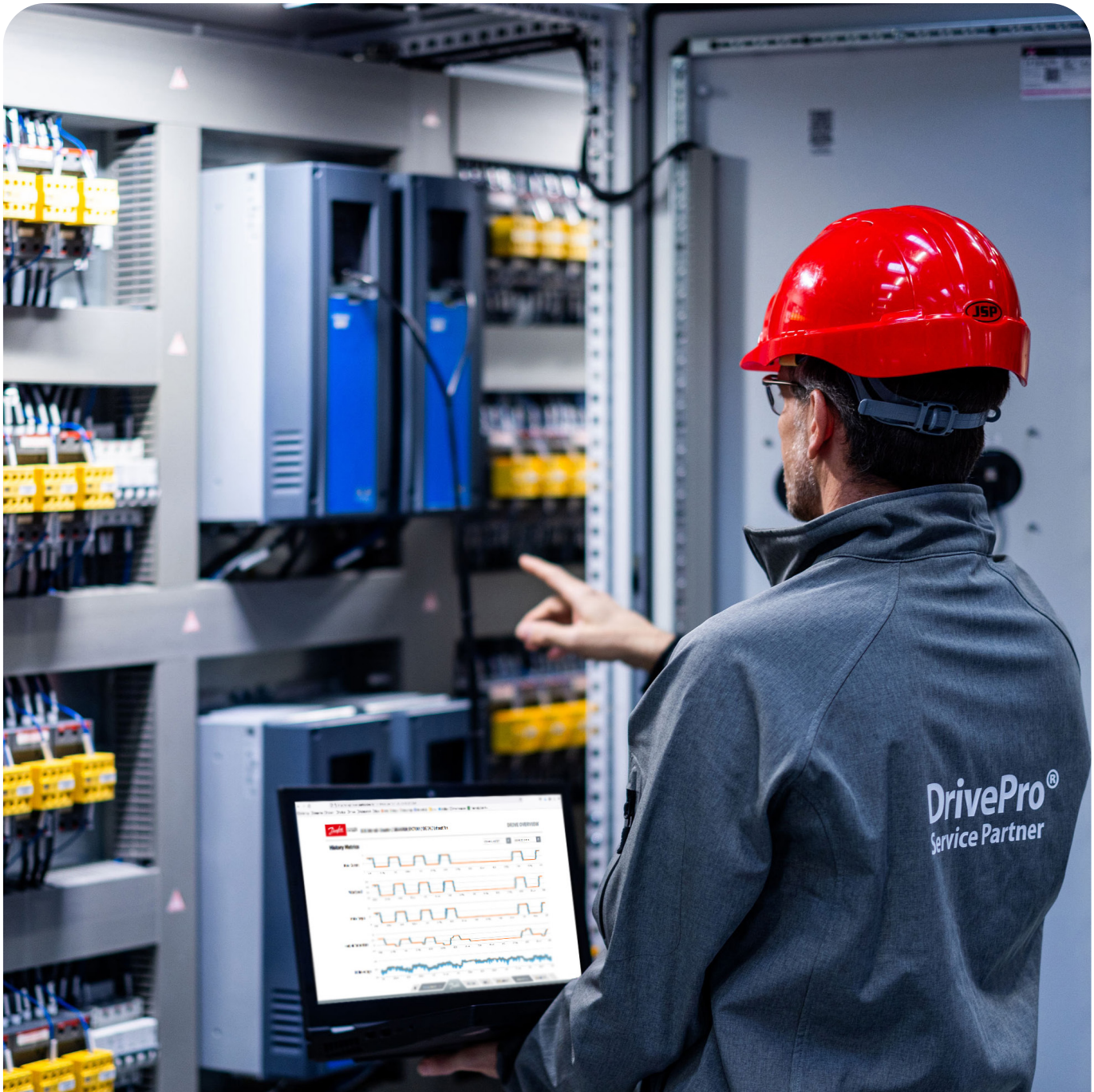
Application Paper | DrivePro® Services
BE523146459201en-000101

DrivePro®
Remote Monitoring
Cybersecurity




DrivePro®
Service Partner
DrivePro®
ThinkPad

Table of contents

Introduction

The global cybersecurity landscape is undergoing a significant transformation, with the introduction of the most stringent cybersecurity legislation ever, for both entities and products. These cybersecurity regulations are concurrently enforced via mandatory requirements related to market access of products and purchasing of operational systems for entities globally.

In Europe, the NIS2 Directive is effective from October 10, 2025. NIS2 requires essential and important entities, all manufacturers and their supply chains, to implement robust information security management systems and secure development procedures for operational systems.

To continue legal sale in the EU, all other software and hardware products must comply with the Cyber Resilience Act Article 11 from Q4 2025 forwards . Products subject to the requirement include Machinery Directive-compliant products, and their vulnerability management processes (at a minimum). The EU Cyber Resilience Act applies from mid-2027 onwards including essential requirements like regular security testing and update management, among others.

Many of today's wireless IoT products must be fully redesigned and made secure-by-design-and default. They must comply with Radio Equipment Directive essential requirements 3 (3def and Article 6), to continue legal sales in the EU from Q4 2025 onwards.

