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® 100 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 5

1.2 Extended requirements 5

1.2.1 DNV: Rules for Classification Ships Edition July 2023 6

1.3 Document Version 6

2 Safety

2.1 Safety Precautions 7

2.2 Qualified Personnel 7

3 Security Measures

4 Security Management

4.1 Overview 9

4.2 Procedure 9

5 IEC 62443-4-2 Certification

6 Extended Requirements

6.1 Overview 11

6.2 DNV Rules for Classification Ships edition July/2023 11

6.2.1 DNV Rules for Classification Ships edition July/2023 11

6.2.2 Color code and Mitigation list 11

6.2.3 Codes for Mitigation to be Achieved with Other Means 12

6.2.4 DNV July/2023 UR E27 Requirements Mitigation List 12

7 Device Specifications

7.1 VACON® 100 Drives 18

7.2 Default Interfaces 19

7.2.1 Overview 19

7.2.2 Control Panel 19

7.2.2.1 Control Panel and Keypad 19

7.2.2.2 Display 19

7.2.2.3 Local and Remote Application 19

7.2.2.4 Application Settings 19
7.2.2.5 User Levels 19
7.2.2.6 Fire Mode 21
7.2.2.7 Copying Parameters 21
7.2.2.8 USB and RS485 21
7.3 Software for VACON® 100 Drives 22

8 **VACON® Live**

8.1 Online Connection 23
8.2 VACON® 100 Options Concept 24
8.2.1 VACON® 100 Options Concept 24
8.2.2 VACON® 100 Option Cards Software 27

9 **Security Configuration Guidelines**

9.1 Introduction to Recommendations 29
9.2 Security Recommendations 29
9.2.1 Local Access 29
9.2.2 Connection to Trusted/Untrusted Networks 29
9.2.3 Unused Ports 30
9.2.4 Secure Password Recommendations 30
9.2.5 Service 30

10 **Software and Firmware Updates**

11 **Supplier Documentation**

1 Introduction

1.1 Purpose of this document

The unified requirement 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® 100 drive as a component in the system. Drives in scope for this document: VACON® 100 and VACON® 100X, in this document referred to as VACON® 100 drives.

As product supplier, Danfoss shares information on VACON® 100 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 requirement 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® 100 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.

Target security level for VACON® 100 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 6.2.4 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.

In this document, a list of issuers with extended requirements can be found:

1.2.1 DNV: Rules for Classification Ships Edition July 2023

The Unified Requirements E26 and E27 are the bases for DNV: Rules for Classification Ships Edition July 2023. In this document, DNV Rules for Classification Ships Edition July 2023 is used as 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 6.2.4 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® 100 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® 100 drives are working towards IEC 62443-4-2 SL1 certification.

6 Extended Requirements

6.1 Overview

In this section, requirements in relation to specific approvals or certificates are listed. These requirements can either have been extended or limited towards IEC 62443.

6.2 DNV Rules for Classification Ships edition July/2023

6.2.1 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.

6.2.2 Color code and Mitigation list

In section 6.2.4 DNV July/2023 UR E27 Requirements Mitigation List, the following color codes will be used to indicate 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.

6.2.3 Codes for Mitigation to be Achieved with Other Means

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

ID	Description
M1	**Access control for enclosure or room where FC drives are installed** The most basic line of defense is physically shielding the drives in enclosures or rooms with access control. The enclosure or room can have access control by locking mechanism where special tools, special keys, or access codes are needed to access the enclosure or room. Only qualified personnel have the means to get access.
M2	**Remove control panel from VACON® 100 drive to prevent local access** Remove the control panel from the VACON® 100 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® 100 drives dose 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 andwell-hosted portion of a certain network or control system. For recommendations to achieve security level SL-1, see section 9.2.1 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.

6.2.4 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. Will be updated once authentication enforcements are implemented.
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. 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 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® 100 related events. VACON® 100 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® 100 related events. VACON® 100 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® 100 related events. VACON® 100 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 needs to 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® 100).
Malicious code protection		

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)
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 • To protect against loading malicious software packages – Software packages are encrypted (firmware). • Software packages are obtained only from trusted source (for example, 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, 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 secure service policy. Software tools provide capability to test that everything work 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 will reach 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 upon 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 have read authorization.	YES	M1 + data is control data.
Use of cryptography		

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)
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		
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® 100 related events. VACON® 100 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 control system level. 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, for example, shutdowns, alarming, and monitoring over lower priority tasks such as, for example, networks scans.	YES	There is task management (Priority schema in OS).
Control system backup		

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 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.
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 is only used ports and protocols related to option boards but there is always built-in ethernet port is available+M1. • Not needed functionalities are disabled, and there are mechanisms to prevent enabling them.

