ENGINEERING
TOMORROW

User guide

Cybersecurity for Danfoss VACON Drives

An Informative Guide for System Integrators to Achieve the Required Security Level with Danfoss Drives VACON® NX Family According to UR E26, UR E27, and IEC 62443-3-3.

drives.danfoss.com | VACON®

Contents

1 Introduction

1.1 Purpose of this document

The unified requirements E26 and E27 are used by the system integrator to explain the cybersecurity of a system. The system integrator or OEM must demonstrate that the system designed has the capability to support the security level intended for different parts/zones in the system.

This document is a guide with recommendations aimed at system integrators using the VACON® NX drive as a component in the system. Drives in scope for this document: NXA, NXB, NXI, NXN, NXP, DCGuard, in this document referred to as VACON® NX drives.

As product supplier, Danfoss shares information on VACON® NX drives to be used in the marine system based on:

- IEC 62443-4-1: Development and production of the components
- IEC 62443-4-2: Description of the product, giving information on threats and mitigations, and how this product is compliant to achieve a certain security level.
- Unified requirements E26 and E27

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

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

Security Level (SL-T)[1]	IEC 62433-3-3 definition
SL-4	Identify and authenticate all users by mechanisms which protect against intentional unauthenticated access by using sophisticated means with extended resources, IACS specific skills, and high motivation.
SL-3	Identify and authenticate all users by mechanisms which protect against intentional unauthenticated access by using sophisticated means with moderate resources, IACS specific skills, and moderate motivation.
SL-2	Identify and authenticate all users by mechanisms which protect against intentional unauthenticated access by using simple means with low skills and low motivation.
SL-1	Identify and authenticate all users by mechanisms which protect against casual or coincidental access to unauthenticated entities.

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

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

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

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

The target security level for VACON® NX drives is SL-1.

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

A list for the UR E27 Mitigation plan can be found in chapter 6.4 DNV July/2023 UR E27 Requirements Mitigation List.

1.2 Extended Requirements

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

1.2.1 DNV: Rules for Classification Ships Edition July 2023

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

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

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

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

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

This document focuses only on SP0 and SP1 requirements.

A list for the UR E27 mitigation plan can be found in section 6.4 DNV July/2023 UR E27 Requirements Mitigation List.

1.3 Document Version

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

The original language of this guide is in English.

Version	Remarks	Software version
Document version 01	Preliminary release	x.x.x

2 Safety

2.1 Safety Precautions

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

2.2 Qualified Personnel

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

Persons with proven skills:

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

3 Security Measures

Integration of security measures to handle misuse or tampering with functionalities in the product. The following measures ensure the integration of security in VACON® NX drives from Danfoss:

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

4 Security management

4.1 Overview

Danfoss drives security management is based on IEC 62443 and ISO 27001.

4.2 Procedure

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

NOTICE

THIS IS A CONTINUOUS PROCESS.

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

5 IEC 62443-4-2 Certification

VACON® drives, including VACON® NX series drives are working towards IEC 62443-4-2 SL1 certification.

6 Extended Requirements

6.1 DNV Rules for Classification Ships edition July/2023

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

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

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

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

NOTICE

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

6.2 Color code and Mitigation list

In section 6.4 DNV July/2023 UR E27 Requirements Mitigation List, the following color codes are used to indicate the solution.

Table 3: Color Codes

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

6.3 Codes for Mitigation to be Achieved with Other Means

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

ID	Description
M1	**Access control for enclosure or room where VACON® NX drives are installed** The most basic line of defense is physically shielding the drives in enclosures or rooms with access control. The enclosure or room can have access control by locking mechanism where special tools, special keys, or access codes are needed to access the enclosure or room. Only qualified personnel have the means to get access.
M2	**Remove control panel from VACON® NX drive to prevent local access** Remove the control panel from the VACON® NX drives under normal operation. If unintended access should happen, removing the control panel will prevent access to the drive parameters. In service cases, an control panel can be handed out by the owner of the installation to a trusted person, for example, a trained service technician.
M3	**Access control handled on system level** On system level, the access control to the user interface (SCADA, HMI, and so on) is recommended to include an access control with password.
M4	**Wireless option is not recommended** VACON® NX drives do not include any wireless options.
M5	**Strength of password handled on system level** It is recommended to introduce guidelines for using strong passwords and how often these passwords are changed. It is recommended that the guidelines are implemented consistently in the deployed engineering tools used.
M6	**System design to ensure connection only to trusted networks** The *trusted network* should be understood, from a cybersecurity viewpoint, as being a strictly limited and well-hosted portion of a certain network or control system. For recommendations to achieve security level SL-1, see section 8.2.1 Local Access.
M7	**Utilize segmentation at network level** Segmentation can be used to divide the network into smaller parts. The purpose can both improve network performance and cybersecurity.

6.4 DNV July/2023 UR E27 Requirements Mitigation List

Drives mitigations are risk based. This means that to control the risks VACON® 100 drives create for the system, different counter measures must be taken on control system, network, and physical security level. All proposed mitigations create low or very low risk on a system level.

Table 5: DNV July/2023 UR E27 Requirements Mitigation List

DNV rules for classification ships edition July/2023 requirements	SP1 (1)	Mitigation at system level recommended (section 3-3)
User identification and authentication		
Human users shall be identified and authenticated for access to the system.	YES	M1, M2, M3
Multifactor authentication is required for human users when accessing the system from or via an untrusted network.	YES^{H}	–
Identification and authentication of devices and software processes shall be implemented on interfaces providing access to the system.	YES^{H}	M1, M2, M3 + There are controls on different protocols to identify devices. Software packages are encrypted (Firmware).
Account management		

Table 5: DNV July/2023 UR E27 Requirements Mitigation List (continued)

DNV rules for classification ships edition July/2023 requirements	SP1[(1)]	Mitigation at system level recommended (section 3-3)
It shall be possible to manage all accounts (human users accounts and non-human user accounts). This shall at least include adding, activating, modifying, disabling, and removing accounts.	YES	M1, M2, M3
Identifier management		
It shall be possible to manage identifiers in the system. The intention is to allow for segregation of duties and least privilege by assignment of different privileges depending on user, role, group, or interface.	YES	M1, M2, M3
Authenticator management		
It shall be possible to manage authenticators in the system. This implies, for example, initializing, changing, and protecting passwords from unauthorized disclosure when stored and transmitted.	YES	M1, M2, M3
Wireless access management		
All users (human and non-human) shall identify and authenticate themselves to access the system by wireless communication.	YES	M4
Strength of password-based authentication		
It shall be possible to configure minimum length of passwords.	YES	M5
Authenticator feedback		
The system shall obscure feedback during the authentication process (for example, display asterisks instead of password characters during login process).	YES	Only pass or fail feedback is given.
Unsuccessful login attempts		
The system shall enforce a limit of consecutive invalid login attempts during a specified time period. Access shall be denied for a configurable period of time or until an administrator unlocks the account. For critical services, the control system shall provide the capability to disallow interactive logons with the service account.	YES	M1, M2, M3
System use notification		
It shall be possible to configure a notification message to be shown when a human user authenticates to the system.	YES	M6
Access via untrusted networks		
Any access from or via untrusted networks shall be monitored (for example, logged, indicated, alarmed) and controlled (for example, denied, restricted).	YES	M6
The system shall deny access from or via untrusted networks if the request is not approved by authorized personnel on board.	Yes [H]	M6
Authorization enforcement		
On all interfaces, human users shall be assigned authorizations in accordance with the principles of segregation of duties and least privilege.	YES	M1, M2, M3 + currently 2 user groups: Operations and service. The control system restricts functionalities and privileges for operations.
Wireless use control		
The system shall authorize, monitor, and enforce usage restrictions for wireless connectivity.	YES	M4

