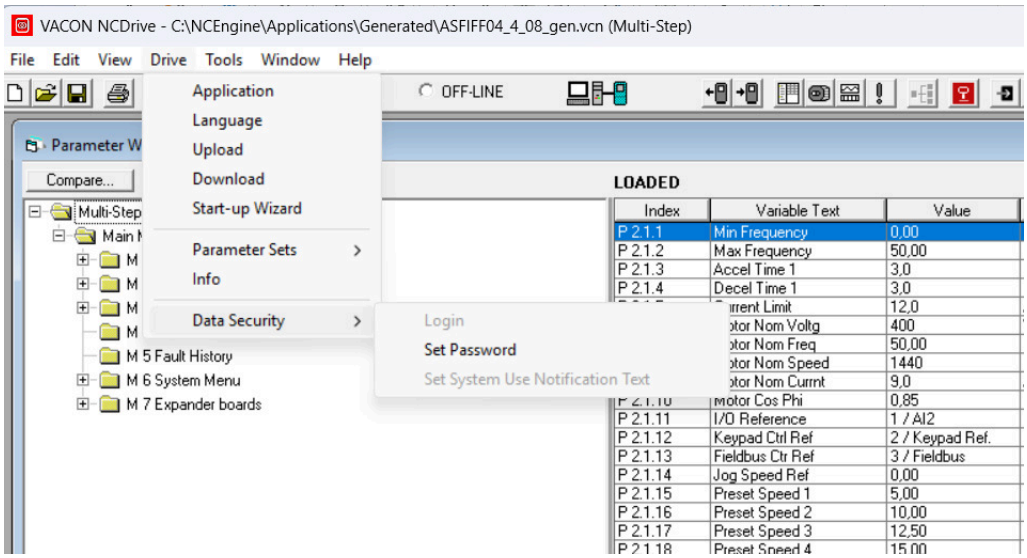
4.5.2 Setting-up Admin Password via VACON® NCDrive

The Admin password can be configured either through the keypad or via the VACON® NCDrive software. Once the password is set, it is required for logging into the Admin user in both the keypad interface and the VACON® NCDrive tool.

If the drive supports security features but they are not enabled, VACON® NCDrive has a *Set Password* menu field enabled.

1. Go to *Drive* > *Data Security* > *Set Password*.

Danfoss Drives Oy © 2026.11



e30bo238.10

Figure 7: VACON® NCDrive *Set Password* Menu Option

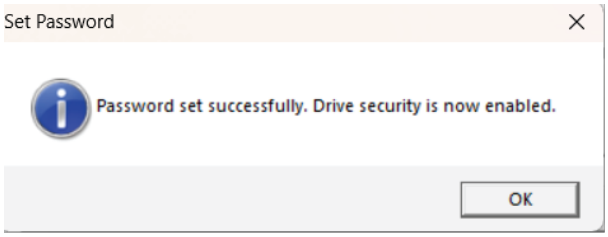
2. Set the new Admin password in the new password field. Enter the same password in the confirm password field and press *Set Password*.



e30bo239.10

Figure 8: Setting the Admin Password

3. A confirmation is displayed after the password is successfully set.



e30bo240.10

Figure 9: Password Set Confirmation

4.5.3 Setting-up Admin Password via Keypad

If a user attempts to log in before the Admin password is set, the keypad displays the Locked error.

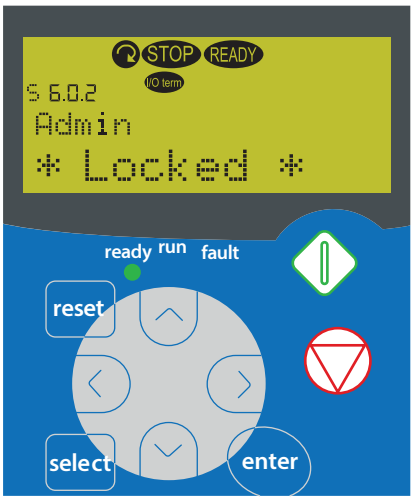


Figure 10: Accessing Log in Menu when Security Features are not Enabled

To set up *Admin* password via keypad:

1. Go to *System Menu* > *Data Security* > *Set password* > *Set Admin Passw.*.

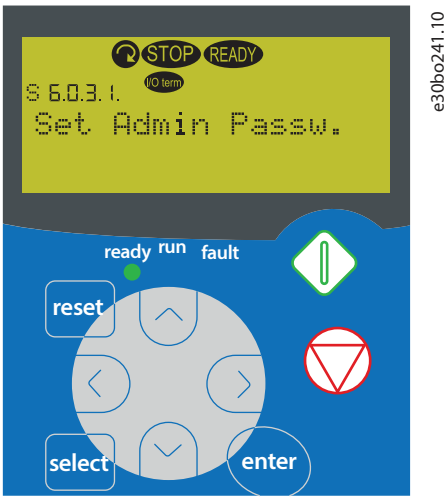


Figure 11: Menu to Set Admin Password

2. Press the right button to activate.
3. Use the [up arrow] and [down arrow] to set the password and press the [enter key].

   When setting the password, it is visible in the display so the user can verify it before proceeding.

Danfoss Drives Oy © 2026.11

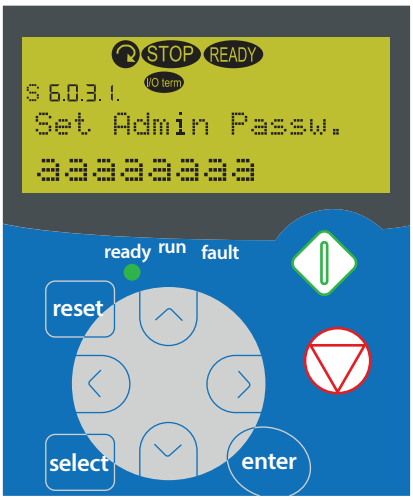


Figure 12: Admin Password Visibility

4. A confirmation is displayed after the password is successfully set.

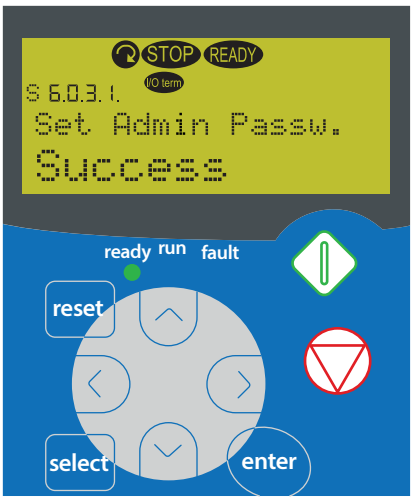


Figure 13: Set Admin Password Status

4.5.4 Changing Admin Password via VACON® NCDrive

The Admin password can be changed from the keypad and via VACON® NCDrive. Changing the password does not affect active sessions that are already authenticated. Active sessions can be terminated by closing them, or by power cycling the drive.

IMPORTANT: The option to change the password is only accessible when the user is logged in as the Admin.

Changing Admin password via VACON® NCDrive

To change Admin password via VACON® NCDrive, go to *Drive* > *Data Security* > *Change Password*.

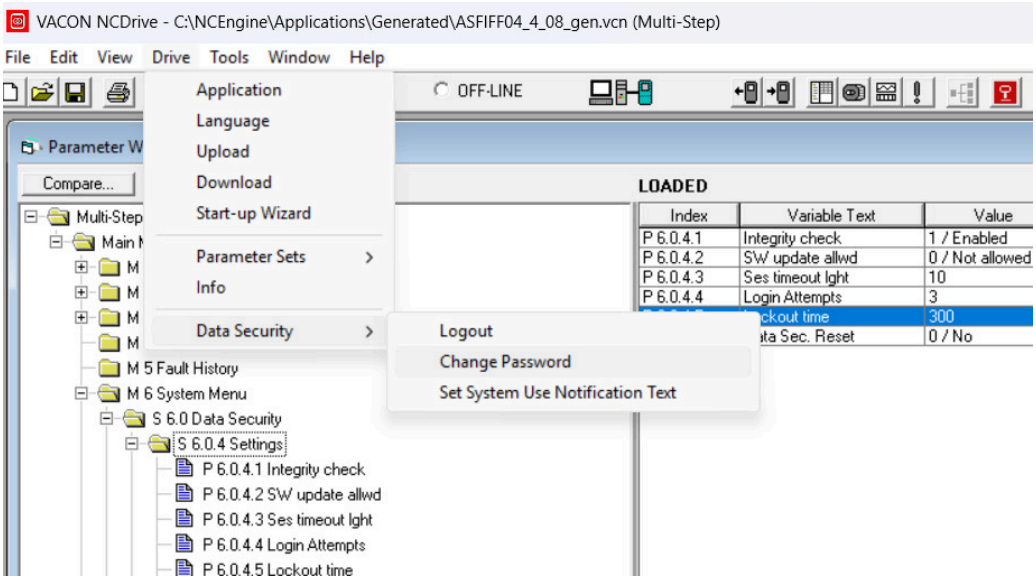


Figure 14: VACON® NCDrive Menu for Changing Admin Password

4.5.5 Changing Admin Password via Keypad

To change password via keypad, go to *System Menu* > *Data Security* > *Set Password* > *Set Admin Passw.*.

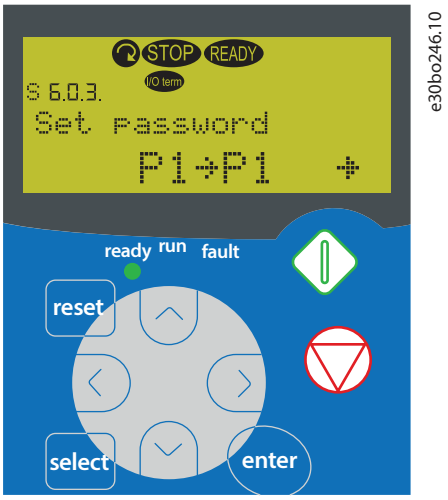


Figure 15: Changing Admin Password via Keypad

Danfoss Drives Oy © 2026.11

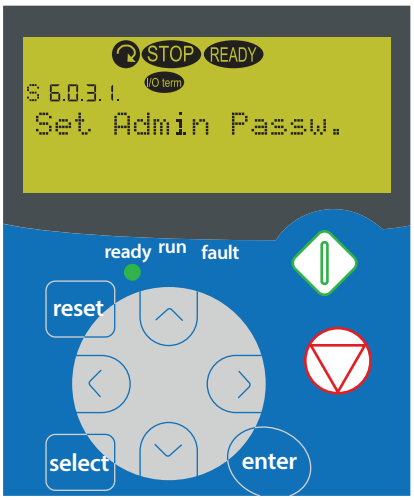


Figure 16: Setting Admin Password via Keypad

1. Confirm the feature by clicking [right arrow]. Using [up arrow] and [down arrow] select the input for the new password.

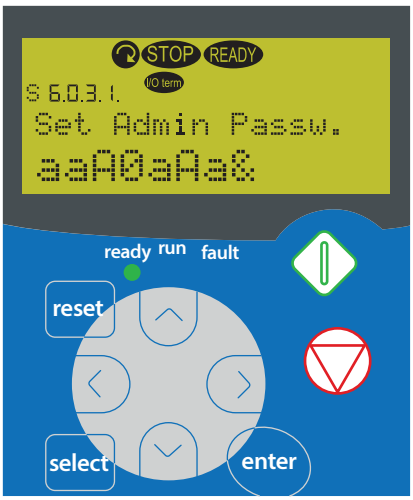


Figure 17: Example of Setting a Password through the Keypad

2. When a new password is set, press [enter key] to confirm.
3. The keypad displays a confirmation message.

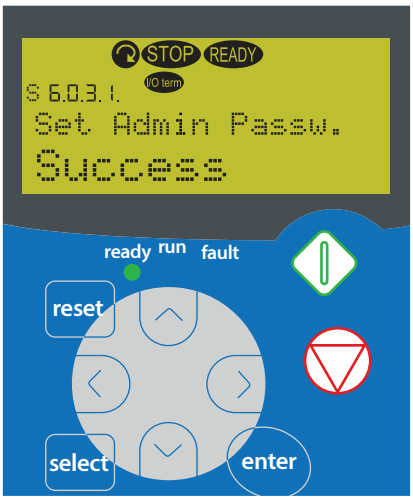


Figure 18: Confirmation Message

4.5.6 Password Requirements

The password requirements such as minimum length and complexity can be configured via parameters.

When the password complexity parameter is enabled, passwords must include characters from at least 3 different character sets:

- Lower case letters
- UPPER CASE letters
- Numbers
- Special characters

The minimum password length can be configured to be 4–12 characters, and the maximum password length is 12 characters.

To configure password requirements, log in to VACON® NCDrive or keypad with Admin credentials, go to the *parameter group System Menu > S 6.0 Data Security* and set the parameters ***P 6.0.4.6 Password min len*** and ***P 6.0.4.7 Complex password*** to the correct values.

4.5.7 Login via VACON® NCDrive

The Login function is available in the *Drive > Data Security* menu.