1) SP1: Required for cybersecure (Essential). Corresponds to IEC62443 SL1 – Protection against casual or coincidental violation.

7 Device Specifications

7.1 VACON® 100 Drives

Frequency converter for use in various marine applications. Applicable in 3 enclosure options:

- Wall-mounted [1], IP21/IP54
- IP00 module[1]
- Enclosed drive[1], IP21/IP54

NOTICE

- Converters EMC classed C2 according to IEC 61800-3 can be installed in “special distribution zone” and “general power distribution zone” in accordance with IEC 60533 provided that precautions are taken to attenuate these effects on the distribution system, so the safe operation is assured.

Feature	Description
Supply voltage range	208-240V/380-480V/380 -500V/525-690V, 50/60 Hz
Voltage variation	- 15%, +10% continuously
Frequency variation	47.5–66 Hz
Output frequency	0–320 Hz
Temperature range in operation	0–40°C (40–60°C when derated 2.5%/°C)
Temperature class	A
Vibration class	A
Humidity class	A
EMC class	DNVGL-CG-0339 general power distribution zone

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, Industrial, Pump, Solar 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.

1) To be installed in an enclosure with an IP degree in accordance with DNV GL Rules with respect to the location.

7.2 Default Interfaces

7.2.1 Overview

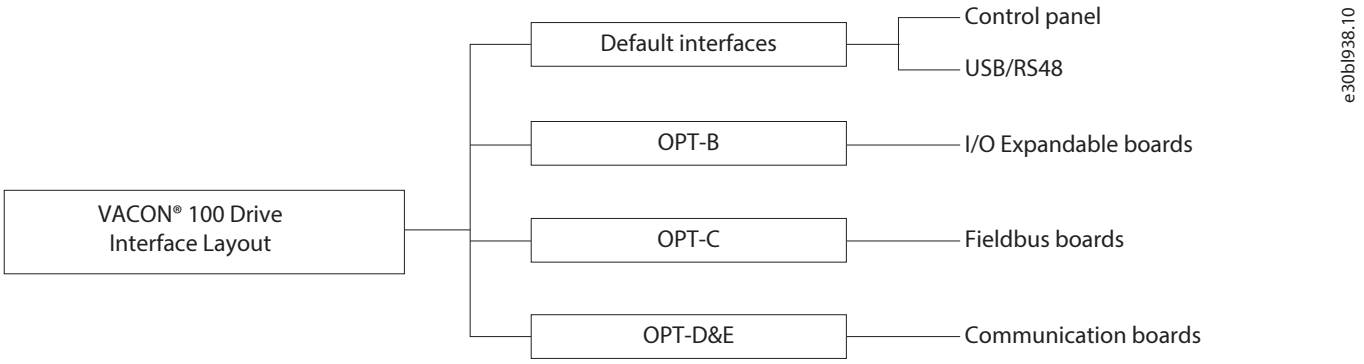


Figure 1: Default Interfaces VACON® 100 Drives

7.2.2 Control Panel

7.2.2.1 Control Panel and Keypad

The control panel is the interface between the AC drive and the user. Use the control panel to control the speed of a motor and monitor the status of the AC drive. The control panel can also be used to set the parameters of the AC drive.

7.2.2.2 Display

Display types: the graphical display. The control panel always has the same keypad and buttons. The display shows this data.

- The status of the motor and the drive.
- Faults in the motor and in the drive.
- The current location in the menu structure.

7.2.2.3 Local and Remote Application

- Use the Local/Remote application when, for example, it is necessary to switch between 2 different control places.
- To change between the Local and the Remote-control place, use DI6. When Remote control is active, give the start/stop commands from fieldbus or from I/O terminal (DI1 and DI2). When Local control is active, give the start/stop commands from the keypad.
- Select the frequency reference for each control place from the keypad, fieldbus, or I/O terminal (AI1 or AI2).
- It is possible to configure all the drive outputs freely in all the applications. There are 1 analog output (Output Frequency) and 3 relay outputs (Run, Fault, Ready) available on the basic I/O board.