Table 5: DNV July/2023 UR E27 Requirements Mitigation List (continued)

DNV rules for classification ships edition July/2023 requirements	SP1 (1)	Mitigation at system level recommended (section 3-3)
Use control for portable and mobile devices		
The system shall enforce usage restrictions of portable and mobile devices.	YES	The product does not use mobile code.
Mobile code		
The system shall restrict use of mobile code such as java scripts, ActiveX, and PDF.	YES	The product does not use mobile code.
Session lock		
The system shall be able to prevent further access after a configurable time of inactivity or following activation of the manual session lock.	YES	M1, M2, M3 + enforced via, secure service policy
Remote session termination		
The system shall automatically terminate a remote session after a configurable time of inactivity, or by manual termination by a responsible crew member. The effect of terminating a remote session during on-going operations shall be considered and not endanger the vessel or its crew.	YES[H]	–
Auditable events		
The system shall generate audit records for access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Each record shall include timestamp, source, category, type, event ID, and event result.	YES	M1, M3 + control system level logging includes VACON® NX drives related events. VACON® NX drive provides fault and error logs
Audit storage capacity		
Sufficient storage capacity for audits records shall be provided. As part of the audit, storage capacity for such records shall be monitored.	YES	M1, M3 + control system level logging includes VACON® NX drives related events. VACON® NX drive provides sufficient storage capacity for fault and error logs.
Response to audit processing failures		
The system shall alert responsible personnel and prevent loss of essential or important functions in the event of an audit processing failure.	YES	M1, M3 + control system level logging includes VACON® NX drive related events. VACON® NX drive provides fault and error logs.
Timestamps		
The system shall timestamp each audit record.	YES [H]	M1, M3 + date and time can be set (after each power cycle it must be updated).
Communication integrity		
The system shall protect the integrity of transmitted information.	YES	M1, M7 + System integrator protects the communication channel with shielded wires.
The system shall apply cryptographic algorithms to protect the integrity of transmitted information.	YES [H]	M1, M7 + control system should protect the integrity of information when transmitted (other than transmission between control system and VACON® NX drive).

Table 5: DNV July/2023 UR E27 Requirements Mitigation List (continued)

DNV rules for classification ships edition July/2023 requirements	SP1 (1)	Mitigation at system level recommended (section 3-3)
Malicious code protection		
The system shall have protection mechanisms against malicious code or unauthorized software. This shall include prevention, detection, reporting and mitigating countermeasures. The protection mechanism shall be kept updated, see also DNV-CG-0325.	YES	M1 + Software packages are obtained only from trusted source (for example, the Danfoss website). Only trusted personnel can do updates and boot.
Malicious code protection shall also be implemented on entry and exit points to the system (for example, removable media, remote access servers, and so on).	YES	M1 + software packages are obtained only from trusted source (for example, the Danfoss website). Only trusted personnel can do updates and boot.
Security functionality verification		
It shall be possible (at least during test phases and scheduled maintenance) to verify that the required security functions operate as intended.	YES	Enforced via a secure service policy. Software tools provide capability to test that everything works as intended.
Input validation		
Inputs that may directly impact control functions shall be validated. This requirement does not address human error when entering, for example, commands or setpoints at a local HMI.	YES	Unused I/O configurations are set to "No operation", and all inputs scaling are set and constantly monitored for unusual changes. Harden the parameter configuration by examining all the minimum/maximum limits.
Deterministic output		
The system shall respond in a fail-to-safe manner as per Pt.4 Ch.9 Sec.2 [2.2] if normal operation may not be maintained as a result of a cyber incident.	YES	Output reaches predetermined state based on user configuration. • Fieldbus failure • Safety function failure • Any other fault
Session integrity		
The system shall protect the integrity of sessions. Invalid session IDs shall be rejected.	YES H	–
The system shall invalidate session IDs after user logout or other session termination (including browser sessions).	YES H	–
The system shall generate a unique session ID for each session. Unexpected session IDs shall be treated as invalid.	YES H	–
Information confidentiality		
The system shall be able to protect the confidentiality of information at rest or in transit that has read authorization.	YES	M1 + data is control data.
Use of cryptography		
If cryptography is required, the system shall use algorithms, key sizes, and mechanisms for key establishment and management based on best practices and recommendations.	YES	M1 + data is control data.
Network segmentation		

Table 5: DNV July/2023 UR E27 Requirements Mitigation List (continued)

DNV rules for classification ships edition July/2023 requirements	SP1 (1)	Mitigation at system level recommended (section 3-3)
Separation of zones in [3.2] shall be implemented by logical or physical network segmentation.	YES	M7
Physical network segmentation is required for OT/IT systems and safety systems. See [3.2.3] and [3.2.5].	YES H	M7
Zone boundary protection		
Communication traversing zone boundaries shall be controlled and monitored to enforce the compartmentalization for zones and conduits.	YES	M7
Communication traversing zone boundaries shall be controlled according to the principle of deny by default, allow by exception.	YES H	M7
It shall be possible to manually stop communication between zones serving essential or important services, including boundaries to safety functions and IT zones (island mode).	YES H	M7
General purpose person-to-person communication restrictions		
External general purpose person-to-person messages shall not be received by the system.	YES	–
Application partitioning		
Data, applications, and services shall be subject to partitioning or separation in accordance with the zoning model. This implies that different zones shall not depend on the same data, applications, or services.	YES	M7
Audit log accessibility		
The system shall provide read-only access to audit records for authorized users.	YES	M1, M3 + control system level logging includes VACON® NX drive related events. VACON® NX drive provides fault and error logs.
Denial of service protection (DoS)		
The system shall be able to operate in a degraded mode during a DoS event. Amendments: • This requirement shall be seen in context with Pt.4 Ch.9 Sec.4 [3.1.3]. • Monitoring and alarming of network status shall follow the requirements in Pt.4 Ch.9 Sec.4 [3.1.4].	YES	Monitoring and alarming are handled on the control system level. The risk for DoS event happening only on drive level is seen as very low. Redundant can be implemented to control the threat.
Resource management		
The system shall be able to schedule system resources for higher priority software processes such as, shutdowns, alarming, and monitoring over lower priority tasks, such as network scans.	YES	There is task management (Priority schema in OS).
Control system backup		
It shall be possible to create a complete backup of the system during normal operation.	YES	Parameter files. Parameters can be stored on the control panel.
Control system recovery and reconstitution		
It shall be possible to recover and reconstitute the system after a cyber incident.	YES	Parameter files. Parameters can be stored on the control panel.

Table 5: DNV July/2023 UR E27 Requirements Mitigation List (continued)

DNV rules for classification ships edition July/2023 requirements	SP1[1]	Mitigation at system level recommended (section 3-3)
Emergency power		
If the system is supplied from 2 or more power sources, switching between these sources shall not affect security functions of the system.	YES	Handled on control system level
Network and security configuration		
It shall be possible to configure the system's network and security parameters according to recommended guidelines from the supplier. An interface shall exist to monitor these settings.	YES	M4, M6 + security-related configurations can be monitored and changed via control panel or service port
Least functionality		
Unnecessary functions, ports, protocols, and/or services shall be disabled, prohibited, or removed from the system.	YES	M1, M2 • Parameters can be locked. • Control system HMIs have restricted access to functionalities. • There are only used ports. • Not needed functionalities are disabled, and there are mechanisms to prevent enabling them.