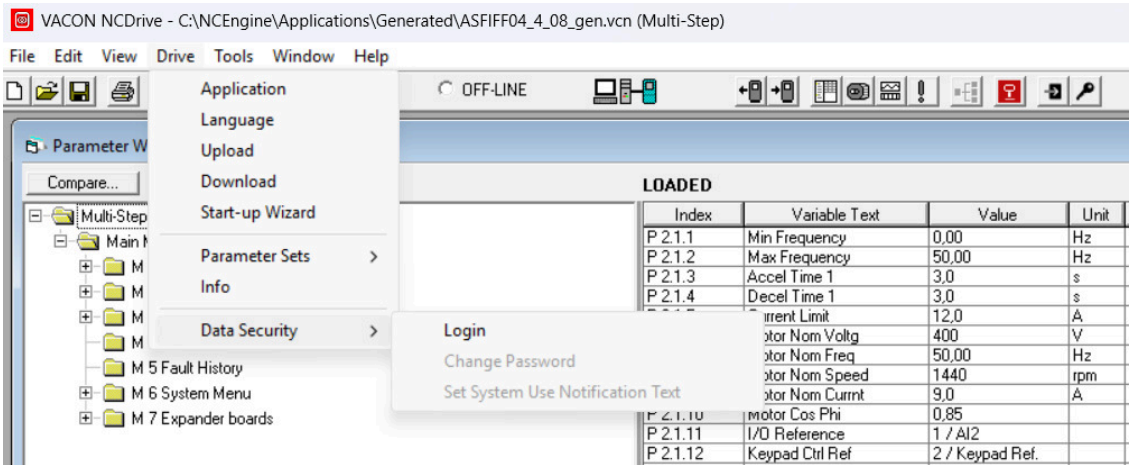


Figure 19: Login Menu

The Login menu item is visible when the user is Anonymous (not logged in). If the *System Use Notification Text* has been configured, it is displayed in the Login screen.



Figure 20: Login Screen with Example System Use Notification Text.

4.5.8 Login via Keypad

1. Navigate to System *Menu > Data security > Login as > Admin*

Danfoss Drives Oy © 2026.11

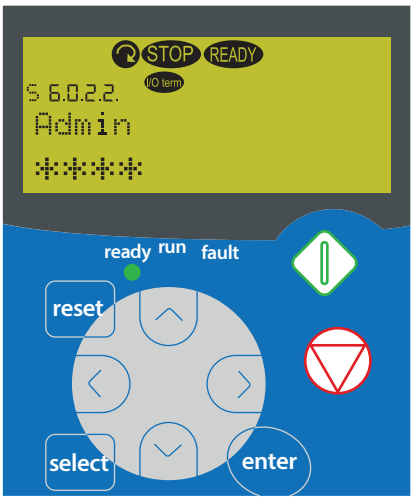


Figure 21: Login via Keypad

2. Press the [enter key] to confirm the action of entering the Admin password.
3. Press the [right arrow key] to confirm the input action and the input starts blinking.
4. Select the input using the [up arrow key] and press the [right arrow key] to advance to the next character.

   - *Lowercase letters*: Press the [up arrow key] to select the correct character and press the right arrow key to confirm.
   - *Uppercase letter*: Press the [select key] 2 times, then use the [up arrow key] to select the correct character and press the [right arrow key] to confirm.
   - *Numbers*: Press the [select key] 3 times, then use the [up arrow key] to select the correct number and press the [right arrow key] to confirm.
   - *Special characters*: Press the [select key] 4 times, then use the [up arrow key] to select the correct character and press the [right arrow key] to confirm.

5. When complete, press the [enter key] to confirm. A confirmation message is displayed after the password has been authenticated.

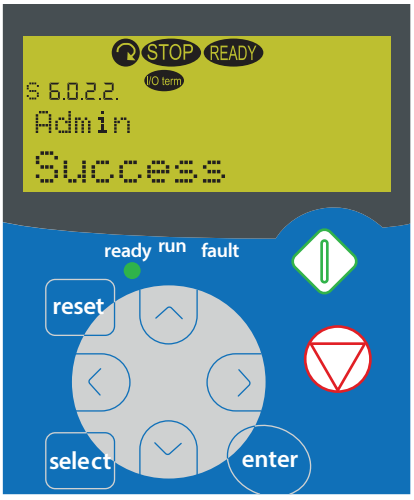


Figure 22: Successful Login Confirmation

4.5.9 Logout via VACON® NCDrive

To logout via VACON® NCDrive go to *Drive* > *Data Security* > *Logout*.

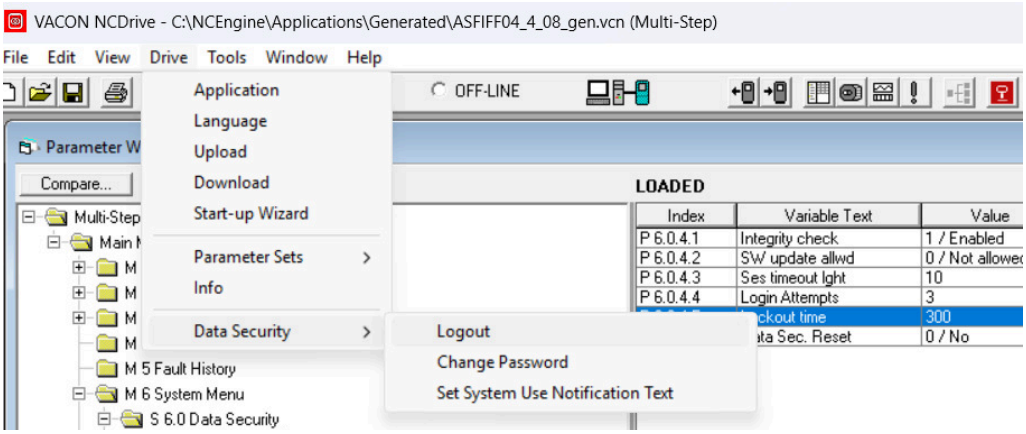


Figure 23: VACON® NCDrive Logout Menu

The user is logged out automatically after a time of inactivity See 4.6 Session Timeout.

4.5.10 Logout via Keypad

To logout via keypad, go to parameter ***P 6.0.2 Logout*** and select *Yes*.

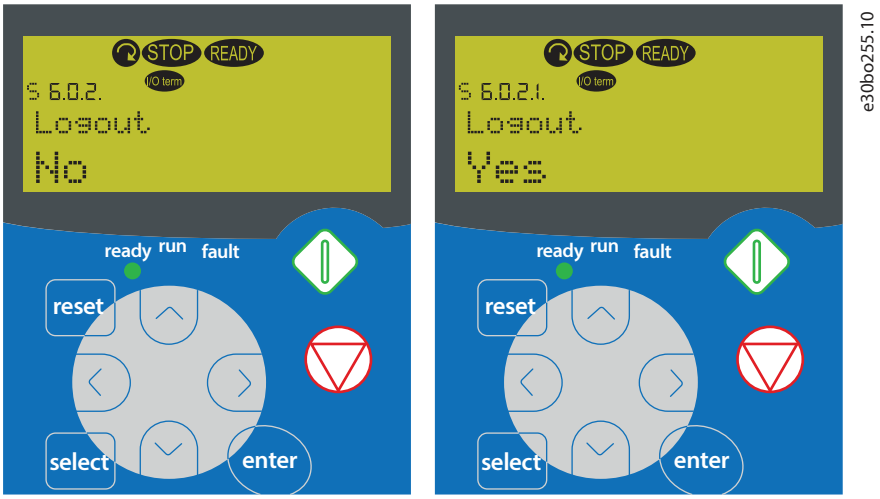


Figure 24: Keypad Logout Menu

The user is logged out automatically after a time of inactivity as described in 4.6 Session Timeout.

4.5.11 Cooldown Period After Repeated Failed Logins

To protect against brute-force credential attacks, the control unit denies login attempts after a threshold of consecutive failed login attempts is exceeded, as set in Parameter ***P 6.0.4.4 Login Attempts***. This activates a lockout time during which all login attempts are denied, even if they are valid. The control unit does not indicate to an attacker that the lockout is active.

It is recommended to set these values to reflect the risk profile of the system. Set the parameter ***P 6.0.4.5 Lockout time*** to the maximum amount of time that it is acceptable for legitimate users to be denied access to the drive. When the lockout timer expires, the ***P 6.0.4.4 Login Attempts*** counter is reset and the drive processes login attempts again.

Set the ***P 6.0.4.4 Login Attempts*** to a value where it is unlikely for legitimate users to accidentally trigger a lockout. The drive counts all failed login attempts from any interface towards the ***P 6.0.4.4 Login Attempts*** value to ensure that attackers do not gain additional attempts by using multiple interfaces or concurrent sessions. The counter is reset upon any successful login. Setting the ***P 6.0.4.4 Login Attempts*** value to *0* disables this function.

Power cycling the drive clears the lockout timer and the threshold counter.

Danfoss Drives Oy © 2026.11

To configure login to VACON® NCDrive or keypad with Admin credentials, go to the *parameter group System Menu > S 6.0 Data Security* and set the parameters ***P 6.0.4.4 Login Attempts*** and ***P 6.0.4.5 Lockout time***to the correct values.

4.5.12 System Use Notification

The system use notification is a configurable message that can be displayed on human user interfaces (keypad or PC tool) before authenticating to the drive. This can be used to provide critical security warnings and to warn that usage of the drive is monitored and unauthorized access is prohibited.

The maximum length of the text is 250 characters and characters from the ISO 8859-1 character set can be used.

IMPORTANT: Use the PC tool to configure the System Use Notification. The keypad does not support configuration and only displays the notification during login.

To configure System Use Notification on VACON® NCDrive:

1. Login into the drive. Go to *Drive > Data Security > Set System Use Notification text*

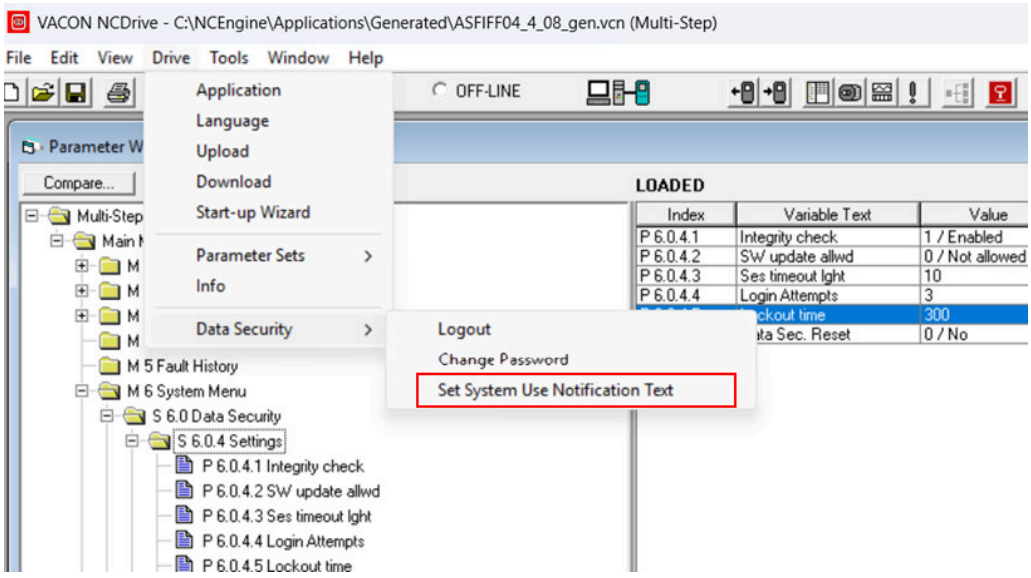


Figure 25: Menu to Set System Use Notification

2. Enter the message in the Set System Use Notification Message and press *Save* to confirm it.

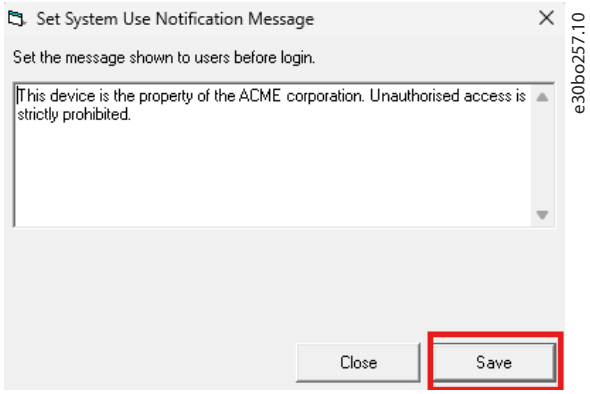


Figure 26: Set System Use Notification Message (Example)

3. The System Use Notification is displayed during login.

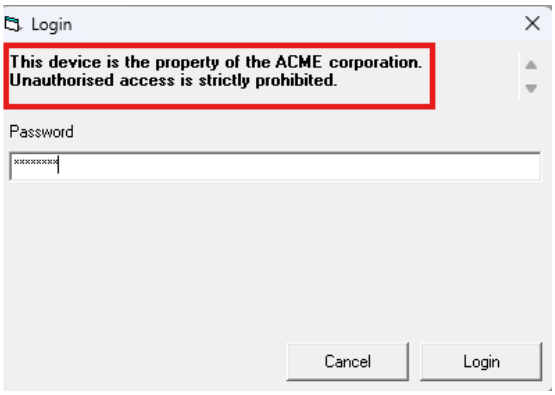


Figure 27: Example of System Use Notification on VACON® NCDrive



Figure 28: Example of System Use Notification on the Keypad

4.5.13 Configuring Anonymous Access Rights and Keypad Settings

An Anonymous user can be assigned access to 5 predefined parameters. The parameter values depend on the application in use. For example, in the Basic application, enabling parameters 125 (Control Place), 123 (Motor direction), and 114 (StopButtonActive) allows an Anonymous user to change the related parameters. The IDs shown in the following figures can be found in the application guide, for example, the Basic application is described in the *VACON® NX All-in-One* Application Guide. This guide is available on the Danfoss website.