7.2.2.4 Application Settings

- P3.11.1 PASSWORD (ID 1806) Use this parameter to set the administrator password.

7.2.2.5 User Levels

7.2.2.5.1 Using the User Levels Menu

Use the User level parameters to keep the personnel who are not approved from making changes in, and prevent accidental changes to, the parameters.

When selecting a user level, the user cannot see all the parameters on the display of the control panel.

7.2.2.5.2 User Lever Parameters

Index	Parameter	Min.	Max.	Unit	Default	ID	Description
P8.1	User level	1	3		1	1194	1 = Normal. All the menus are visible in the main menu. 2 = Monitoring. Only the monitoring and user level menus are visible in the main menu. 3 = Favourites. Only the favourites and user level menus are visible in the main menu. 4 = Monitoring & Favourites. Monitoring, favourites, and user level menus are visible in the main menu.
P8.2	Access code	0	99999		0	2362	If the value is set to be other than 0 before going to Monitoring from, for example, Normal, the access code has to be given when going back to Normal. This prevents personnel who are not approved from making changes in the parameters on the control panel.

⚠ CAUTION

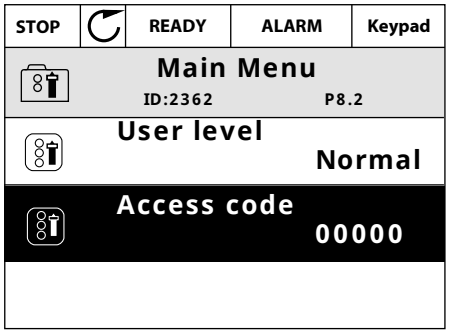
DO NOT LOSE THE ACCESS CODE.

- If the access code is lost, contact the nearest service center or partner.

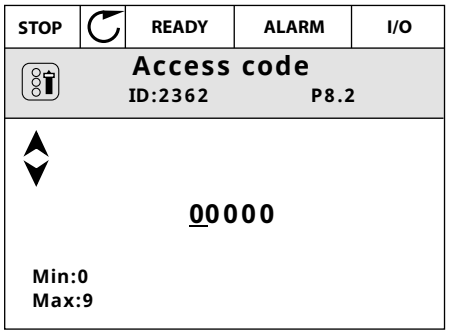
7.2.2.5.3 Changing the Access Code of the User Levels

Procedure

1. Go to the *User levels*
2. Go to the item *Access code* and push the arrow button Right.



3. To change the digits of the *access code*, use all the arrow buttons.



4. Accept the change with the *OK* button.

7.2.2.6 Fire Mode

When ***fire mode*** is active, the drive resets all faults that occur and continues to operate at the same speed until it is not possible. The drive ignores all commands from the keypad, fieldbuses, and the PC tool. It only obeys the signals ***Fire mode activation***, fire mode reverse, run enable, run Interlock 1, and run Interlock 2 from I/O.

The fire mode function has 2 modes, the test mode and the enabled mode. To make a selection of a mode, write a password in ***parameter P3.17.1 (Fire Mode Password)***. In the test mode, the drive does not automatically reset the faults, and the drive stops when a fault occurs.

It is also possible to configure fire mode with the fire mode wizard, which is activated in the Quick Setup menu with ***parameter B1.1.4***. When fire mode is active, an alarm is shown on the display.

7.2.2.7 Copying Parameters

NOTICE

- This feature is available with graphical keypad only. The parameter copy function can be used to copy parameters from one drive to another.

The parameters are first saved to the keypad, then the keypad is detached and connected to another drive. Finally, the parameters are downloaded to the new drive restoring them from the keypad.

Before any parameters can successfully be copied from one drive to another, the drive has to be stopped when the parameters are downloaded.

Go to *user settings menu* and locate the *parameter backup submenu*. In the *parameter backup submenu*, there are 3 possible functions to be selected:

- Restore factory defaults will re-establish the parameter settings originally made at the factory.
- Select Save to keypad to copy all parameters to the keypad.
- Restore from keypad will copy all parameters from keypad to a drive display.