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

7 Device Specifications

7.1 VACON® NX drives

Frequency converter for use in various marine applications. Constant/variable torque applications. Air and liquid cooled. CHxx = liquid cooled, FRxx = air cooled, FIxx = Inverter module, Air cooled.

Feature	Description
Supply voltage range	208–690 V, 50/60 Hz
Voltage variation	- 10%, + 10%
Frequency variation	+/-10 %
Output frequency	0–320 Hz
Temperature range in operation	• Air cooled: 0–40 °C (40–50 °C when derated 1.5% / °C, 50–55 °C when derated 2.5% /°C) • Liquid cooled: 0–50 °C (CH6x series 50–55 °C when derated 2.5% / °C)
Temperature class	A
Vibration class	A
Humidity class	A
Protection class	IP00, IP21, and IP54
EMC class	DNV CN 2.4/IEC 61800-3 To be used on EMC class A locations
FC modules	3 x 380–500 V, 7.5–5150 kW 3 x 525–690 V, 110–5300 kW
Common DC modules	465–800 V DC, 7.5–5150 kW 640–1100 V DC, 110–5300 kW

In all drives, a firmware is downloaded during production to operate the functions in the drive. Due to the different use of the drives, System interface, Marine, DC-to-DC converter, Grid converter, Industrial, and Flow each has its own firmware version. For each series, the firmware version is the same in all power sizes.

Operating, changing settings, or updating firmware to the drive can be done by different methods: control panel, commissioning software, or via different fieldbus options.

7.2 Default interfaces

7.2.1 Overview

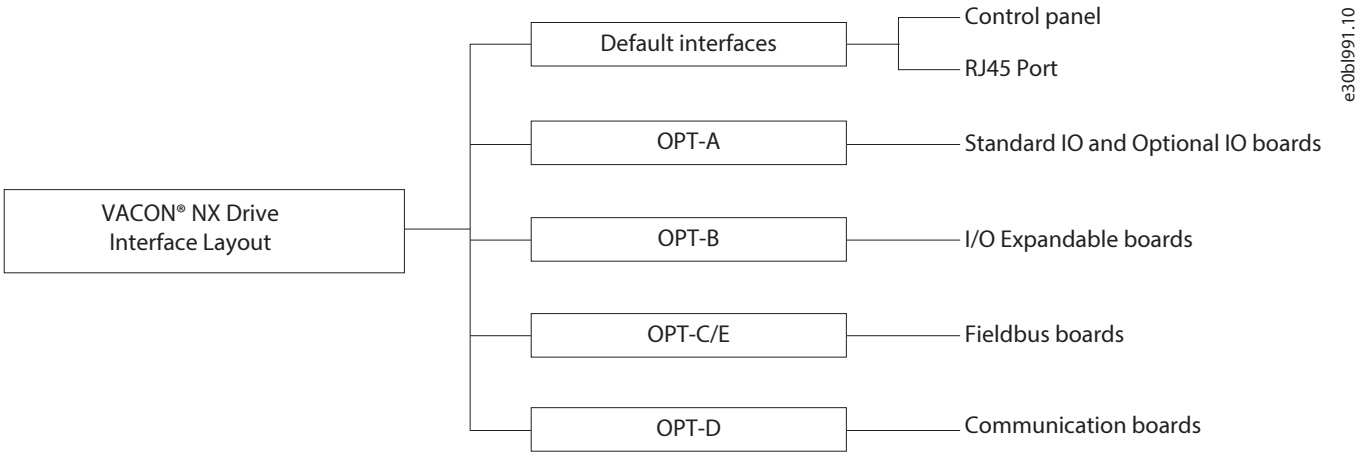
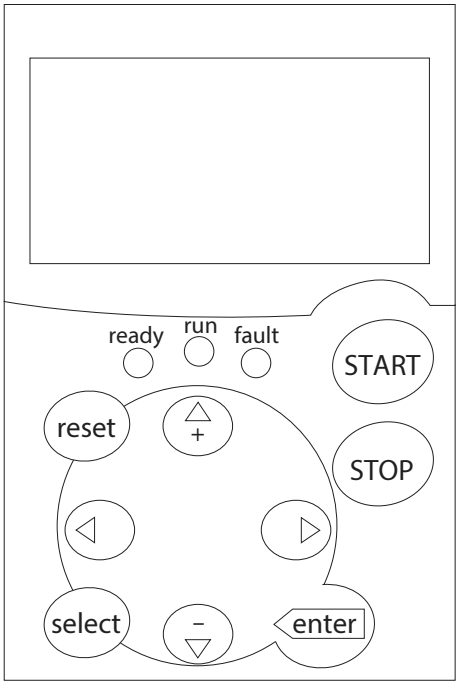


Figure 1: Default Interfaces VACON® NX Drives

7.2.2 Local Control Panel Type 1

The control panel is the link between the VACON® AC drive and the user. The local control panel type 1 comes with the following features:



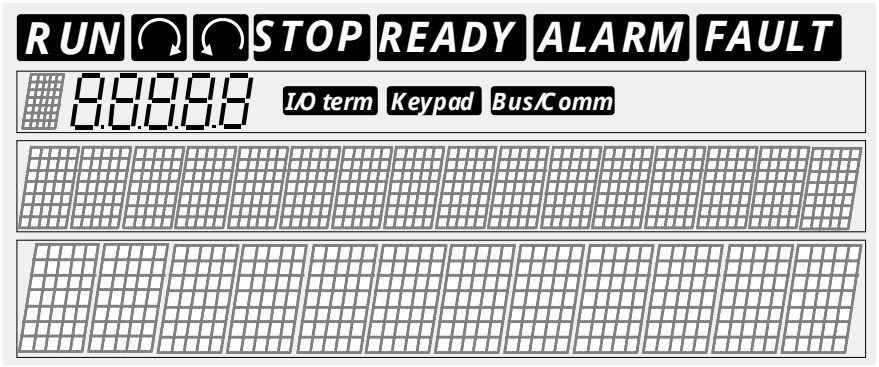


Figure 2: Local Control Panel Type 1

- Removable panel with plug-in connection.
- Alphanumeric display with 7 indicators for the Run status (RUN, ↻, ↺, STOP, READY, ALARM, FAULT) and 3 indicators for the control place (I/O term/Keypad/BusCom).
- 3 status indicator LEDs (green, and red).
- The control information, that is the number of menus, the description of menu or the shown value and the numeric information are presented on 3 text lines.

- Graphical and text keypad with multiple language support.
- Parameter backup and copy function with the panel's internal memory.
- The startup wizard ensures a hassle-free setup. Select the language, application type, and main parameters during the 1st power-up.