Editing these parameters requires logging in to the Admin account as described in 4.5.2 Setting-up Admin Password via VACON® NCDrive.

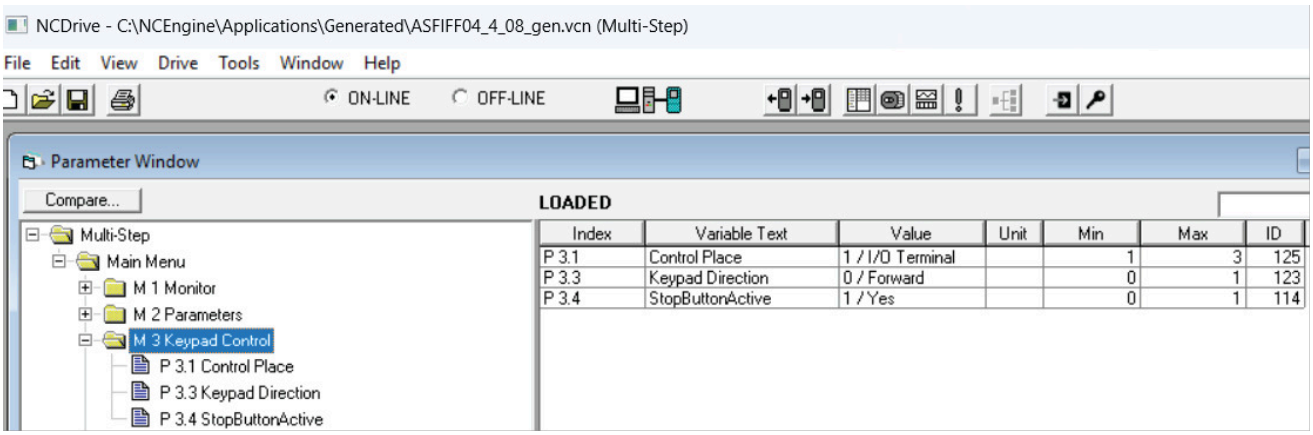
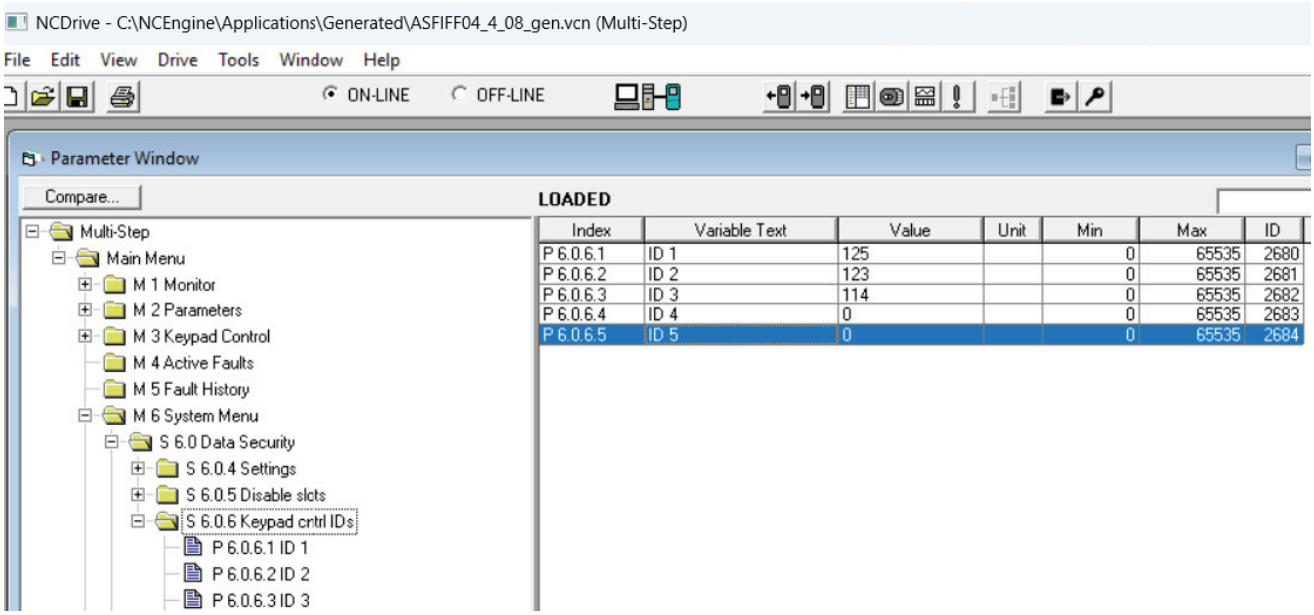


Figure 29: Keypad Customization Settings

Danfoss Drives Oy © 2026.11



e30bo261.10

Figure 30: Configuring Anonymous User Access to Parameters

4.6 Session Timeout

An Admin session can be automatically terminated after a configurable period of inactivity. The timeout is reset whenever there is human activity on an interface, for example, on the keypad a button must be pressed. Setting the timeout value to 0 disables the timeout.

The inactivity timer is related to the session, so if 2 sessions are connected simultaneously, automatic termination happens only to the session that exceeds the configured period of inactivity. It does not affect the other sessions.

VACON® NX drive functionality supports multiple concurrent sessions, one via each communication interface:

1. Keypad or VACON® NCDrive connected via the same interface
2. CAN (OPTD2/OPTD6 option board)
3. RS232 (OPTD3 option board)
4. Ethernet connection (OPTE option board)

> IMPORTANT: If VACON® NCDrive is closed when the session is active, the session remains active until the automatic session timeout is triggered.

To configure session timeout login to VACON® NCDrive or keypad with Admin credentials, go to the *parameter group System Menu* ***S 6.0 Data Security*** and set the ***P 6.0.4.3 Ses timeout lght*** parameter to the correct value.

4.7 Audit Logging

VACON® NX includes comprehensive audit logging capabilities. Audit logs can be accessed using the VACON® NCDrive tool.

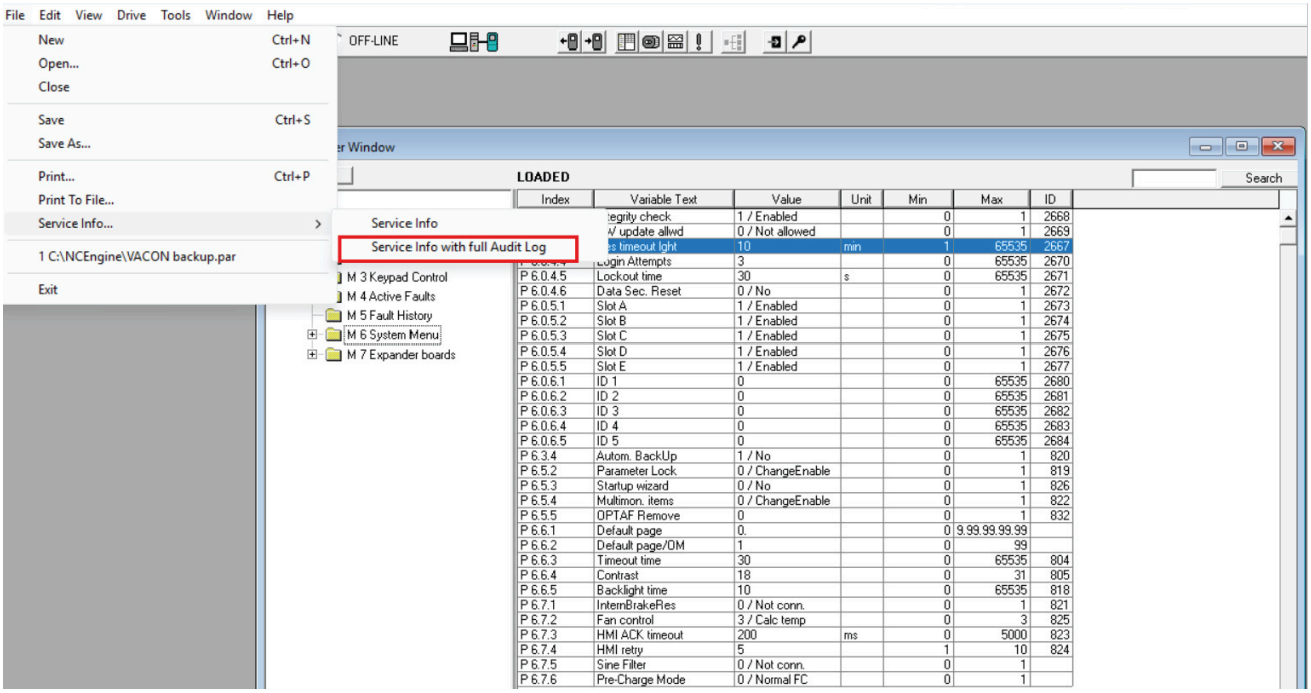
The audit log can store up to 2000 records and uses a ring buffer mechanism. When the storage capacity is reached, new entries automatically overwrite the oldest records.

The drive generates an alarm when the number of stored audit log records exceeds a configurable threshold, which is set to 90% by default. This alarm is displayed on both the keypad and in the VACON® NCDrive tool.

Unlike other alarms, the generated alarm does not automatically reset. The alarm can be cleared either from the keypad using the *Reset* button or via the *Fault List* in VACON® NCDrive.

To configure login to VACON® NCDrive or keypad with Admin credentials, navigate to the parameter group *System Menu S 6.0 > Data Security* and set the parameter ***P 6.0.4.8 AudLog threshold*** to the correct value.

To access the full audit login VACON® NCDrive, navigate to *File > Service Info > Service Info with full Audit Log*.



e30bo262.10

Figure 31: Audit Log in VACON® NCDrive

A log file opens the Service Info. Audit logs can be found at the bottom of the Service Info.

Danfoss Drives Oy © 2026.11

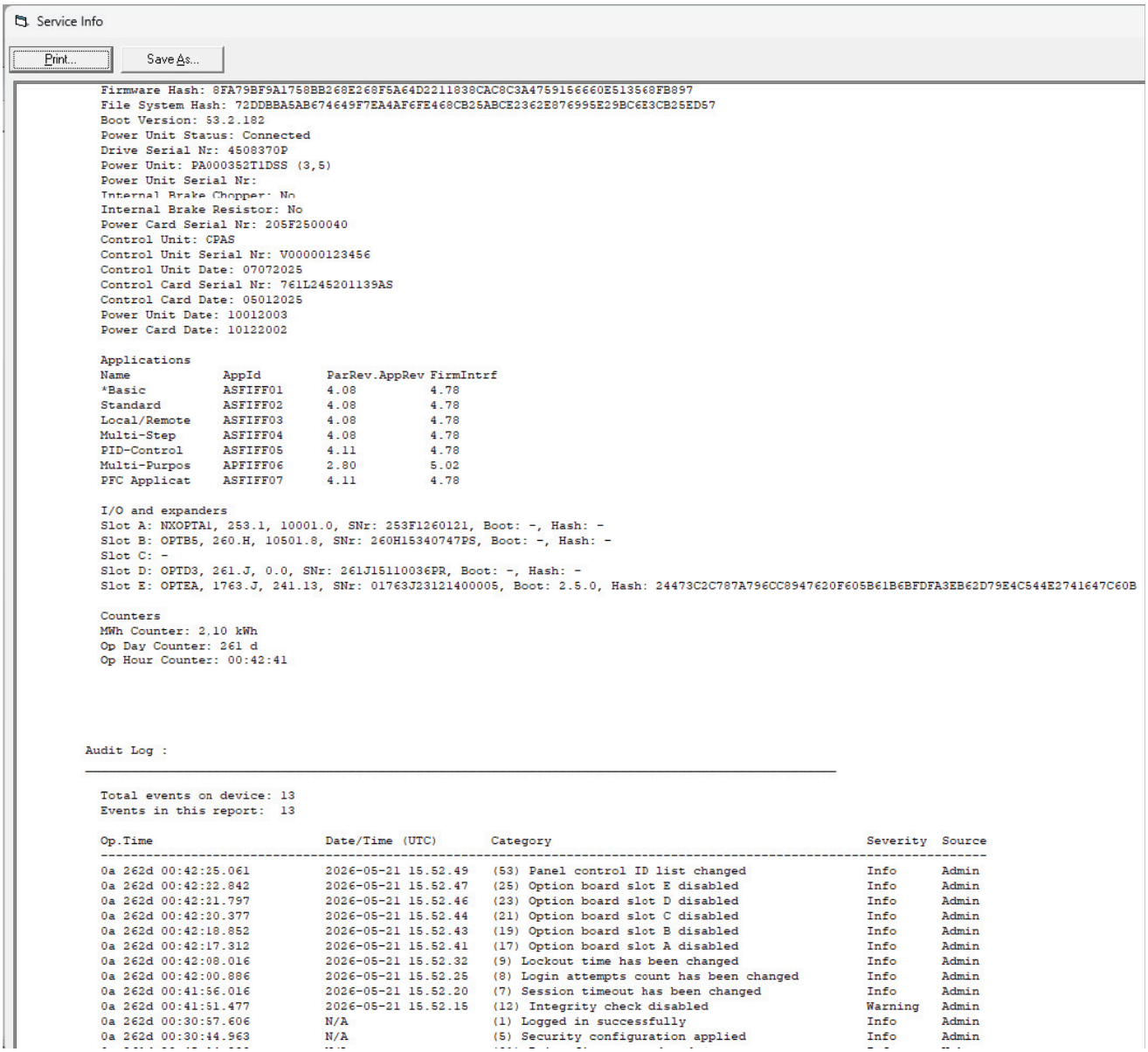


Figure 32: Service Info with Audit Log

Audit log messages contain the information shown in Table 6.