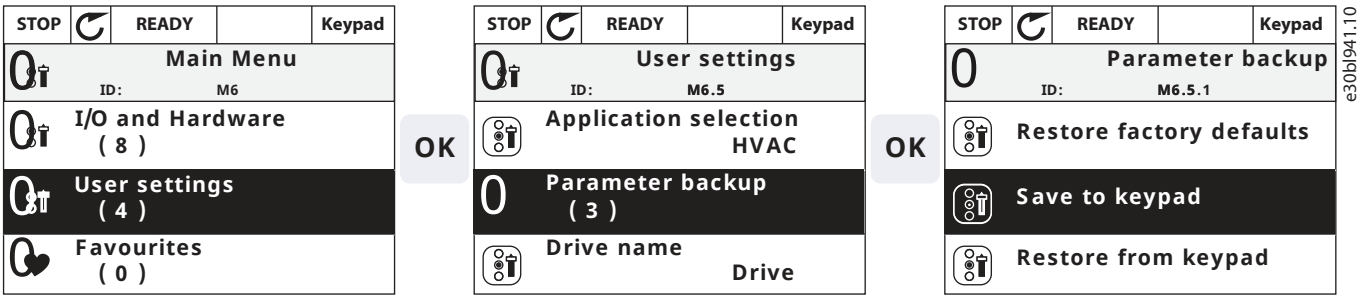


Figure 2: Copying Parameters to a Drive Display

7.2.2.8 USB and RS485

- To download a new software, connect the PC into the control panel connector with the CAB-USB/RS485
- When the drive is supplied from mains, download a new software with the VACON® Loader PC tool and a CAB-USB/RS485 cable.
- When the drive is not supplied from mains, use an external 24 V DC power supply to power-up to the control unit. In MR8 and MR9, the external 24 V DC powers up the control unit, and in MR10 and MR12, it powers up to the control unit and the measurement board(s). After the power-up, download the software.

7.3 Software for VACON® 100 Drives

Table 6: Software for VACON® 100 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® Live	A software tool used for commissioning, parameterization, monitoring and diagnosing, VACON® 100 family and VACON® 20 family drive products. Included is VACON® Loader for updating drive firmware.	
Firmware, Application & Option boards Software Update		
VACON® Loader	VACON® Loader is used to update drive firmware for the VACON® 100 family and VACON® 20 family drive products. Included in the full VACON® Live installation package.	

8 VACON® Live

8.1 Online Connection

When opening the application, user will be asked to operate online or offline.

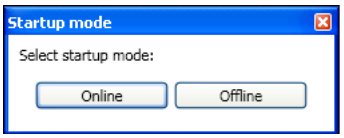


Figure 3: Online/Offline Selection Dialog

Online connection requires defining some communication settings. Devices can be also searched by pressing the *Scan* button. Devices can connected via Serial or Ethernet.

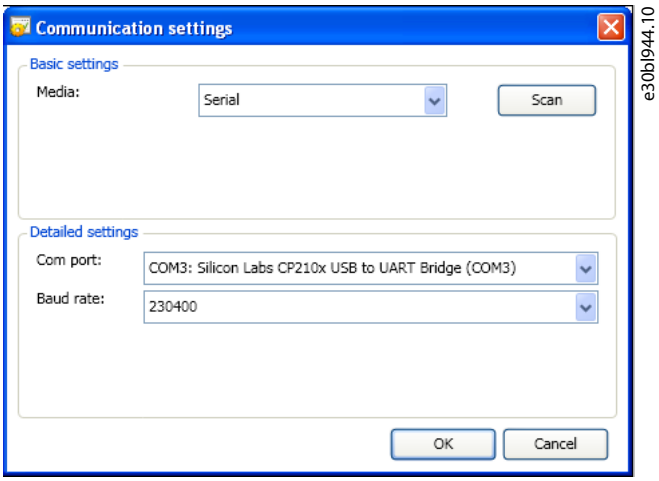


Figure 4: Defining Serial Settings

While defining the Ethernet settings, it is possible to add multiple favorite Ethernet addresses to a favorite list by writing the IP-address of the device to the field and by pressing *Add* button. From the favorite list it's possible to connect multiple devices simultaneously by selecting the addresses from the favorite list and by pressing the *OK* button.