Activating password protection and setting a password

- **Password (S6.5.1):** The application selection can be protected against unauthorized changes with the Password function (S6.5.1). By default, the password function is not in use. To activate the function, enter the edit mode by pushing the Menu button *Right*. A blinking 0 appears in the display. Set a password with the Browser buttons. The password can be any number between 1 and 65535.
- The password can be set in digits too. In the edit mode, push the Menu button *Right* once again and another 0 appears in the display. Set the units and push the Menu button *Left*. Then set the tens, and so on. Confirm the password setting with the *Enter* button. Wait until the Timeout time (P6.6.3) has expired before the password function is activated (see *VACON® NXP & NXS user manual* page 100).
- When changing applications or the password, enter the current password when prompted. The password must be entered with the Browser buttons. Deactivate the password function by entering the value 0.

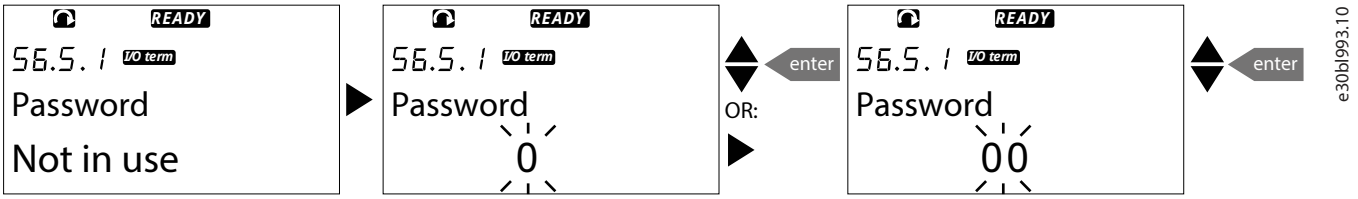


Figure 3: Setting a Password

NOTICE

STORE THE PASSWORD IN A SECURE LOCATION!

No changes can be made unless a valid password is entered.

- **Parameter lock (P6.5.2):** Use this function to prohibit changes to the parameters. If the parameter lock is activated, the text *locked* will appear on the display when a parameter value is to be edited.

NOTICE

- This function does not prevent unauthorized editing of parameter values.

- Enter the edit mode by pushing the Menu button *Right*. Use the Browser buttons to change the parameter lock status. Accept the change with the *Enter* button or return to the previous level with the Menu button *Left*.

Parameter locking

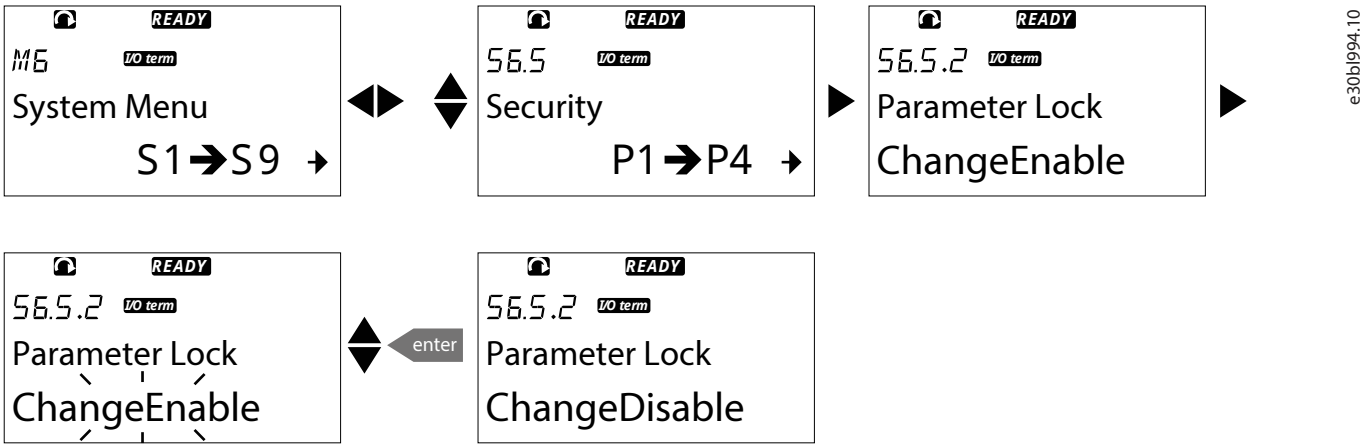


Figure 4: Step to Lock Parameter

Entering a password

The password is entered with the Browser buttons.

7.2.3 Local Control Panel Type 2

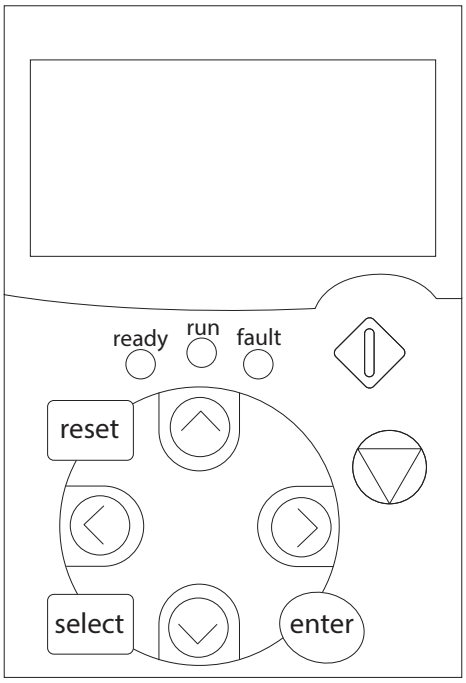


Figure 5: Local Control Panel Type 2

The Local Control Panel Type 2 comes with the following features:

- Removable panel with plug-in connection.
- Graphical and text keypad with multiple language support.
- Text display multi-monitoring function.
- Parameter backup and copy function with the panel's internal memory.
- The startup wizard ensures a hassle-free set up. Select the language, application type, and main parameters during the 1st power-up.

Activating password protection and setting a password

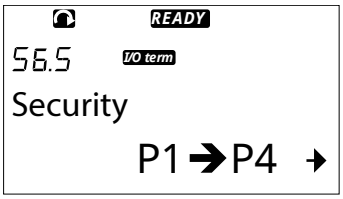


Figure 6: Activating password protection

- Scroll down in the *System* menu until the location indication S6.5 shows on the 1st line of the display.
- To go to the *Security* submenu from the *System* menu, push the Menu button Right.
- Password (S6.5.1) Helps to prevent unauthorized changes in the application selection with the Password function (S6.5.1). By default, the password is not active.
- To set a password 1 In *Security*submenu, push the Menu button Right.
- To go to the edit mode, push the Menu button Right. The display shows a flashing '0'.
- There are 2 options to set a password: with the Browser buttons or by digits. The password can be a number between 1 and 65535.
- Push the Browser buttons *Up* and *Down* to find a number.
- Push the Menu button *Right*. A second '0' shows in the display.
  - Push the navigation buttons to set the digit on the *Right*.
  - Push the Menu button *Left* and set the digit on the *Left*.
  - To add a 3rd digit, push the Menu button *Left*. Set up to 5 digits with Menu and Browser buttons.
  - To accept the new password, push the *Enter* button. The password activates after the Timeout.