Table 6: Audit Log Message Structure

Column	Description
Timestamp	A millisecond counter that is saved over powerdowns
Unix time	Real date counter [1]
Category	Event category
Severity	Event severity
Source	Source for the log event

1) This has valid data only if real time has been set after the drive startup. Time can be set using SNTP via Ethernet option board or writing to a parameter with ID 2551 by a suitable fieldbus protocol.

4.8 Disable Option Board Slots

It is recommended to disable all unused option board installation slots, to mitigate physical attacks where someone would install a malicious/additional board to the drive. If there is an option board installed, but not used, it is recommended to disable the slot.

Option board slots can be enabled or disabled via parameters ***P 6.0.5.1 Slot A*** – ***P 6.0.5.5 Slot E***.

To configure login to VACON® NCDrive or keypad with Admin credentials, navigate to the *Parameter group System Menu > S 6.0 Data Security* and set the parameters ***P 6.0.5.1 Slot A***– ***P 6.0.5.5 Slot E*** to the correct value.

4.9 Physical Tamper Resistance and Detection

VACON® NX drive does not include built-in physical tamper-protection features. If the installation environment requires tamper resistance, place the drive in a securely locked area or enclosure appropriate for its size and other physical constraints.

4.10 Denial of Service Protection

Denial of Service (DoS) is a type of attack that attempts to make devices or network resources unavailable to its intended users. This is commonly done by sending a flood of messages to overwhelm the interfaces or services so they can no longer respond to legitimate requests.

When network traffic exceeds the resource limits of the VACON® NX drives, messages are dropped/rejected to ensure that essential functions continue to work. Some fieldbuses detect connection disruptions and cease operation and go to a failsafe state.

4.11 Control System Backup and Recovery

4.11.1 Control System Backup and Recovery Management

Backup and restoration of the VACON® NX configuration can be performed using multiple methods. The process varies depending on whether the Admin password has been set.

Backups can be made either via a PC tool or the keypad. When user management is active and the Admin password is set, the Anonymous user can make backups, but only the Admin user can restore a backup to the drive. The keypad can make a backup, but the security parameters are excluded. The VACON® NCDrive PC tool is required for a full backup that includes security parameters. The backup file created with NC Drive also contains the short Service Info, excluding the audit log. This Service info is described in 4.12 Device Component Inventory (Service Info).

Backups made from a drive with security features disabled can be restored to a drive with security features enabled by the Admin user. However, backups made from a drive with security features enabled cannot be restored to a drive where security features are disabled.

When making backups, it is recommended to power cycle the drive first, to clear temporary values and perform an integrity check, which helps to ensure consistency of all data. The integrity of data transfers between the drive and the PC is validated with CRC.

The integrity of backup files on a PC can be validated by following the steps:

1. Make a backup of the drive via the 4.11.2 Backup via VACON® NCDrive.
2. Use VACON® NCDrive to compare the values in the drive to the values stored in the backup file.
3. Calculate, for example, the SHA-256 hash (or use a similarly secure digest algorithm) of the file and store the result in a secure location.
4. Store the backup file in a secure location accessible only to authorized personnel.
5. Before restoring a backup file to a drive, verify that the hash of the file matches the stored value.

```
PS C:\> Get-FileHash C:\nx\backups\20260430.par

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          9296C52765A502FC11321ECB5E16022C7974581853679746C3A6A90CC7E7D6C3       C:\nx\backups\20260430.par
```

e30bo264.10

Figure 33: Example of Calculating SHA-256 Hash with PowerShell

Danfoss Drives Oy © 2026.11

4.11.2 Backup via VACON® NCDrive

To make a backup via VACON® NCDrive, select the disk icon on the home screen as shown in Figure 34. This performs the backup operation and saves the backup file to a selected path.

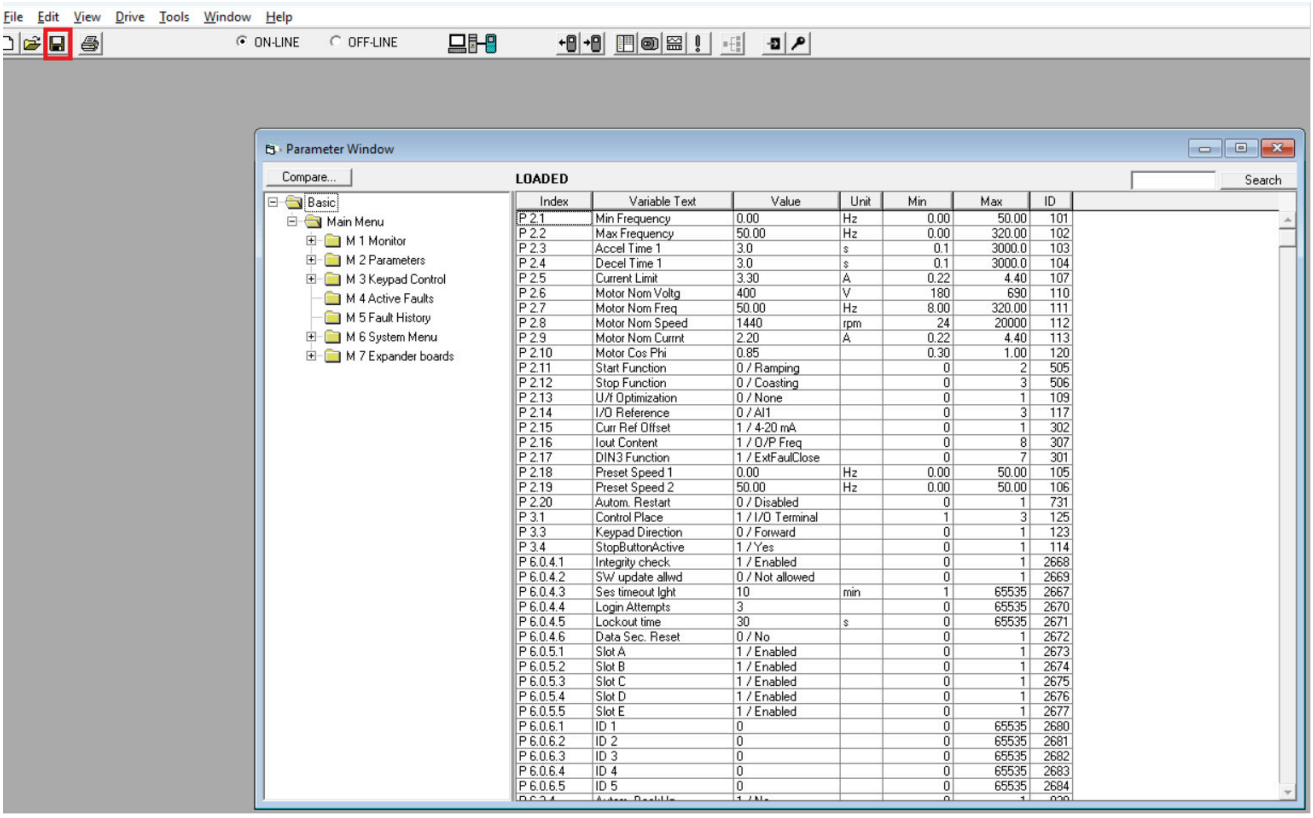


Figure 34: Backup via PC Tool, VACON® NCDrive

4.11.3 Backup via Keypad

To backup via the keypad, login as Admin. Go to *System Menu* > *Copy Parameters* > *Up to keypad* > *All param* > *All parameters* and press the *enter key*.

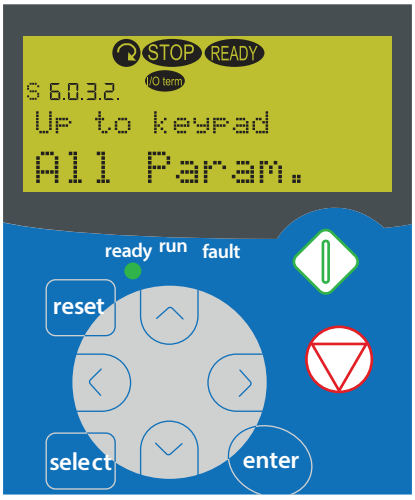


Figure 35: Backup via the Keypad

4.11.4 Automated Backup via VACON® NCDrive

To configure automatic backups login using admin credentials. Go to *System Menu* > ***P 6.3.4 Autom. BackUp*** and set the value to *Yes*.

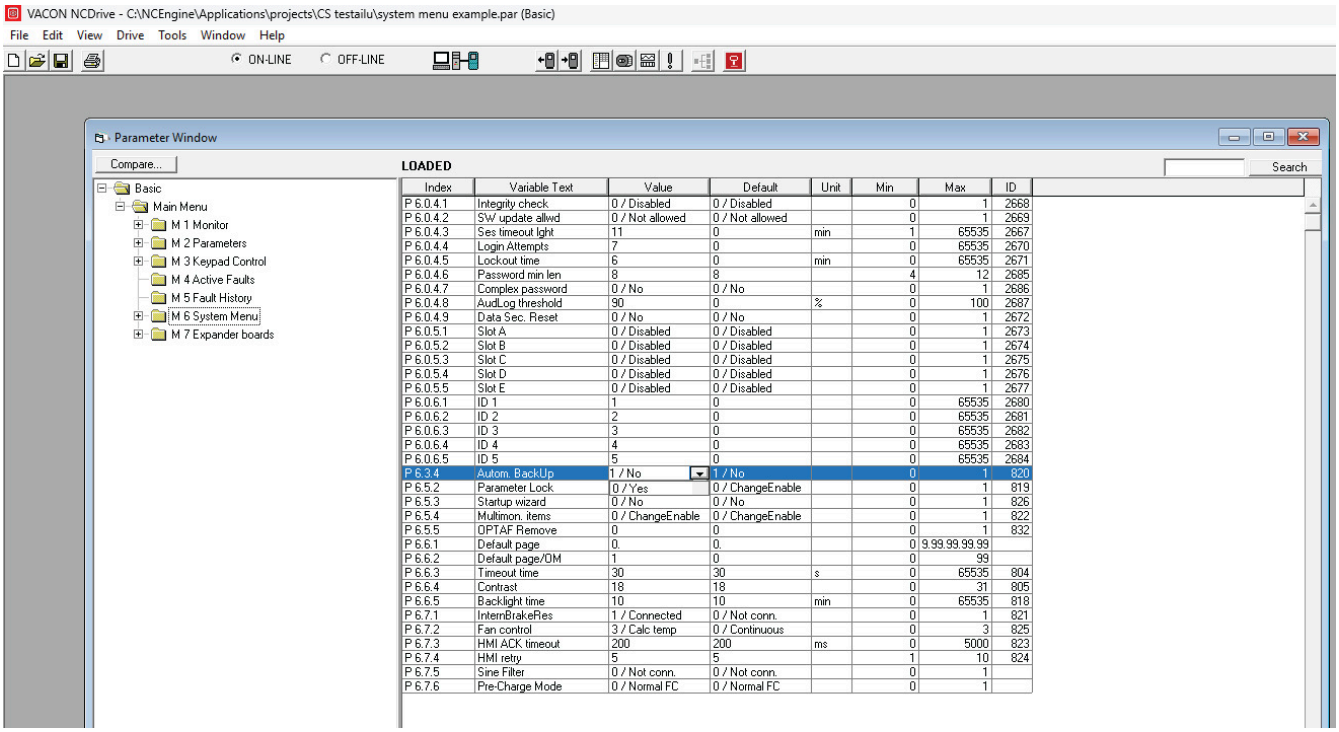


Figure 36: Setting the Automatic Backup via VACON® NCDrive

4.11.5 Automated Backup via Keypad

When active, every time a parameter is changed, the Keypad backup file is updated. To configure automatic backups on the keypad:

1. Login as Admin, go to *System Menu* > *Copy Parameters* > *Autom. BackUp.*

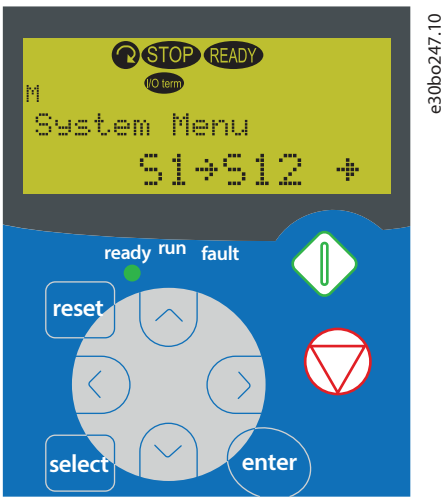


Figure 37: System Menu

Danfoss Drives Oy © 2026.11

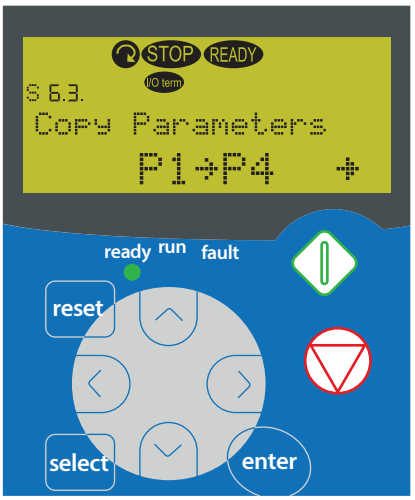


Figure 38: Copy Parameters

2. Set the value to *Yes*.

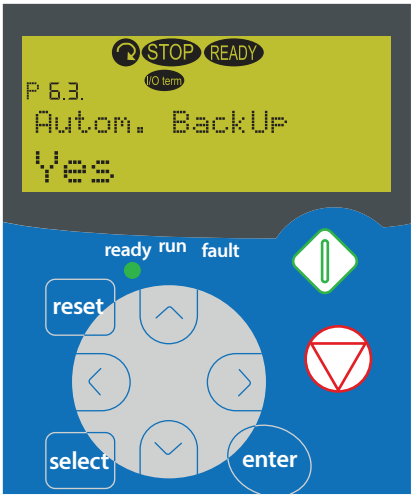


Figure 39: Automated Backup

3. A confirmation is displayed.

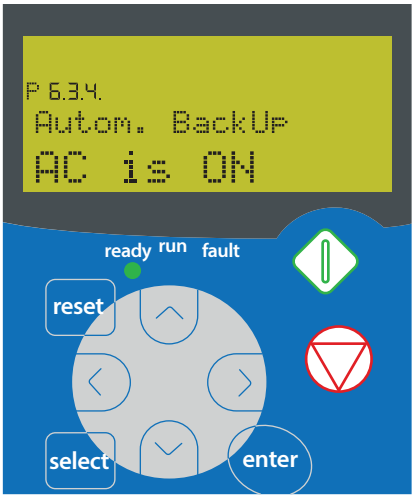
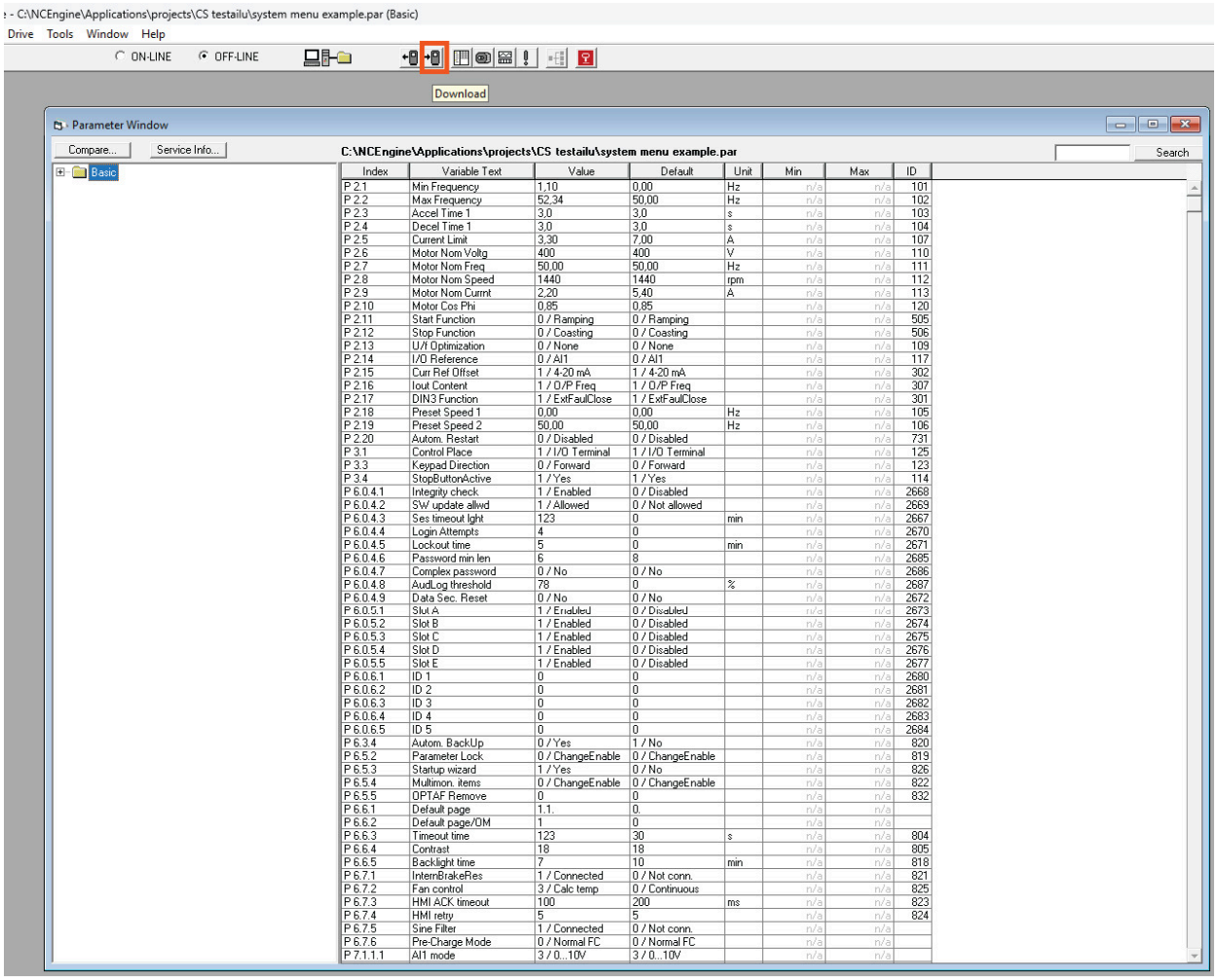


Figure 40: Automated Backup Confirmation

4.11.6 Restore Backups via VACON® NCDrive

To restore a backup via VACON® NCDrive

1. Log in as Admin on the drive and open the backup parameter file.
2. The icon with an arrow going towards the drive as highlighted in Figure 41.



e30bo272.10

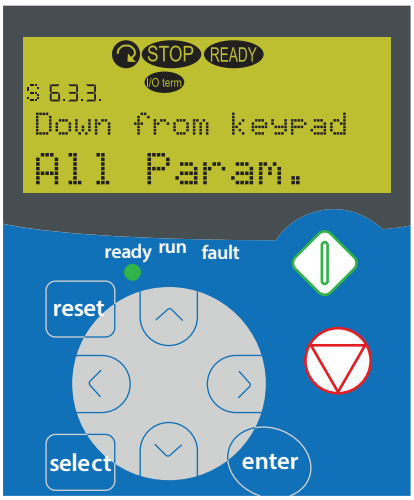
Figure 41: Restoring a Backup via VACON® NCDrive

Figure 41 shows an updated window with restored parameters.

4.11.7 Restore Backups via Keypad

To restore a backup via keypad, log in as Admin user. Go to *System Menu* > *Copy Parameters* > *Down from keypad* > *All param.* select *All parameters* and press the [enter key].

Danfoss Drives Oy © 2026.11



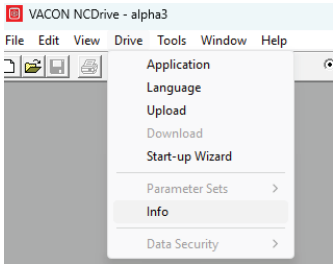
e30bo273.10

Figure 42: Restore a Backup from the Keypad

4.12 Device Component Inventory (Service Info)

VACON® NX supports viewing component inventory, which is a list of versions of internal components. These can be compared to a list of expected versions, for example for purposes of audit, certification, or to check if updates are required.

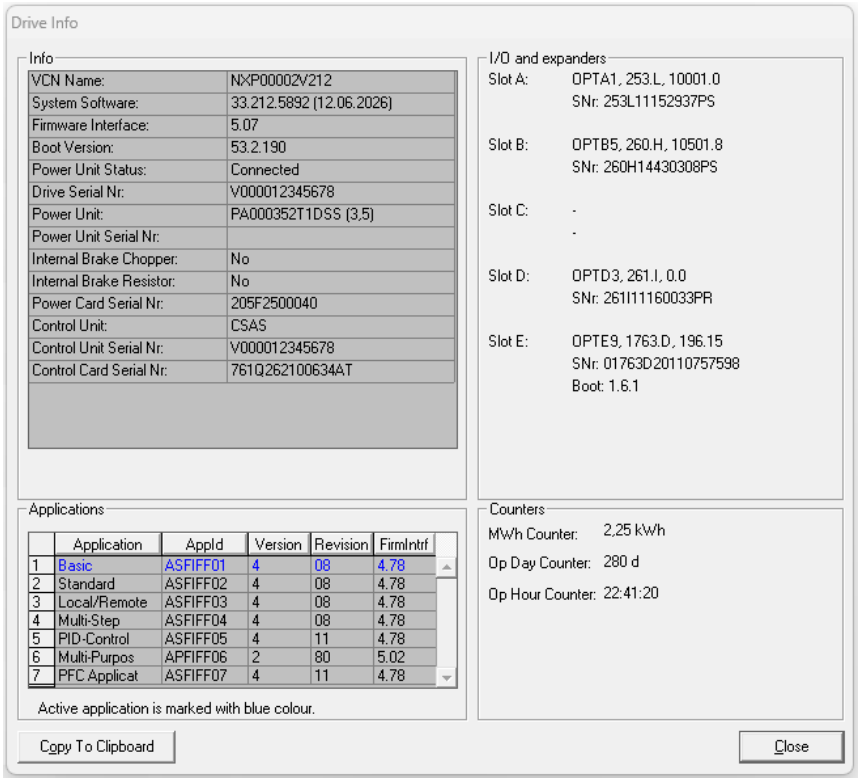
VACON® NCDrive shows the hardware and firmware related information in two different locations. They can be found either via Drive Info (Figure 43) or Service Info (Figure 45) options.



e30bo274.10

Figure 43: Drive Info Menu

The Drive Info is a single info window that can be inspected and copied to the clipboard for storing.



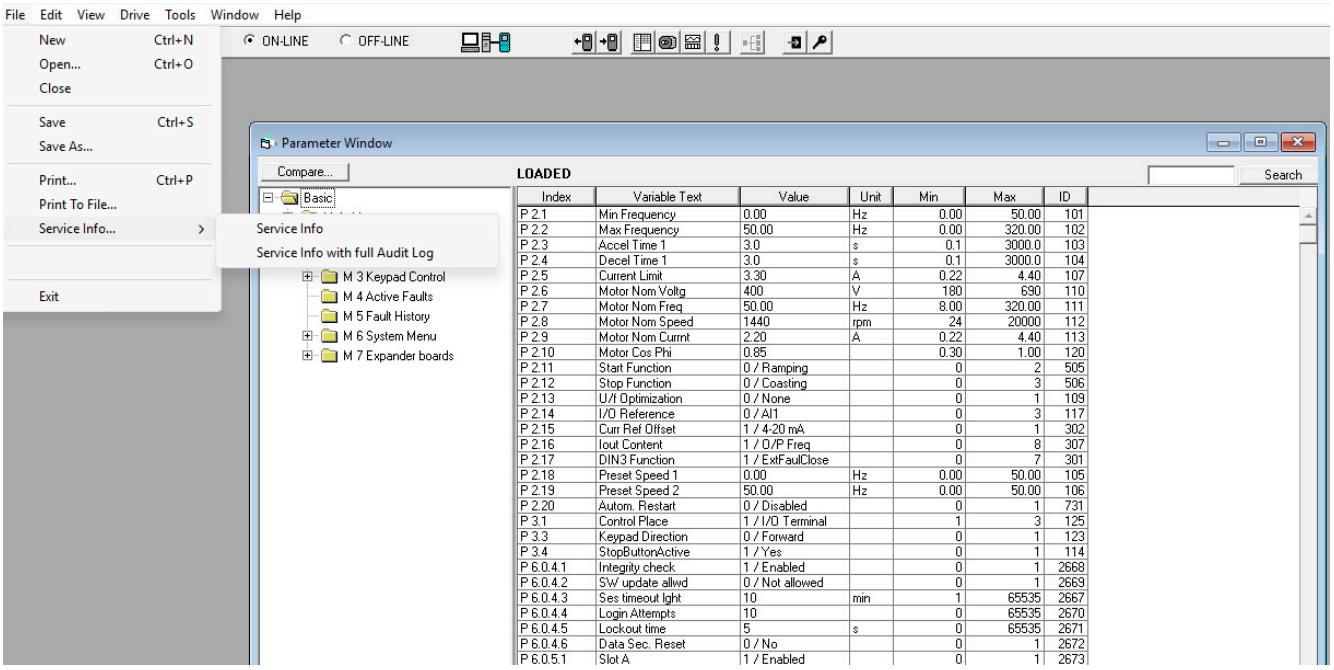
e30bo275.10

Figure 44: Example of Drive Info Output

The Service Info is a text-based output which is also used for debugging purposes and must be delivered to Danfoss support if a support case is opened. There are 2 levels of Service Info output: the regular short *Service info without audit log* (Figure 46) and long *Service info with full audit log* included, see Figure 32 in section 4.7 Audit Logging.

The long *Service Info with full Audit Log* may contain sensitive information, so for purposes of component inventory monitoring or support requests, the short Service Info is sufficient.