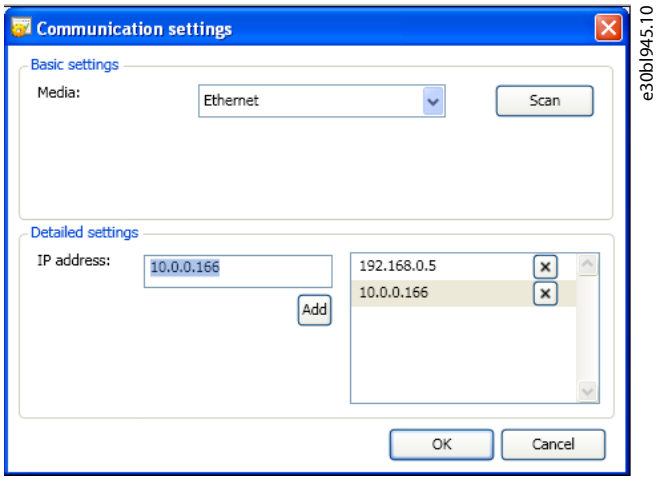


Figure 5: Defining Ethernet Settings

Use the ***scan view*** to select which devices to connected to. ***Scan view*** searches devices only from selected media. User can also enable automatic scanning from ***options***. Automatic scan searches devices from all connected media. If only 1 device is found, the application will automatically connect to that device.

NOTICE

- If problems occur with finding devices while bluetooth devices are enabled, disconnect bluetooth. Sometimes bluetooth devices create multiple virtual serial ports, which might cause long delay to serial port scanning.

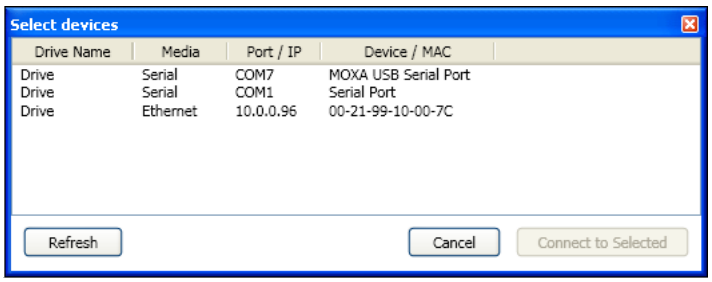


Figure 6: Device Scanning

After settings are defined, the application will connect to the desired device.

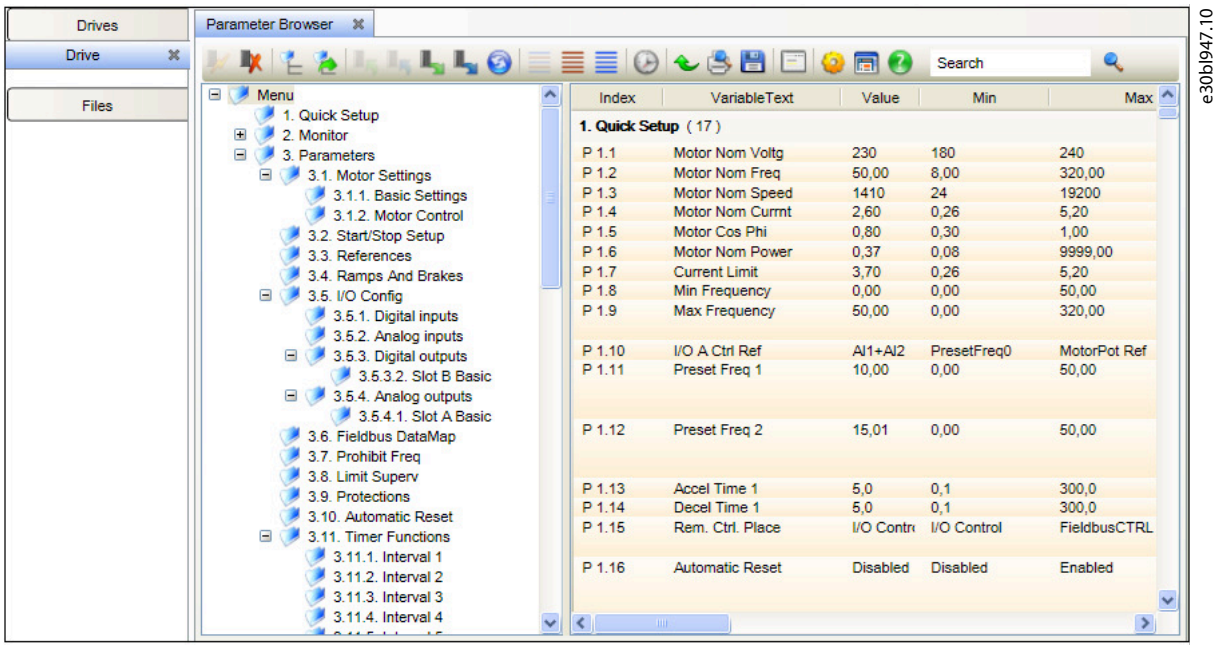


Figure 7: Device has been Connected

If the application was opened in offline state, online connection can still be created by selecting ***New Drive*** from ***Drive menu***. This action opens same settings dialog as shown when opening the application.