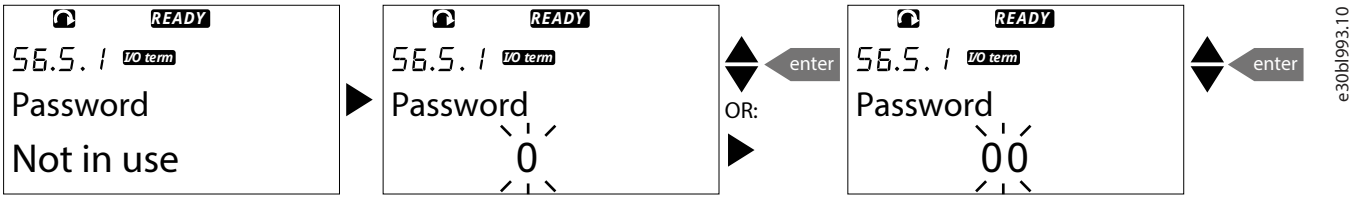


Figure 7: Setting a Password

Entering a password

When accessing the submenu that has password protection, the display shows 'Password?', enter the password with the Browser buttons.

7.3 Software for VACON® NX Drives

7.3.1 Overview

Table 6: Software for VACON® NX Drives

Software	Overview	Software packages and supporting documents
Commissioning Tool		For software packages and supporting documents, refer to www.danfoss.com and software help menu for the procedure.
VACON® NC drive	A software tool used for commissioning, parameterization, monitoring, and diagnosing VACON® NX family drive products.	
Firmware, Application & Option Boards Software Update		
VACON® NCLoad	A software tool for updating drive firmware and installation of software applications for the VACON® NXP family drive products.	
Option Boards Software Update		
VACON® NCIPConfig	A software tool used for managing Ethernet-based network options for the VACON® NXP communication OPT_C option boards and for updating option board software.	
VACON® Loader	A software tool used for managing Ethernet-based network options for the VACON® NXP communication OPT_E option boards and for updating option board software.	
Functional Safety Configuration Software		
VACON® Safe	A software tool used for easy configuration, customizing the safety application, and adapting the settings of safety parameters for the VACON® advanced safety options OPT-BL/OPT-BM/OPT-BN.	
Service Tool		
VACON® Service Tool	Device Properties service programming tool set up instructions to control unit and power unit.	The software *Device Properties Service.exe* is available in the Danfoss drives service extranet.

7.3.2 VACON® NC Drive

VACON® NC Drive is a commissioning tool for parameterization of an application running in a frequency converter. VACON® NC Drive provides the following benefits.

- It is possible to change the parameter settings in the frequency converter via a PC instead of a panel.
- The parameter settings can be changed even in offline mode and save the settings to a file for later downloading to a frequency converter.
- With VACON® NC Drive, the parameter settings can be printed for archiving purposes.
- It is possible to monitor up to 8 signals simultaneously in graphical format and set triggers which allow to see what happened in the frequency converter when a trigger is fired.
- It is possible to control the motor by setting the references and commanding the motor to start or stop or change direction by clicking buttons in the operating window.
- The fault history and active faults can be viewed in the diagnostic page.

Types of communication used:

- Ethernet TCP/IP

- RS232
- CAN interface

NOTICE

- The Ethernet communication in VACON® NC Drive is not any faster than serial communication, because VACON® NC Drive sends and receives all the messages through Ethernet as it uses a serial port.

7.3.3 Firmware and Application Update

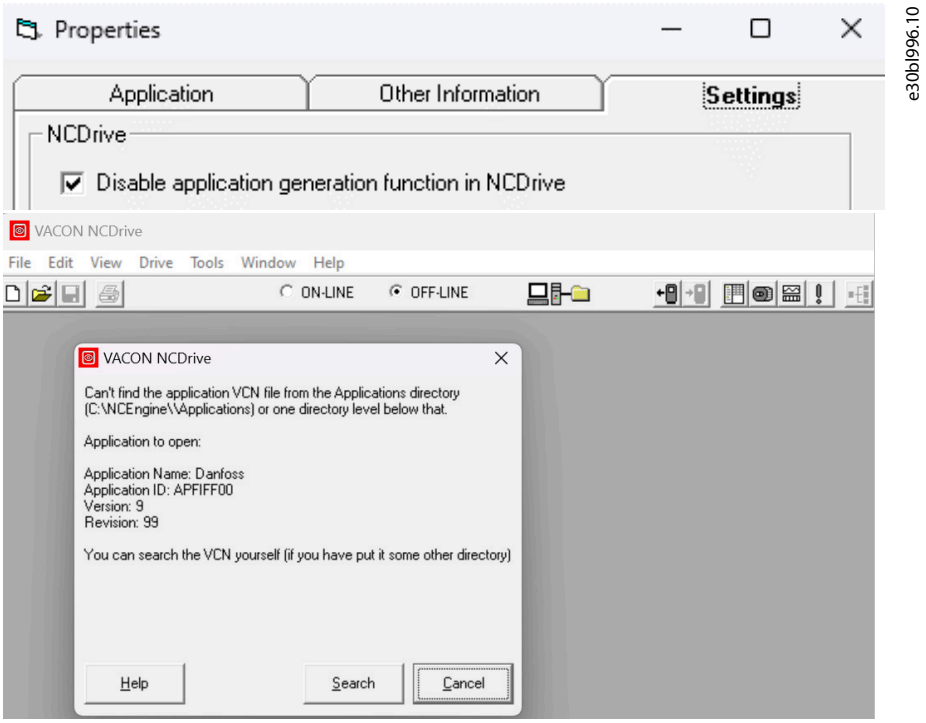
VCN packets

VCN packets are used by NC Drive and NCLoad programs. These packets can contain various kinds of information in the form of compressed files. VCN packets have a type that tells NC Drive and NCLoad what they contain. A VCN packet may be a packet that contains a firmware file to load with the NCLoad program and all the databases of the applications that this firmware contains. A VCN packet may be a packet that contains 1 or more application files and their databases, or it can be a packet that contains an option board program.

NC Drive shows only VCN packets that contain application databases. For example, option board VCN does not contain any applications, so it does not contain any application databases either.

VCN packets are automatically generated during the application development process by the application compiler. There is also a possibility to generate the database by reading it from a frequency converter and saving it to a hard drive. This method reads only the information that the NC Drive needs. These VCN databases cannot be used in application development or with NCLoad.

During the NX-application software development process, it is possible to activate the blocking of the virtual connection (generated gen.VCN) to the drive. The NCDef-tool has an option to disable virtual connection with NC Drive without loadable application (VCN-file).



e30bl996.10

Figure 8: NCDef (NX-parameter Defining Tool)

VACON® NCLoad

VACON® NCLoad is a program for loading system programs, applications, and option board programs to a frequency converter. When selecting an application package, Option Package, and system program package (VCN file) in the respective browser window, all the application, Option, and System in that package are selected by default for loading.