The Service Info can be retrieved via the *File* > *Service Info* menu item and selecting the correct version from the menu



e30bo276.10

Figure 45: Service Info Menu

Danfoss Drives Oy © 2026.11

```
Serialnumber:       11174043
Device:             NXP
System software:    NXP00CS4V212 (33.212.5821)
Firmware:           5.06
Application:        Basic (xxxxxxxx.vcn, ASFIFF01 4.08)
Parameter file:     Not Saved
```

Index	Text	Value	Unit	Min	Max	ID
P 2.1	Min Frequency	0.00	Hz	0.00	50.00	101
P 2.2	Max Frequency	50.00	Hz	0.00	320.00	102
P 2.3	Accel Time 1	3.0	s	0.1	3000.0	103
P 2.4	Decel Time 1	3.0	s	0.1	3000.0	104
P 2.5	Current Limit	3.30	A	0.22	4.40	107
P 2.6	Motor Nom Voltg	400	V	180	690	110
P 2.7	Motor Nom Freq	50.00	Hz	8.00	320.00	111
P 2.8	Motor Nom Speed	1440	rpm	24	20000	112
P 2.9	Motor Nom Currnt	2.20	A	0.22	4.40	113
P 2.10	Motor Cos Phi	0.85		0.30	1.00	120
P 2.11	Start Function	0 / Ramping		0	2	505
P 2.12	Stop Function	0 / Coasting		0	3	506
P 2.13	U/f Optimization	0 / None		0	1	109
P 2.14	I/O Reference	0 / AI1		0	3	117
P 2.15	Curr Ref Offset	1 / 4-20 mA		0	1	302
P 2.16	Iout Content	1 / O/P Freq		0	8	307
P 2.17	DIN3 Function	1 / ExtFaulClose		0	7	301
P 2.18	Preset Speed 1	0.00	Hz	0.00	50.00	105
P 2.19	Preset Speed 2	50.00	Hz	0.00	50.00	106
P 2.20	Autom. Restart	0 / Disabled		0	1	731
P 3.1	Control Place	1 / I/O Terminal		1	3	125
P 3.3	Keypad Direction	0 / Forward		0	1	123
P 3.4	StopButtonActive	1 / Yes		0	1	114
P 6.0.4.1	Integrity check	1 / Enabled		0	1	2668
P 6.0.4.2	SW update allwd	0 / Not allowed		0	1	2669
P 6.0.4.3	Ses timeout lght	10	min	1	65535	2667
P 6.0.4.4	Login Attempts	10		0	65535	2670
P 6.0.4.5	Lockout time	5	s	0	65535	2671
P 6.0.4.6	Data Sec. Reset	0 / No		0	1	2672
P 6.0.5.1	Slot A	1 / Enabled		0	1	2673
P 6.0.5.2	Slot B	1 / Enabled		0	1	2674
P 6.0.5.3	Slot C	1 / Enabled		0	1	2675
P 6.0.5.4	Slot D	1 / Enabled		0	1	2676
P 6.0.5.5	Slot E	1 / Enabled		0	1	2677
P 6.0.6.1	ID 1	0		0	65535	2680
P 6.0.6.2	ID 2	0		0	65535	2681
P 6.0.6.3	ID 3	0		0	65535	2682
P 6.0.6.4	ID 4	0		0	65535	2683
P 6.0.6.5	ID 5	0		0	65535	2684
P 6.3.4	Autom. BackUp	0 / Yes		0	1	820
P 6.5.2	Parameter Lock	0 / ChangeEnable		0	1	819

Figure 46: Example of Service Info Output

4.13 Update VACON® NX Firmware

Updating the firmware of VACON® NX drives is described in their specific guides as the procedure can vary. Refer to chapter 3.6 Software and Firmware Updates.

When the Admin password is set, the firmware/application update feature is access controlled via the configuration parameter ***P 6.0.4.2 SW update allwd***. If this parameter is set to *0/Not allowed*, firmware/application update cannot be performed. It must be set to *1/Allowed* before performing a firmware/application update. This parameter resets to *0/Not allowed* during a power cycle.

IMPORTANT: The ***P 6.0.4.2 SW update allwd*** parameter is changed from *1/Allowed* to *0/Not allowed* when the Admin password is set.

To configure login to VACON® NCDrive or keypad with Admin credentials, go to the parameter group *System Menu > S 6.0 Data Security* and set the ***P 6.0.4.2 SW update allwd*** parameter value to *1/Allowed*.

After this, the usual update procedure for the drive can be followed according to the guide.

Sometimes, it is be necessary to install older firmware on a drive which has cybersecurity features enabled. As older firmware does not support security features, the following process must be followed to make firmware downgrades possible.

1. Log in with Admin credentials.
2. Perform a secure reset. See section 6.3 Secure Reset Function
3. Power cycle the drive.
4. Perform a normal software update using the older firmware version.

Danfoss Drives Oy © 2026.11

5 Security Configuration Guidelines

5.1 Overview

There are several common methods for improving the security of a system, also known as security hardening guidelines. This chapter presents some general examples or recommendations, but it is ultimately the responsibility of the user to evaluate which techniques or mitigations are relevant to their environment and application.

5.2 General Principles

5.2.1 General Security Principles

The following list provides examples of general principles for system hardening. Some of these principles are described in more detail in the subsequent chapters.

Restrict physical access

Place the drive in a physically secure area, or in a physically secure enclosure. Ensure that only authorized personnel have access.

Restrict network access

Monitor and restrict data transmitted to and from the drive on networks and interfaces.

Reduce the attack surface

Turn off and disable unused ports, interfaces, services, protocols, applications, features, and other functionality that is not necessary for the correct operation of the device.

Set up user management and access control

Enable human user interfaces to distinguish between authorized and unauthorized personnel by setting up authentication and access control.

Perform regular maintenance

Monitor logs regularly or automatically to detect irregularities. Keep the device up to date with the newest software versions. Perform regular backups and restore operations as part of business continuity policies. Follow the Danfoss website for news bulletins and disclosures on vulnerabilities.

Create a threat model of the system

Assess the threats against the system in which the VACON® NX is a component. Examine the unmitigated risks that are identified in this chapter and deploy compensating countermeasures in the system as needed.

5.2.2 Restrict Physical Access

The VACON® NX drives are intended to be installed either in a physically secure enclosure, such as a lockable control cabinet, or in a physically secure area, such as a switching room or access-controlled area. Protect the device and its control interfaces against physical access by unauthorized personnel.

For additional physical protection, cabinet opening mechanisms can be connected to grid power to ensure that the device is electrically shut off if the enclosure is opened.

The keypad can be removed, and the device interfaces must be protected to prevent unauthorized access. For service cases, the keypad port can be used for PC tool connectivity, or a control panel can be given to trusted personnel.

5.2.3 Restrict Network Access

Organize communication networks according to security best practice guidelines using techniques such as network segregation, virtual networks, or deep packet inspection.

Ensure that Operational Technology (OT) and Information Technology (IT) networks are separated, and only exchange data in controlled and restricted manners. The IEC 62443 standard uses the “Zone” and “Conduit” concepts to organize network communication.

The VACON® NX drives are intended to be used only on trusted networks, meaning subnets that are monitored and preferably also physical access restricted. The drives are not suitable for connecting to untrusted networks such as the Internet, without additional compensating countermeasures.

Most industrial fieldbus technologies and IP services do not support security features. They are to be connected to a trusted subnet that is monitored, restricted, and isolated.

Fieldbus communication based on serial protocols has no security features and rely on the physical security of the wires. These are usually point-to-point or bus topologies and visual inspection can be used to verify the integrity of the connections.

5.2.4 Reduce the Attack Surface

5.2.4.1 Reducing System Attack Surface

To reduce risk, minimize the number of services or interfaces that accept commands. This reduces the attack surface.

Disable all services, ports, and features on the drive that are not necessary for the operational function of the system. Some services are enabled by default or are enabled due to configuration selections that depend on them.

With OPTEA and OPTE9 option boards, it is possible to disable unused physical ports and communication protocols. Similarly, unused expansion slots (A, B, C, D, and E) can be disabled as described in section 4.8 Disable Option Board Slots. It is recommended to enable only the functionalities required for the system.

The OPTEA or OPTE9 option board enables DHCP by default. If a DHCP server is not available, the drive assigns a link-local IP address. The board also enables Address Conflict Detection (ACD) by default, an ARP feature that prevents devices from using the same IP address. Some Fieldbus protocols, such as PROFINET, may automatically disable this feature.

When enabling a fieldbus protocol, like PROFINET, the user automatically enables multiple other protocols used in its environments. For PROFINET, the protocols are LLDP, DCP, and RPC. Some of these can be disabled with option board’s ***P 7.5.1.4.15 IP Port Filter*** parameter.

Table 7: List of Services, Ports, and Interfaces

Service/Port/Interface	Port(s)	Default setting	Can be disabled
DHCP	UDP 67, 68	Enabled	Yes, user can select from DHCP, DCP, or fixed IP
SNTP	UDP 123	Disabled	Yes
Drive discovery	UDP 65380	Enabled	Yes
HMI	UDP 65390, 65391	Enabled	Yes
ARP	-	Enabled	No
ICMP	-	Enabled	Yes
IGMP	-	Enabled	No
SNMP v2	UDP 161	Enabled	Yes
TFTP	UDP 69	Disabled	Available on OPTEA option board. Only open when PROFINET is used and the board is in OPTCx mode. OPTCx mode is described in the User guide VACON® OPTEA/OPTE9 Ethernet Board manual.
Ethernet based Fieldbus protocols (PROFINET, EtherNet/IP)	Multiple	Enabled	Yes, multiprotocol board, user can select one or disable

Danfoss Drives Oy © 2026.11

Table 7: List of Services, Ports, and Interfaces - (continued)

Service/Port/Interface	Port(s)	Default setting	Can be disabled
Modbus TCP	TCP 502	Enabled, when Modbus selected	Yes
Modbus UDP	UDP 502	Enabled, when Modbus is selected	Yes
DLR	-	Enabled, when PROFINET is selected	Yes
MRP	-	Enabled, when PROFINET is selected	Yes
LLDP	-	Enabled, when PROFINET is selected	Yes
DCP	-	Enabled, when PROFINET is selected	Yes
RSTP	-	Enabled	No
EtherCAT Fieldbus	-	Enabled	No. Option board can be physically removed or slot for the specific option board disabled via VACON® NCDrive.
Ethernet over EtherCAT	-	Disabled	Yes
Other Fieldbus protocols, for example, RS485	-	Enabled	Option board can be physically removed or slot for the specific option board disabled via VACON® NCDrive.
Physical Ethernet ports (1 and 2)	-	Enabled	Yes
Control serial port	-	Enabled	No

5.2.4.2 Disabling PC-Tool Connectivity from OPTEA/OPTE9 Cards

If a VACON® NX drive is equipped with OPTEA or OPTE9 option boards, it is possible to establish an Ethernet connection to the drive from various VACON® PC tools. This Ethernet communication protocol does not provide integrity, authenticity, or confidentiality protections and operates as a plaintext connection. If user management is active and this connection is used, the Admin password is sent in plaintext over the network and can be eavesdropped upon.

It is recommended to disable this connection service when it is not in use, and to ensure that the network is trusted and monitored before using the service.

The PC tool connectivity via the OPTEA/OPTE9 option boards can be disabled through the keypad.

Select *Expander boards* > *OPTEA/OPTE9* > *Parameters* > *IP Settings* > *Drive PC Tool* and set the value to *Disabled*. See Figure 47 and Table 8



Figure 47: Disable PC Tool Ethernet Access via the Keypad

Table 8: Values for Parameter VACON® PC Tool

Value	Name	
1	Full	Default value. Allows VACON® Live, VACON® Loader, VACON®NCDrive, or other VACON® PC tool access.
2	Configuration	Disables VACON® Loader access. Allows connections from VACON® configuration tools.
3	Disabled	Disables access from Ethernet for all VACON® PC tools.

5.2.4.3 Disabling SNMP Functionality

OPTE series option boards include SNMPv2 functionality with hard-coded community name. SNMP functionality is needed in PROFINET networks for device identification purposes.

If SNMP is not needed or is needed only during commissioning, the recommendation is to disable it from the NX configuration for more secure drive operations.

Figure 48 shows the location of this parameter. It is a bit mask for various port functions, and the full table for these functions can be found from 'VACON® OPTEA/OPTE9 Ethernet Board User Guide'. Set a specific bit to disable the corresponding function on the option board. Create the required bitmask manually and then convert it to a decimal value. The following description applies only to disabling SNMP. To disable additional functionality, refer to the 'VACON® OPTEA/OPTE9 Ethernet Board User Guide'.

To disable SNMP, enter number 2 to this field.

It is number 2, because bit 1 is for SNMP, and when converting 01 to decimal, the result is 2.