8.2 VACON® 100 Options Concept

8.2.1 VACON® 100 Options Concept

The control board is situated inside the control unit of the VACON® 100 drive. There are 2 board slots (labelled D and E) on the VACON® 100X control board and 3 board slots (labelled C, D and E) on the VACON® 100, VACON® 100 FLOW, and VACON® 100 HVAC control board.

Usually, when the AC drive is delivered from the factory, the control unit includes at least the standard board, which is installed in the standard board slot. The I/O boards mounted at the factory are indicated in the type code of the AC drive. The expander slots D, E (VACON® 100X) and C, D, E (VACON® 100, VACON® 100 FLOW, VACON® 100 HVAC) are available for different option boards.

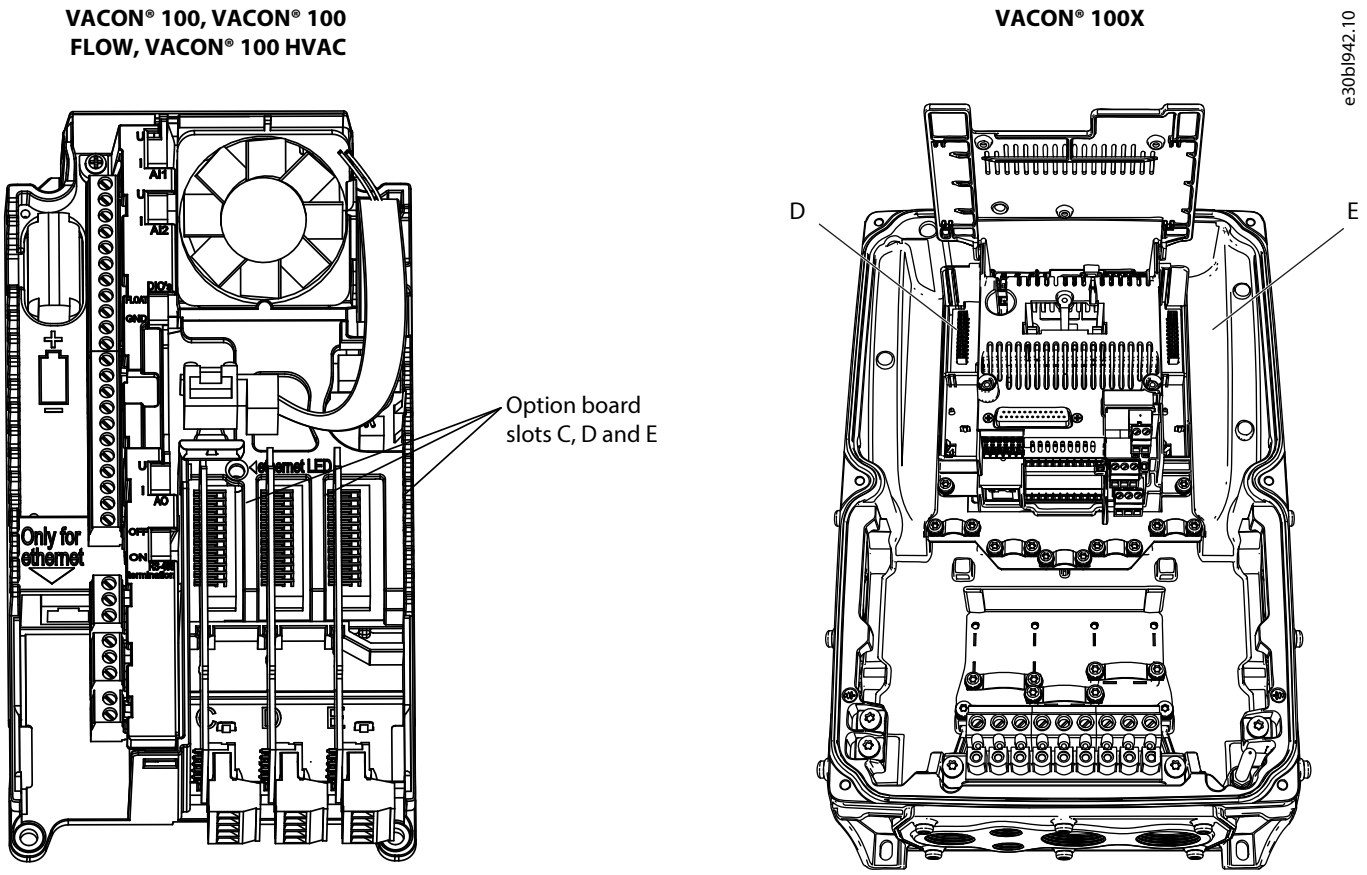


Figure 8: The Expander Slots for Different Option Boards

Table 7: Options for VACON® 100 INDUSTRIAL, VACON® 100 FLOW

Factory option	Loose option	Description	Option slot				AC drive		
			B	C	D	E	VACON® 100 INDUSTRIAL	VACON® 100 FLOW	Enclosed
I/O options									
-	OPT-F3-V	Standard I/O board: 2 x AI, 6 x DI, 1 x AO, 10 Vref, 24 Vin, 2 x 24 Vout, RS485, 3 x RO	☐	☐			☐	☐	☐
+SBF4	OPT-F4-V	Optional I/O board: 2 x AI, 6 x DI, 1 x AO, 10 Vref, 24 Vin, 2 x 24 Vout, RS485, 2 x RO, Thermistor input	☐				☐	☐	☐
+S_B1[1]	OPT-B1-V	6 x DI / DO, programmable		☐	☐	☐	☐	☐	☐
+S_B2[1]	OPT-B2-V	2 x RO, Thermistor input		☐	☐	☐	☐	☐	☐
+S_B4[1]	OPT-B4-V	1 x AI, 2 x AO (isolated)		☐	☐	☐	☐	☐	☐
+S_B5[1]	OPT-B5-V	3 x RO		☐	☐	☐	☐	☐	☐
+S_B9[1]	OPT-B9-V	1 x RO, 5 x DI (42-240 VAC)		☐	☐	☐	☐	☐	☐
+S_BF[1]	OPT-BF-V	1 x AO, 1 x DO, 1 x RO		☐	☐	☐	☐	☐	☐
+S_BH[1]	OPT-BH-V	3 x Temp sensor inputs (PT100, PT1000, KTY84-130, KTY84-150, KTY84-131, NI1000)		☐	☐	☐	☐	☐	☐