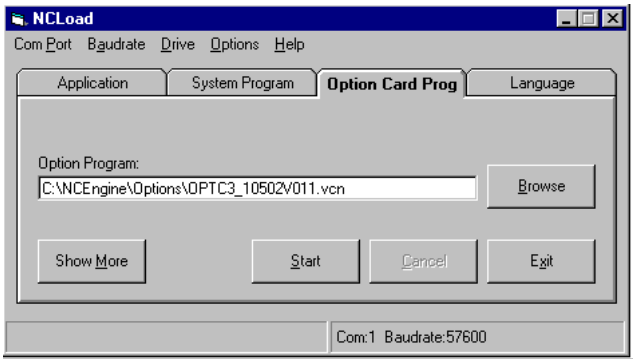


Figure 9: VACON® NCLoad Option Program

7.3.4 VACON® Safe PC tool

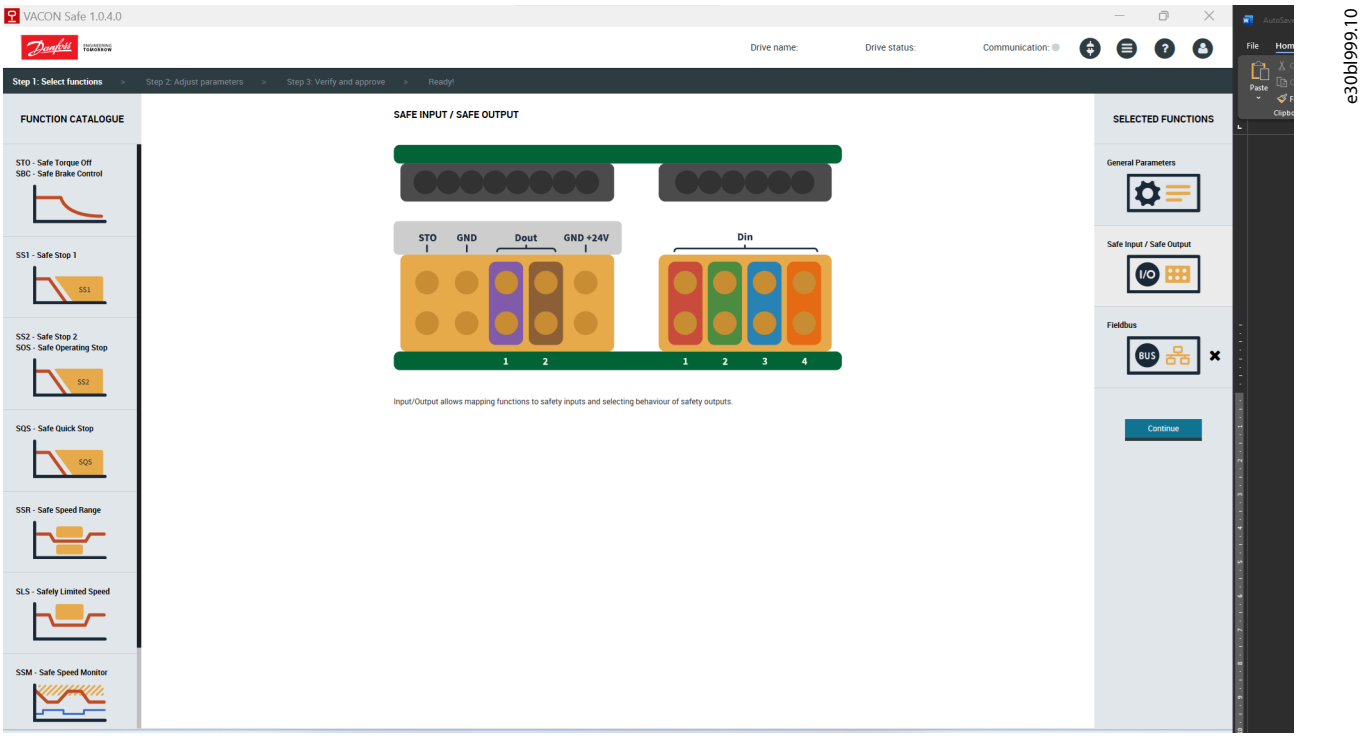


Figure 10: VACON® Safe PC tool

The VACON® Safe PC tool is a software used for to following reasons:

- Easy configuration.
- Customizing the safety application.
- Adapting the settings of safety parameters for the VACON® Advanced Safety Options OPT-BL/OPT-BM/OPT-BN.
- Easy integration Fail-safe controllers.
- Fail-safe I/O.
- Fail-safe drives allow the implementation of safety requirements in every machine.

The PROFIsafe device extends the advantages of functional safety to the next level of flexibility. It enables extension from an isolated safety device to interconnecting and cooperating safety-related devices within a plant.

7.4 VACON® NX Options concept

The VACON® option boards are divided in 5 groups according to their characteristics: types A, B, C, D, and E.

Usually, when the AC drive is delivered from the factory, the control unit includes at least the standard compilation of 2 basic boards (I/O board and relay board) which are normally installed in slots A and B. The I/O boards mounted at the factory are indicated in the type code of the AC drive. The 3 expander slots C, D, and E are available for different option boards, that is, I/O expander boards, fieldbus boards, and adapter boards.

OPT_ A

- Basic boards used for basic I/O (NXS, NXP); normally preinstalled at the factory.
- This board type uses Slots A, B, and C

OPT_B

- Option board used for I/O expansion.
- Normally plugged in to Slot B, C, D, and E

OPT-C and OPT-E

- Fieldbus boards (example Profibus or Modbus)
- These boards are connected to Slots D and E

NOTICE

- OPT-C types of boards legacy options, will not get any updates related to cybersecurity requirements.

OPT-D

- Adapter boards.
- Boards with fiber optic adapters. System Bus Fiber Optic Adapter Board.
- Connect the adapter board into Slot D and E.