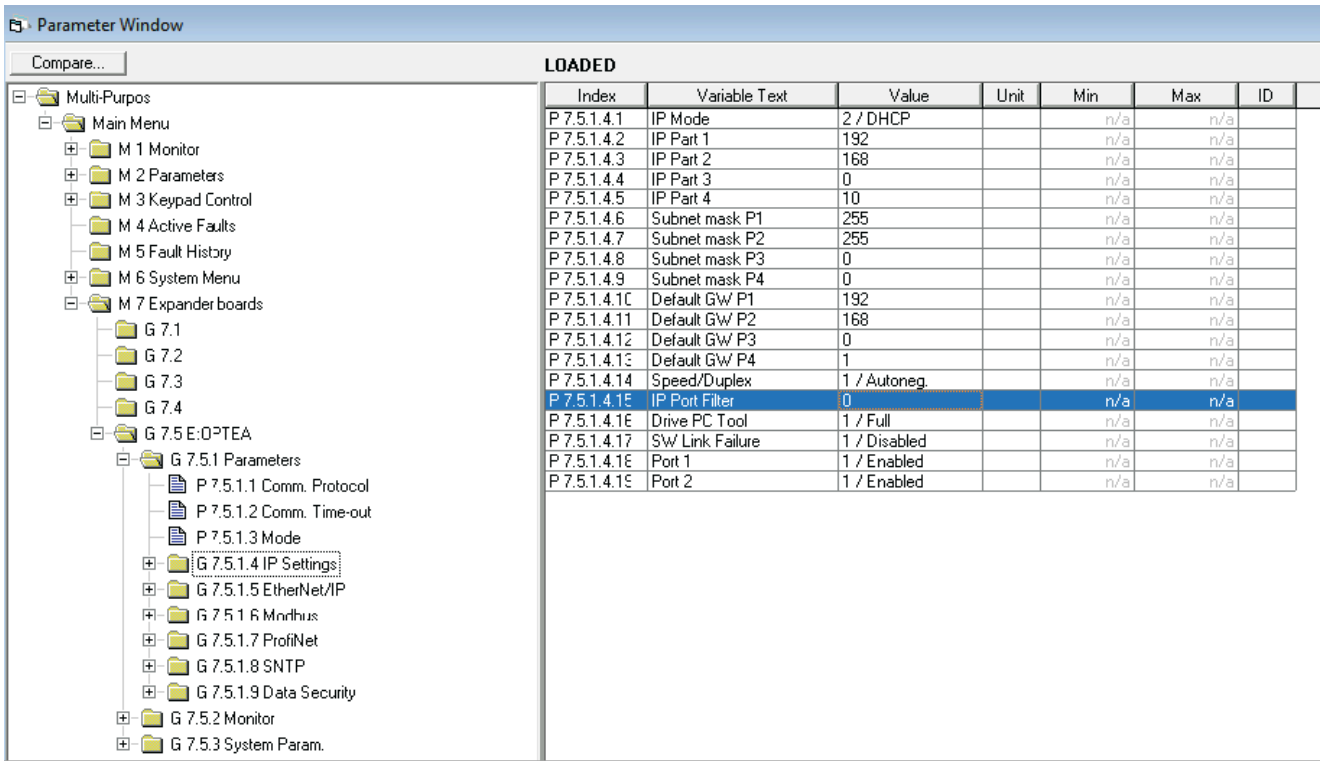


Figure 48: Parameter for Disabling SNMP

5.2.5 Set up User Management and Access Control

When VACON® NX drives arrive from the factory there is no user management configured. If any security features are required, first configure the Admin password as described in section 4.5.2 Setting-up Admin Password via VACON® NCDrive.

By default, the Anonymous user is permitted read access to all parameters. In addition, 5 parameters can be enabled for write access if required for operational purposes. It is recommended to enable only the required parameters, as described in section 4.5.13 Configuring Anonymous Access Rights and Keypad Settings

Danfoss Drives Oy © 2026.11

Enabling the user management features limits the risk of accidentally changing critical parameters, as modifying them requires user authentication once the Admin password has been set.

Passwords are inherently insecure because they are revealed every time they are used, and it is not possible to control or verify who has knowledge of a password. Ensure that passwords are changed when authorized personnel leave their roles.

Password strength correlates primarily with length rather than complexity. To maximize security, it is recommended to set the minimum password length as long as possible.

5.2.6 Perform Regular Maintenance

Monitor log files regularly by using VACON® NCDrive. Logs can be used to detect irregularities or unexpected activity, and faults and warnings.

Regularly back up the system and devices, and test the backups to ensure they work as expected. Include this process in the business continuity policy and operational exercises.

Stay informed about vulnerabilities that may impact Danfoss products and services: https://www.danfoss.com/en/service-and-support/coordinated-vulnerability-disclosure/danfoss-security-advisories/

Maintain the firmware of the VACON® NX and the PC Tools at the latest version: https://www.danfoss.com/en/service-and-support/downloads/

When performing service or maintenance, only use trusted devices to connect to the VACON® NX products.

5.3 Security Limitations and Non-Mitigated Threats

Based on a threat model of the VACON® NX drives, some threats are considered not fully mitigated by security measures in the drives itself. This may be due to technical limitations or because the drive cannot mitigate these without support from the system environment. It is also not feasible to make a threat model of every possible system and environment that the device can be installed into. To ensure that the securities of the target system users are required to carry out a threat model and security risk assessment on system level.

The threats have been broadly categorized according to MITRE® Common Attack Pattern Enumeration and Classification (CAPEC™). Website: https://capec.mitre.org/data/definitions/3000.html

Similar to the CAPEC™ framework, some common mitigations are listed after this as suggestions. Users are responsible for identifying and implementing appropriate mitigations according to their own risk assessment.

CAPEC-173: Action Spoofing and CAPEC-416: Manipulate Human Behavior

Threat: An authorized user can be tricked into changing configurations or performing actions on behalf of an adversary, for example installing outdated software with known vulnerabilities.

Common mitigations: Be aware of phishing attempts and only follow instructions from authorized sources. Validate the authenticity of software before installing.

CAPEC-94: Adversary in the Middle (AitM)

Threat: Communication channels and external interfaces are generally vulnerable to interception, alteration, and integrity and authentication violations, since they do not use secure protocols with mutual authentication. This includes the keypad, and most fieldbuses, especially protocols using serial connections. An adversary with physical access to these external interfaces of the device can sniff traffic and spoof identities.

Common mitigations: Protect access to the device, both physically and over the network. Protect access to the environment/system. Monitor and intercept malicious network communication. Set up access control to restrict access over the network.

Use secure protocols where possible. Use certificates or tokens for authentication instead of passwords. Use packet inspection or other intrusion monitoring mechanisms on insecure networks. Use network segmentation/isolation with strict control of data flows between networks and devices. For serial communications, ensure that connections are point to point and the cabling is visible for easy inspection, or is physically secured. Regularly fetch and analyze logs from the device.

CAPEC-176: Configuration/Environment Manipulation and CAPEC-165: File Manipulation

Threat: Files or settings are altered, either locally in the device or in other connected devices that the device relies on. Files in EEPROM or flash memory have basic integrity checks, but are not protected against malicious alteration. Option boards have no protection against configuration changes. External backup files can be maliciously altered. Log files can be altered.

Common mitigations: Protect access to the device, both physically and over the network, to prevent malicious data or commands. Set up access control to prevent unauthorized configuration changes or restoring of malicious backup configurations. Set up logs to be sent to an external device, or regularly fetch logs from the device. Protect backup files and log files on external devices, for example PCs, to ensure their integrity and authenticity.

CAPEC-116: Excavation

Threat: An adversary probes the device to solicit information that can be used for malicious purposes. If certain configuration values or production numbers are business sensitive, the adversary can read or infer these via side-channel attacks. Sensitive information can be disclosed on internal communication buses, on I/O connections, in log files, node status information, service lists, and configuration values. Side-channel attacks can measure temperature or volumes of coolant flows and infer production volumes.

Common mitigations: Protect access to the device, both physically and over the network. Protect access to the environment/system.

CAPEC-130: Excessive Allocation

Threat: The device is degraded or its availability is impacted by exhausting resources via crafted malicious inputs (as opposed to Denial of Service via flooding attacks).

Common mitigations: Protect access to the device, both physically and over the network. Protect access to the environment/system. Monitor and intercept malicious network communication that attempts to crash or cause unexpected behavior, especially on fieldbuses or other insecure protocols.

CAPEC-21: Exploitation of Trusted Identifiers

Threat: Shared login credentials are compromised. Network identities are spoofed. Most fieldbuses do not authenticate communications and are vulnerable to DNS/ARP/IP spoofing.

Common mitigations:

- Use unique login credentials for each device.
- Do not reuse passwords.
- Do not share passwords.
- Do not use passwords. Use credentials or other proofs of authentication that do not rely on shared secrets.
- Monitor and intercept malicious network communication.

CAPEC-22: Exploiting Trust in Client

Threat: An adversary exploits the implicit trust that the device has in an internal or external interface, trust in external devices, and so on.

The device has a trust boundary for the physical hardware: Anything internal in the enclosure of the device is implicitly trusted. For example, internal buses, I/O connectors, hardware slots, RAM memory bus, flash storage memory bus, option boards, or power boards.

Similarly, all internal API calls between software components are also trusted, as is all communication between software in different internal hardware components, for example, communication between the control unit and power unit. There is no authentication of signal sources.

Some external interfaces are also implicitly trusted, for example, I/O connectors, serial interfaces, most Ethernet-based fieldbus protocols that have no security features, and the keypad connector.

Common mitigations:

- Protect access to the device, physically and over the network.
- Protect access to the environment/system.

Danfoss Drives Oy © 2026.11

- Monitor and intercept malicious network communication.
- Set up access control to restrict access over the network and via the keypad.
- Set up logs to be sent to an external device, or regularly fetch logs from the device.

CAPEC-554: Functionality Bypass and CAPEC-212: Functionality Misuse

Threat: An adversary bypasses functionality intended to protect the device, or uses a legitimate function to achieve a negative technical impact.

The device can have outdated software with known vulnerabilities, or can be downgraded to a version with known vulnerabilities. Invalid or manipulated backup files are restored.

Common mitigations:

- Set up access control to protect the software update function of the device from unauthorized use.
- Keep up to date on new software versions and bulletins for vulnerabilities found in existing devices.
- Implement processes for timely updates of devices when new software is released.
- Regularly audit devices to ensure that they are using the newest version of software.

CAPEC-624: Hardware Fault Injection and CAPEC-607: Obstruction and CAPEC-507: Physical Theft

Threat: Signals, events, or the environment are disrupted to cause faulty behavior in the device.

- Fiber optic or I/O cables are intentionally connected to the wrong place.
- The power grid, phase/voltage, or power supply is manipulated which causes the device to restart or fail.
- Motor outputs are manipulated with an external device, or motor cables are tampered with.
- Other devices cause disturbances on the connected network or power grid.
- External cooling systems are manipulated to cause malfunctions.
- Flash memory is worn out by provoking repeated write operations that cause bad sectors or read errors.
- Necessary configurations or settings are deleted.
- Denial of Service via resource depletion, flooding attacks, and so on, on network interfaces.

The device can be stolen, or parts of it can be stolen that contain sensitive data or affect the availability of the system. The device is commonly in an enclosure or a cabinet, and some disassembly is required to remove option boards, the keypad, the control unit, and so on.

External components may be stolen, such as cables and wires, which cause a denial of service until replaced.

Common mitigations:

- Protect access to the device, both physically and over the network.
- Protect access to the environment/system.
- Monitor networks for intrusion and Denial of Service attacks.
- Set up logs to be sent to an external device, or regularly fetch logs from the device.

CAPEC-161: Infrastructure Manipulation

Threat: An adversary affects the flow of data between devices in the network. Devices are vulnerable to credential stuffing attacks or brute-force logins if weak or compromised passwords are used, or the network is unmonitored. Fieldbuses generally have no authentication or security features.

Common mitigations:

- Protect network access to the device.
- Protect access to the environment/system.

- Monitor the network for malicious activity.
- Enforce a policy that users make long passwords.

CAPEC-153: Input Data Manipulation

Threat: Lack of input validation of the format, structure, or composition of data leads to exploits. Applications can receive altered data from the network. Fieldbuses generally have no security features and altered, invalid, or malicious data from the network are processed.

Common mitigations:

- Monitor the network for malicious activity.
- Detect network intrusions.
- Use deep packet inspection to reject incorrectly formatted data on the network.

CAPEC-117: Interception

Threat: An adversary monitors data streams for information gathering purposes, but does not alter the contents of data. They can eavesdrop in many places to disclose information about production volumes, for example, by monitoring harmonics, currents, or power consumption.

I/O signals, insecure fieldbuses, and other network communication are also vulnerable to eavesdropping.

Common mitigations:

- Protect networks that transmit sensitive data in plaintext, segregate, and monitor them.
- Protect against physical side-channel eavesdropping attacks by masking the relationship between inputs and outputs of production.

CAPEC-438: Modification During Manufacture

Threat: The Danfoss supply chain can be attacked. Malicious logic can be inserted by insiders or included via third-party software components. Malicious code can be added during the manufacturing process.

Common mitigations: Danfoss takes several precautions against supply chain attacks. The software development and manufacturing process are security certified to IEC 62443-4-1, Maturity Level 3 (ML3).

CAPEC-122: Privilege Abuse

Threat: Authorized personnel can access functions they were not supposed to. This allows an adversary to exploit incorrectly configured access control, or move laterally in a system. The keypad and PC tools allow full access by default.

There is no authentication or confidentiality on the physical interface of the keypad, an adversary with physical access can sniff credentials and spoof identities.

Common mitigations:

- Set up access control to restrict access to functions and settings that are not necessary for users.
- Protect access to the device, both physically and over the network.
- Protect access to the environment/system.
- Monitor the network for malicious activity.
- Monitor log files regularly, set up log files to be sent to an external device.
- Keep the device up to date with the newest software versions.

CAPEC-233: Privilege Escalation

Threat: Some of the option boards contain an engineering and debugging interface (JTAG) that is intended to be accessible only by authorized Danfoss personnel.

Danfoss Drives Oy © 2026.11

Option boards do not have a JTAG connector in place, but soldering pads are available in the PCB. Accessing JTAG requires soldering work to get the correct connector in place, but that is all that is required. JTAG interface does not have any authentication in place.

Common mitigations:

- Protect physical access to the device.
- Protect access to the environment/system.