Communication options									

Table 7: Options for VACON® 100 INDUSTRIAL, VACON® 100 FLOW (continued)

Factory option	Loose option	Description	Option slot				AC drive		
			B	C	D	E	VACON® 100 INDUSTRIAL	VACON® 100 FLOW	Enclosed
+FBIE	-	Industrial Ethernet protocols: PROFINET IO and EtherNet/IP (software option on-board					☐	☐	☐
+S_C4[(1)]	OPT-C4-V	LonWorks			☐	☐	☐	☐	☐
+S_E3[(1)]	OPT-E3-V	PROFIBUS DPV1			☐	☐	☐	☐	☐
+S_E5[(1)]	OPT-E5-V	PROFIBUS DPV1 (D9)			☐	☐	☐	☐	☐
+S_E6[(1)]	OPT-E6-V	CANopen			☐	☐	☐	☐	☐
+S_E7[(1)]	OPT-E7-V	DeviceNet			☐	☐	☐	☐	☐
+S_EC[(1)]	OPT-EC-V	EtherCAT			☐	☐	☐	☐	☐
Other options									
+S_BJ[(1)]	OPT-BJ-V	Safe Torque Off (STO) / Safe Stop 1 (SS1) / ATEX				☐		☐	☐
+HMTX	VACON-PAN-HMTX-MK01	Text keypad					☐	☐	☐
+HMPA	PAN-HMPA-MK01	Panel adapter IP54 (dummy keypad)					☐	☐	☐
+SRBT	-	Real time clock battery					☐	☐	
+IP54	VACON-ENC-IP54-MR04/05/06	IP54 enclosure; loose option also available for frames MR4, MR5, MR6					☐	☐	☐
+IP00	-	IP00 available for frames MR8-MR12					☐	☐	
+EMC4	-	Change to EMC-level C4 for IT networks					☐	☐	☐
+DBIN	-	Internal integrated dynamic braking MR7-MR12					☐		☐
+QFLG	ENC-QFLG-MR04/05/06/07	Flange mounting MR4-MR7 / MR8 IP00 / MR9 IP00 Loose option available for frames MR4-MR7					☐	☐	
+QDSS	-	Drive supply switch for MR4-MR7 (IP54) and MM4-MM6					☐	☐	
+QGLC	-	Conduit plate with inch holes, MR4-MR9					☐	☐	☐
+EMAR	-	Marine construction					☐	☐	☐
+POCM	-	Integrated common mode filter for IP00 frames MR10 and MR12 and enclosed drives					☐	☐	☐
+PODU	ENC-QMMF-MM04/05/06	Integrated dU/dt filter for IP00 frames MR10 and MR12 and enclosed drives					☐	☐	☐
+PCTB	-	External power connection block for IP00 frames MR10 and MR12					☐	☐	