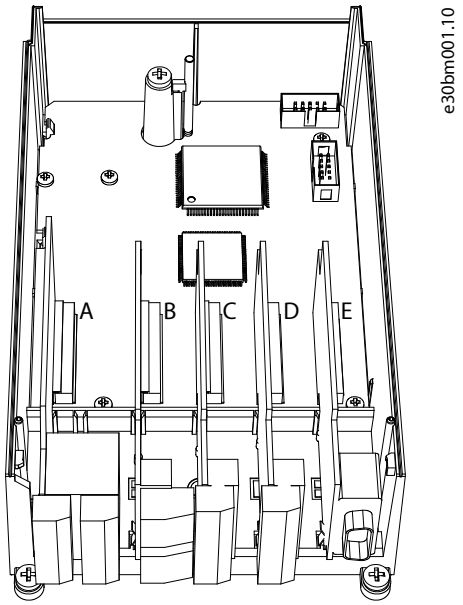


Figure 11: VACON® Option Board Slots

Table 7: Standard Option Boards

Type	Description	Card slot					Module			Card description
		A	B	C	D	E	AFE	INU	BCU	
Basic I/O boards (OPTA)										
OPTA1	DI/DO/AI/AO/ 10V/ 24 V	☐	–	–	–	–	☐	☐	☐	–
OPTA2	Relay output (NO/NC)	–	☐	–	–	–	☐	☐	☐	–
OPTA3	Relay output + Thermistor input	–	☐	–	–	–	☐	☐	☐	–
OPTA4	Encoder TTL type	–	–	☐	–	–	–	–	–	–
OPTA5	Encoder HTL type	–	–	☐	–	–	–	–	–	–
OPTA7	Double encoder HTL type	–	–	☐	–	–	–	–	–	–
OPTA8	OPTA1 + analog signals galvanically isolated as a group	☐	–	–	–	–	☐	☐	☐	–
OPTA9	OPTA1 + 2.5mm^2 connectors	☐	–	–	–	–	☐	☐	☐	–
OPTAE	Encoder HTL type (Divider + direction)	–	–	☐	–	–	–	–	–	–
OPTAF	STO, ATEX therm	–	☐	–	–	–	–	–	–	–
OPTAK	Sin/Cos encoder interface	–	–	☐	–	–	–	–	–	–
OPTAN	DI/AI/AO	☐	–	–	–	–	☐	☐	☐	–
I/O expander boards (OPTB)										
OPTB1	Programmable I/O	–	☐	☐	☐	☐	☐	☐	☐	–
OPTB2	Relay output + Thermistor input	–	☐	☐	☐	☐	☐	☐	☐	–
OPTB4	Analog input/output analog signals galvanically isolated separately	–	☐	☐	☐	☐	☐	☐	☐	–
OPTB5	Relay output	–	☐	☐	☐	☐	☐	☐	☐	–
OPTB8	Temperature Measurement option PT100	–	☐	☐	☐	☐	☐	☐	☐	–
OPTB9	DI + relay output	–	☐	☐	☐	☐	☐	☐	☐	–
OPTBH	Temperature Measurement option pt100, pt1000, Ni1000, KTY84	–	☐	☐	☐	☐	☐	☐	☐	–
OPTBB	EnDat + Sin/Cos 1 Vp-p	–	–	☐	–	–	–	☐	–	–
OPTBC	Resolver, 3xDO (Wide range)	–	–	☐	–	–	–	☐	–	–
OPTBE	EnDat/SSI/BiSS C	–	☐	☐	☐	☐	–	☐	–	–
OPTBL	Advanced safety option	–	–	☐	☐	☐	–	☐	–	–
OPTBM	OPTBL+ HTL/TTL encoder	–	–	☐	☐	☐	–	☐	–	–
OPTBN	OPTBL+ Sin/Cos encoder	–	–	☐	☐	☐	–	☐	–	–
Fieldbus boards (OPTC and OPTE)[(1)]										
OPTE2	RS485 with screw terminal	–	–	–	☐	☐	☐	☐	☐	RS485 with screw terminal
OPTE3	PROFIBUS DP with screw terminal	–	–	–	☐	☐	☐	☐	☐	PROFIBUS DP with screw terminal
OPTE5	PROFIBUS DP with D9-connector	–	–	–	☐	☐	☐	☐	☐	PROFIBUS DP with D9-connector
OPTE6	CANopen	–	–	–	☐	☐	☐	☐	☐	CANopen

Table 7: Standard Option Boards (continued)

Type	Description	Card slot					Module			Card description
		A	B	C	D	E	AFE	INU	BCU	
OPTE7	DeviceNet	–	–	–	☐	☐	☐	☐	☐	DeviceNet
OPTE8	RS485 with D9-connector	–	–	–	☐	☐	☐	☐	☐	RS485 with D9-connector
OPTE9	Dual-port Ethernet	–	–	–	☐	☐	☐	☐	☐	Dual-port Ethernet
OPTEA	Advanced Dual-port Ethernet	–	–	–	☐	☐	☐	☐	☐	Advanced Dual-port Ethernet
OPTC2	RS485 with screw terminal	–	–	–	☐	☐	☐	☐	☐	RS485 with screw terminal
OPTC3	PROFIBUS DP with screw terminal	–	–	–	☐	☐	☐	☐	☐	PROFIBUS DP with screw terminal
OPTC4	LonWorks	–	–	–	☐	☐	☐	☐	☐	LonWorks
OPTC5	PROFIBUS DP with D9-connector	–	–	–	–	☐	☐	☐	☐	PROFIBUS DP with D9-connector
OPTC6	CANopen	–	–	–	☐	☐	☐	☐	☐	CANopen
OPTC7	DeviceNet	–	–	–	☐	☐	☐	☐	☐	DeviceNet
OPTC8	RS485 with D9-connector	–	–	–	☐	☐	☐	☐	☐	RS485 with D9-connector
OPTCI	Modbus/TCP	–	–	–	☐	☐	☐	☐	☐	Modbus TCP
OPTCJ	BACnet MS/TP	–	–	–	☐	☐	☐	☐	☐	BACnet MS/TP
OPTCP	PROFINET I/O	–	–	–	☐	☐	☐	☐	☐	PROFINET I/O
OPTCQ	EtherNet/IP	–	–	–	☐	☐	☐	☐	☐	EtherNet/IP
Communication boards (OPTD)										
OPT-D1	SystemBus adapt, 2xfibre-optic	–	–	–	☐	☐	☐	☐	☐	System Bus adapter (2 x fiber optic pairs)
OPT-D2	SystemBus (1xfiber), isolated CAN	–	–	–	☐	☐	☐	☐	☐	System Bus adapter (1 x fiber optic pair) and CAN-bus adapter (galvanically de-coupled)
OPT-D3	RS232 adapter (no galvanically isolated)	–	–	–	☐	☐	☐	☐	☐	RS232 adapter board (galvanically decoupled), used mainly for application engineering to connect another keypad.
OPT-D6	CAN-Bus (galvanically decoupled)	–	☐	–	☐	☐	☐	☐	☐	CAN-bus adapter (galvanically decoupled)
OPT-D7	Line voltage measurement	–	–	☐	–	–	☐	☐	–	Line voltage measurement

1) OPTE series fieldbus boards provides the most recent features on the market and they are recommended for new installation.

VACON® NX frequency converters can be connected to Ethernet using an Ethernet fieldbus board **option board:**

- OPTCI-MODBUS/TCP
- OPTCQ-ETHERNET IP
- OPTCP Profinet
- OPTE9 Dual Port Ethernet
- OPTEA Advanced Dual Port Ethernet

The option boards can be installed in the board slots D or E.

7.5 VACON® NX Drive Option boards Software

VACON® NCIPConfig

A software tool used for managing Ethernet-based network options for the VACON® NXP communication option cards and for updating option card software.

Update the OPTCI option board program with the NCIPConfig tool

Sometimes, it may be necessary to update the option board's firmware. Differing from other VACON® option boards, the EtherNet/IP option board's firmware is updated with the NCIPConfig tool.

NOTICE

- The IP addresses of the PC and the option board must be in the same area when the software is loaded. To start the firmware update, scan the nodes in the network according to the instructions. Once all the nodes are in the view, the new firmware can be updated by clicking the VCN packet field in NCIPCONFIG 's table view on the right.

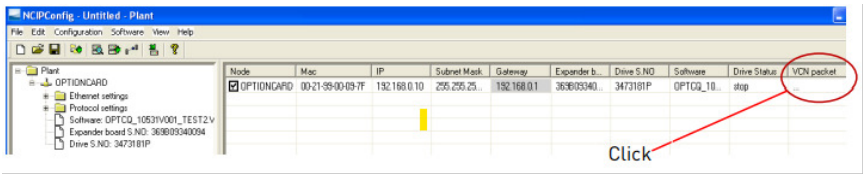


Figure 12: Update VCN Packet Field on NCIPConfig Tool

Choose a new firmware packet from the open window pop-up.

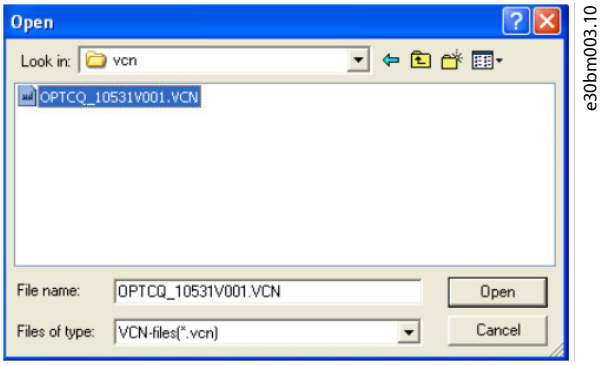


Figure 13: Choose a New Firmware Packet

Send the new firmware packet to the option board by checking its box in the ***VCN Packet*** field at the right corner of the table view. After selecting all nodes to be updated by checking the boxes, send the new firmware to the board by selecting ***Software*** then ***Download***.