6 Decommissioning

6.1 Disposal of the Drive

Securing disposal of data stored in VACON® NX drives is needed to prevent potential disclosure of data.

Follow each of the instructions in the following chapters to erase different data in the drive. There are 3 steps needed to clear all the data and return the device to factory default settings, and these must be performed in the following order:

1. Erase user customized application.
   - Not required if such application is not used.
2. Perform a secure reset for the drive.
3. Clear data stored in the keypad.

6.2 Erase User Customized Application

If the drive includes customized applications that must be removed, this can be performed easily by installing the publicly available NX drive firmware package to the drive. It includes the basic applications and it overwrites the applications stored in the drive. See 4.13 Update VACON® NX Firmware.

6.3 Secure Reset Function

Activating the secure reset function resets the parameter values and security configurations in the drive to the factory default settings. Reset does not change the selected application. The audit log is cleared, and a single entry is recorded indicating that a secure reset was performed and the time at which it occurred.

If there is a custom application in place and it must be removed, refer to the instructions in 6.2 Erase User Customized Application.

To perform a secure reset, log in to VACON® NCDrive or keypad with Admin credentials, go to the parameter group *System Menu* > *S 6.0 Data Security* and set the parameter *P 6.0.4.9 Data Sec. Reset* to *1/Enabled*.

IMPORTANT: When the parameter *P 6.0.4.9 Data Sec. Reset* is set to *1*, the drive starts the reset process and reboots automatically.

Danfoss Drives Oy © 2026.11

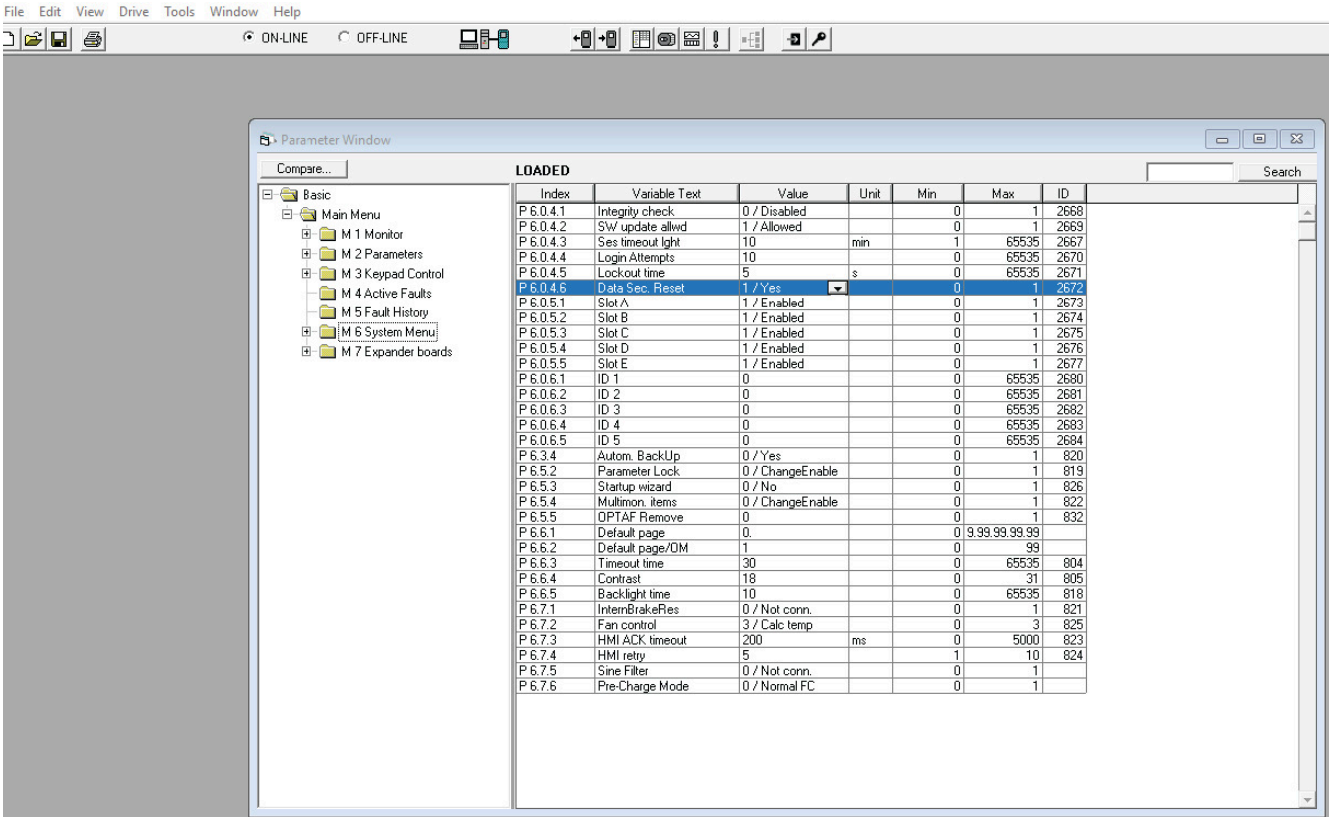


Figure 49: Secure Data Reset via PC Tool

To perform the secure reset via the keypad go to *System Menu* > *Data Security* > *Settings* > *Data Sec. Reset*. Select the value *Yes* and press the [enter key].

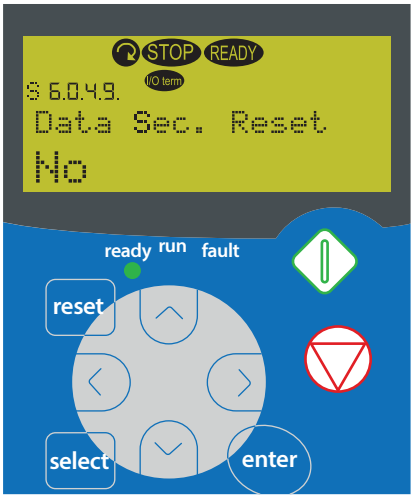


Figure 50: Secure Data Reset via Keypad

6.4 Clear Data Stored in the Keypad

The backup data in the keypad is erased by overwriting it with the factory default parameters after performing a data secure reset as described in 6.3 Secure Reset Function.

To overwrite a keypad backup, go to *System Menu* > *Copy Parameters* > *Up to keypad*. Select *All param.* and press the [enter key] to confirm.

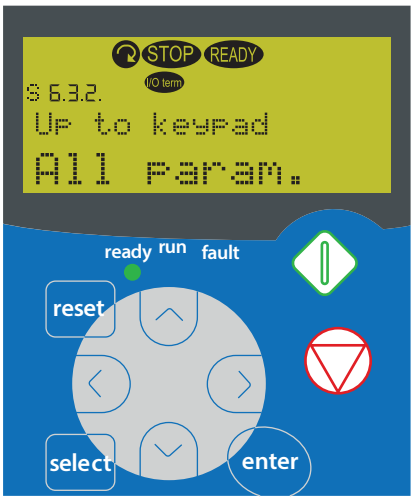


Figure 51: Making a Backup to the Keypad to Erase the Existing Backup

6.5 Backups

If a backup of the drive parameters and configuration is taken as described in section 4.11.1 Control System Backup and Recovery Management, the externally saved files include all data from the drive, except audit and event logs. It is thus recommended to remove those backup files if they are not needed anymore.

6.6 Remaining Data After Various Resets

6.6 Remaining Data After Various Resets lists how various types of saved data are handled during different types of resets. This information can be used to analyze what type of reset is needed.

Table 9: How Data is Handled During Different Types of Resets

Feature	Factory Reset [1]	Secure Reset
Application parameters	Reset to factory default	Reset to factory default
System menu	No impact	Reset to factory default
Secure Settings	No impact	Reset to factory default
Option board parameters	No impact	Reset to factory default
Parameter set 1 and 2	No impact	Reset to factory default
Keypad backup	No impact	No impact

1) Factory Reset is described, for example, in the VACON®NXS/NXP Air-cooled Wall-mounted and Standalone Operating Guide.

Danfoss Drives Oy © 2026.11

7 Appendix

7.1 Achieved Security Level Capabilities for Component Requirements

Table 10: Achieved Security Level Capabilities for Component Requirements

ID	Component Requirement	Achieved SL-C	Comment
CR 1.1	Human user identification and authentication	SL-C 1	
CR 1.2	Software process and device identification and authentication	SL-C 1	
CR 1.3	Account management	N/A	Not applicable because the product has only one administrative account defined.
CR 1.4	Identifier management	N/A	Not applicable because the product has only one administrative account defined.
CR 1.5	Authenticator management	SL-C 2	
CR 1.6	Wireless access management	N/A	The product supports no wireless communication.
CR 1.7	Strength of password-based authentication	SL-C 2	
CR 1.8	Public key infrastructure certificates	N/A	Product does not have any functionalities which require public key certificates.
CR 1.9	Strength of public key authentication	N/A	Product does not have any functionalities which require public key certificates.
CR 1.10	Authenticator feedback	SL-C 4	
CR 1.11	Unsuccessful login attempts	SL-C 4	
CR 1.12	System use notification	SL-C 4	
CR 1.13	Access via untrusted networks	N/A	The product must not be connected to untrusted networks.
CR 1.14	Strength of symmetric key-based authentication	N/A	The product does not support symmetric key-based authentication.
CR 2.1	Authorization enforcement	SL-C 1	
CR 2.2	Wireless use control	N/A	The product supports no wireless communication.
CR/EDR 2.4	Mobile Code	N/A	The product supports no mobile code.
CR 2.5	Session lock	SL-C 4	
CR 2.6	Remote session termination	SL-C 4	
CR 2.7	Concurrent session control	SL-C 4	
CR 2.8	Auditable events	SL-C 4	
CR 2.9	Audit storage capacity	SL-C 4	
CR 2.10	Response to audit processing failures	SL-C 4	
CR 2.11	Timestamps	SL-C 3	
CR 2.12	Non-repudiation	SL-C 3	
CR/EDR 2.13	Use of physical diagnostics and test interfaces	SL-C 2	
CR 3.1	Communication integrity	SL-C 1	

Table 10: Achieved Security Level Capabilities for Component Requirements - (continued)

ID	Component Requirement	Achieved SL-C	Comment
CR/EDR 3.2	Protection from malicious code	SL-C 4	
CR 3.3	Security functionality verification	SL-C 3	
CR 3.4	Software information integrity	SL-C 1	
CR 3.5	Input validation	SL-C 4	
CR 3.6	Deterministic output	SL-C 4	
CR 3.7	Error handling	SL-C 4	
CR 3.8	Session integrity	SL-C 1	
CR 3.9	Protection of audit information	SL-C 3	
CR/EDR 3.10	Support for updates	SL-C 1	Hash values can be delivered on request.
CR/EDR 3.11	Physical tamper resistance and detection	SL-C 1	
CR/EDR 3.12	Provisioning product supplier roots of trust	SL-C 1	
CR/EDR 3.13	Provisioning asset owner root of trust	SL-C 1	
CR/EDR 3.14	Integrity of the boot process	SL-C 1	
CR 4.1	Information confidentiality	SL-C 1	To achieve SL-C 1, PC tool connectivity via Ethernet must be disabled when not used for configuration of the product, according to 5.2.4.2 Disabling PC-Tool Connectivity from OPTEA/OPTE9 Cards.
CR 4.2	Information persistence	SL-C 2	
CR 4.3	Use of cryptography	SL-C 4	
CR 5.1	Network segmentation	SL-C 4	
CR 6.1	Audit log accessibility	SL-C 2	
CR 6.2	Continuous monitoring	SL-C 1	
CR 7.1	Denial of service protection	SL-C 1	
CR 7.2	Resource management	SL-C 4	
CR 7.3	Control system backup	SL-C 4	
CR 7.4	Control system recovery and reconstitution	SL-C 4	
CR 7.6	Network and security configuration settings	SL-C 4	
CR 7.7	Least Functionality	SL-C 4	
CR 7.8	Control system component inventory	SL-C 4	

7.2 Fault Codes Related to Cybersecurity Features

This section describes the VACON® NX fault/alarm codes which are related to the cybersecurity features of VACON® NX drives. Other fault codes are listed in their relevant VACON® NX guides.

Danfoss Drives Oy © 2026.11

Table 11: Cybersecurity Fault Codes

Code	Fault	Subcode	Description	Recommendations
27	Data security module	S1	Pepper is invalid	Use the most recent VACON® NCLoad to install firmware.
		S3	Error in resetting EEPROM after secure reset	Perform a secure factory reset again. If the fault reoccurs, contact Danfoss Drives Service.
		S4	File system hash calculation failed	Try reinstalling the application.
		S5	File system hash does not match with stored hash	Try reinstalling the application.
		S6	File system hash storing failed	Try reinstalling the application.
		S7	File system hash has been updated	Reset fault. If the fault reoccurs, contact Danfoss Drives Service.
		S8	Device does not contain pepper	Use the most recent VACON® NCLoad to install firmware.
		S9	Admin password incorrect	Perform a secure factory reset, restore parameter values from backup, set the admin password again.
		S255	Fatal error	Contact Danfoss Drives Service.
28	Audit Log	S1	Audit log writes failed	Contact Danfoss Drives Service.
		S3	The number of audit log events reached the configurable warning level	-

Danfoss Drives Oy © 2026.11

Danfoss Drives Oy
Runsorintie 7
FIN-65380 Vaasa
www.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.

BC563869736695en-010101
Danfoss Drives Oy © 2026.11

1 7 2 Z 4 0 8 9 A