Table 7: Options for VACON® 100 INDUSTRIAL, VACON® 100 FLOW (continued)

Factory option	Loose option	Description	Option slot				AC drive		
			B	C	D	E	VACON® 100 INDUSTRIAL	VACON® 100 FLOW	Enclosed
Kits and cables									
-	VACON-PAN-HMDR-MK01-xx	VACON® 100 door mounting kit, xx = cable lengths NM (no cable), 2M, 3M, 6M, 15M (2, 3, 6, 15 meter)							
-	VACON-PAN-HMHH-MK01	Hand held panel kit, VACON brand							
-	CAB-USB/RS485	PC cable for SW tools, USB to RS-485, cable length 3 m							
-	VACON-ENC-IN12-MR0x	Type 12 kit, 0x = enclosure sizes (04, 05, 06)							

1) Replace '_' with preferred option slot (Example +SCB5 means option board B5 will installed to option slot C in factory)

Table 8: Allowed slots on VACON® drives

I/O board	VACON® 100, VACON® 100 FLOW, VACON® 100 HVAC	VACON® 100X
Board OPTB1	C,D,E	D,E
Board OPTB2	C,D,E	D,E
Board OPTB4	C,D,E	D,E
Board OPTB5	C,D,E	D,E
Board OPTB9	C,D,E	D,E
Board OPTBF	C,D,E	D,E
Board OPTBH	C,D,E	D,E
Board OPTF3	C,D,E	-
Board OPTF4	C,D,E	-

8.2.2 VACON® 100 Option Cards Software

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.

9 Security Configuration Guidelines

9.1 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® 100 drive. From the below described principles, it is up to the system integrator to decide which principles give the needed protection for the system.

Reduction of the attack surface

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

Protection of access to enclosures and rooms

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

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

9.2 Security Recommendations

9.2.1 Local Access

Protection methods, recommendations for drives in protection class IP00/IP21/IP54

The VACON® 100 drives of protection class IP54 are as IP00, IP20, and IP21 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® 100 drives under normal operation. If unintended access should happen, removing the control panel will prevent 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.

9.2.2 Connection to Trusted/Untrusted Networks

The *trusted network* as being a strictly limited and well-hosted portion of a certain network or control system.

If network deployment will be in an uncontrolled environment without responsible physical access control and account/domain management, as being a strictly limited and well-hosted portion of a certain network or control system.

VACON® 100 drives shall be connected only inside the trusted networks, which will ensure that the measure for access is under control.

This connection shall be created so that the drive connects only to the PLC point-to-point or via switches. Switches shall 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 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® 100 drives does 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 VACON® 100 Live tool
- Ping response
- VACON® 100 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.

9.2.3 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.

9.2.4 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.

9.2.5 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.

10 Software and Firmware Updates

- VACON® Live A software tool used for commissioning, parameterization, monitoring, and diagnosing VACON® 100 family and VACON® 20 family drive products. Included is VACON® Loader for updating drive firmware.
- VACON® Loader: VACON® Loader is used to update drive firmware for the VACON® 100 family and VACON® 20 family drive products.
- Included in the full VACON® Live installation package.

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

11 Supplier Documentation

Various resources are available to give a better understanding of installation and making use of advanced drive operation, programming, and directives compliance. Below list are documents which is 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 VACON® filter guide provides information about RFI-filters, dU/dt filters, and sine filters.
- Supplemental publications, drawings, EPLAN macros, and manuals are available at www.danfoss.com.

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

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

ENGINEERING
TOMORROW

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

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