NOTICE

DO NOT DO A POWER-UP CYCLE WITHIN 1 MINUTE AFTER DOWNLOADING THE OPTION BOARD SOFTWARE.

This may cause the option board to go to “Safe Mode”.

- This situation can only be solved by re-downloading the software. The Safe Mode triggers a fault code (F54). The board slot error F54 may also appear due to a faulty board, a temporary malfunction of the board, or disturbance in the environment.

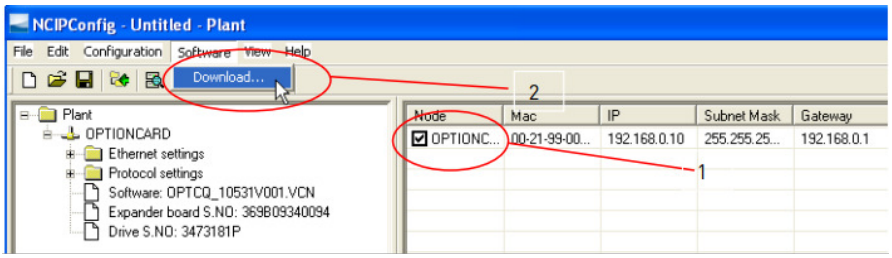


Figure 14: Send the New Firmware to the Board

OPTEA and OPTE9 boards enable updating option board firmware over Ethernet with VACON® Loader

VACON® Loader:

VACON® Loader is used to update drive firmware for the VACON® 100 family, VACON® 20, and VACON® OPT_E Options family drive products.

Included in the full VACON® Live installation package.

Updating Firmware over Ethernet with VACON® Loader:

Use these instructions to upload the Fieldbus or VACON® control firmware over Ethernet with VACON® Loader.

OPTEA and OPTE9 boards enable updating option board firmware over Ethernet with VACON® Loader. The option board works as a gateway for the firmware update. It means that it is not possible to update the firmware of the option board which is being used as the update gateway.

If the firmware loading fails (for example, network is lost during update), the option board remembers the used Ethernet settings and remains in state waiting for reconnection and firmware update.

Setting the drive parameters with VACON® NC Drive

Use these instructions to set the drive parameters with VACON® NCDrive.

Also, option board parameters can be configured with VACON® NCDrive (except for the PROFINET NameOfStation parameter). However, it is recommended to use the VACON® NCIPConfig tool to configure the option board in the VACON® NXS/P AC drives.

Make sure that the option board IT settings are configured with VACON®NCIPConfig.

NOTICE

- The VACON® NCDrive software is recommended to be used in LAN (Local Area Network) only.

8 Security Configuration Guidelines

8.1 Introduction to Recommendations

There are different possibilities to prevent access to local or remote, to change settings, and to view data or settings in the VACON® drives. From the below described principles, it is up to the system integrator to decide which principles give the needed protection for the system.

Reduction of the attack surface

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

Protection of access to enclosures and rooms

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

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

8.2 Security Recommendations

8.2.1 Local Access

Protection methods, recommendations for drives in protection class IP21/IP54/IP55/IP66

The VACON® NX drives of protection class IP55/66 are as IP20 to be used for installation in a lockable control cabinet/switching room. The locked control cabinet/switching room must provide sufficient protection against access by unauthorized persons.

For installation where the above described access prevention is not possible, the following prevention methods can be recommended:

- Removing the control panel from the VACON® NX drives under normal operation. If unintended access should happen, removing the control panel prevents access to, for example, the drive parameters. In service cases, an control panel can be handed out by the owner of the installation to a trusted person, for example, a trained service technician.
- For having access to USB port and Ethernet TCP/IP, the front cover must be removed using tools. This will complicates access at certain levels but not fully prevent access. But for security level SL-1, this is seen as fulfilling the requirements.

8.2.2 Connection to Trusted/Untrusted Networks

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

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

VACON® NX drives must only be connected inside the trusted networks, which ensure that the measure for access is under control.

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

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

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

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

Ethernet options:

Ethernet option module must be positioned in a trusted network.

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

- PC tool communication
- Change of IP settings remotely using NCP IP configuration tool
- Ping response
- VACON® NX drives do not support wireless connections. Remote access is possible only via other devices. It is not recommended to provide remote access through any devices other than PLC.

8.2.3 Unused Ports

The drives have pins that enable different ports when option boards are used. Therefore, there are only ports that are used. If there are unused ports, integrators must take protection measures to protect the integrity of the drive.

8.2.4 Secure Password Recommendations

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

It is important to:

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

When updating passwords, consider the following guidelines:

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

8.2.5 Service

PLC detects when the drives are in service mode. The service is done using PC software tools which are operated on the service PC. The drives have a Com Port interface to provide connection to the service PC. During the service a trusted person, for example, a trained service technician is allowed to attach only trusted devices to the drive.

Recommendations for service PC:

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

9 Software and Firmware Updates

- VACON® NCLoad: A software tool for updating drive firmware and installation of software applications for the VACON® NXP family drive products.
- VACON® NC Drive: A software tool used for commissioning, parameterization, monitoring, and diagnosing VACON® NXP family drive products.
- VACON® NCIPConfig: A software tool used for managing ethernet-based network options for the VACON® NXP communication option boards and for updating option board software.
- VACON® Safe: A software tool used for easy configuration, customizing the safety application, and adapting the settings of safety parameters for the VACON®Advanced safety options OPT-BL/OPT-BM/OPT-BN.
- VACON® Loader: VACON® Loader is used to update drive firmware for the VACON® NX family Options firmware update.
- VACON® Service Tool: The device properties service programming tool sets up instructions to control unit and power unit. The software *Device properties service.exe* is available on the Danfoss drives service extranet.
- Included in the full VACON® Live installation package.

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

10 Supplier Documentation

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

- The design guide provides specifications and information to be used when including the VACON® drive in an application.
- The operating guide provides detailed information for the installation and start-up of the drive.
- The programming guide provides greater detail on how to work with parameters. It also contains application examples.
- The condition-based monitoring programming guide provides information on working with condition-based monitoring (CBM) parameters on the Danfoss VACON® AC drives.
- The VACON® 100 INDUSTRIAL, FLOW, and 100 X installation guide describes how to select the optimal brake resistor.
- The OPT-AF safe torque off, ATEX option board user manual, and advanced safety options operating guide describes how to use Danfoss VACON® drives in functional safety applications. This manual is supplied with the drive when the Safe Torque Off option is selected.
- The VACON® NX brake resistor user manual describes how to select the optimal brake resistor.
- The VACON® NX Active Front (AFE) user manual provides with the necessary information about the installation, commissioning, and operation of VACON® NX Active Front End.
- The active front end application manual provides information about the active front end application.
- The VACON® filter guide provides information about RFI-filters, dU/dt filters, and sinus filters.
- Supplemental publications, drawings, EPLAN macros, and manuals are available at www.danfoss.com.

Optional equipment is available that may change some of the information described in these publications. Be sure to follow the instructions supplied with the options for specific requirements.

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

ENGINEERING
TOMORROW

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