This paper describes cybersecurity considerations outlined in EU and global cybersecurity regulations and standards applicable to the DrivePro® Remote Monitoring solution. It provides readers with insights into the dedicated cybersecurity components which are integrated into the DrivePro® Remote Monitoring solution. These components ensure compliance with the regulations and standards, ultimately building a resilient system.

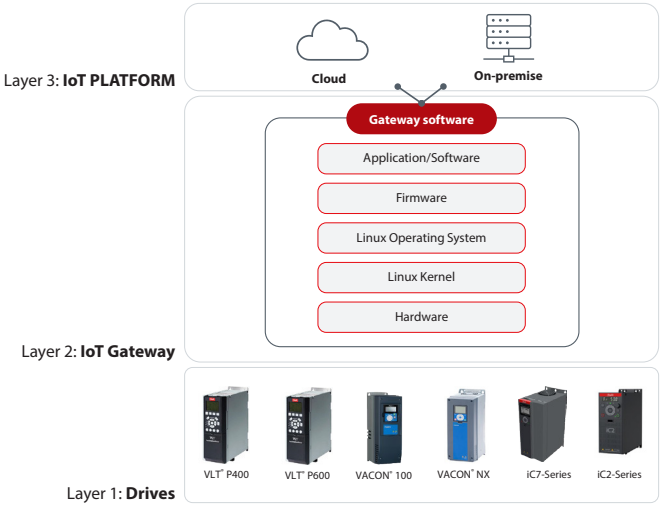


Figure 1: Layers of the DrivePro® Remote Monitoring solution

This paper shares information regarding cybersecurity features of Danfoss DrivePro® Remote Monitoring solution. It also describes security guidelines for the components present in the Danfoss DrivePro® Remote Monitoring solution. There are three layers in the Danfoss DrivePro® Remote Monitoring solution architecture as shown in Figure 1. They are:

Layer 1: Drives

This layer includes the entire portfolio of drives that DrivePro® Remote Monitoring supports, such as VACON® NX, VACON® 100, many VLT® drives, and new-generation drives like iC2 series and iC7 series.

Layer 2: IoT Gateway

The IoT Gateway combines different elements of hardware and software to provide a mechanism to collect drive data and make it available for the IoT platform. In this paper, we dive into the detail of these hardware and software stacks and uncover the security mechanism behind them.

Layer 3: IoT Platform

The IoT platform is a Cumulocity GmbH1-based Danfoss solution. DrivePro® Remote Monitoring provides both fully-cloud and on-premises capabilities of the IoT platform. This paper shares information on the cybersecurity standards and best practices used and recommended by Cumulocity GmbH IoT Platform as a component of the DrivePro® Remote Monitoring solution.

Cybersecurity in DrivePro® Remote Monitoring

2. 1 Drives

2.1.1 VACON® NX and VACON® 100 drives

VACON® drives, including VACON® NX series and VACON® 100 drives are working towards IEC 62443-4-2 SL1 certification. As product supplier, Danfoss shares information on VACON® NX & 100 drives 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.

In VACON® NX product lifecycle, defense-in-depth strategy is developed around the idea that this product, that was developed long ago without consideration of cybersecurity, is now equipped with understanding, process, actions, and roles and responsibilities related to cybersecurity. The following practices are already implemented and under continuous development:

- Security-related documentation. For example, roles and responsibilities, cybersecurity strategy, compliance with security requirements
- Secure implementation of new features and updates, including consideration of security guidelines and security best practices
- Security hardening and testing

Software for VACON® NX drives such as VACON® NC drive, VACON® NCLoad, VACON® NCIPConfig, VACON® Loader, VACON® Safe, and VACON® Service Tool is compliant with IEC 62443-3-3 SL-1. A detailed description of implementing UR E26, URE27, and IEC 62443-3-3 is provided in the white paper.

2.1.2 VLT® drives

For system certification according to IEC 6244311 and other cybersecurity standards, Danfoss can assist with mitigation solutions at system level, where interaction between VLT® drives and other system components like PLC define the total system. Cybersecurity requirements and directives, NIS2 and CRA come into force 2024–2026. Therefore, VLT® drives will meet these requirements by end-2024.

These VLT® drives are used in Operational technology: VLT® HVAC Drive FC 102, VLT® Refrigeration Drive FC 103, VLT® AQUA Drive FC 202, and VLT® AutomationDrive FC302.

Therefore, Danfoss has chosen to use requirements in IEC 62443 to implement and certify products in scope for cybersecurity:

- IEC 62443-3-3: Technical requirements for control system (where VLT is a subcomponent). SL-1 is applicable to the PC tool, VLT® Motion Control Tool MCT 10.
- IEC 62443-4-1: Secure product development lifecycle process (process for development and manufacturing).
- IEC 62443-4-2: Technical requirements for component (VLT® drive)

2. 2 IOT gateway

2.2.1 Hardware

When selecting a hardware vendor in the European Union, it's crucial to consider various security mechanisms to ensure compliance with regulations and protect against cyber threats. The EU Cyber Resilience Act (CRA) has introduced new cybersecurity requirements for hardware and software products with digital elements (PDEs), making it essential for organizations to be careful in evaluating potential vendors. Danfoss has the role of the "distributor" as per CRA guidelines for DrivePro® Remote Monitoring solution. The solution uses trusted gateway hardware vendors who meet Danfoss security requirements at par with EN 18031-1 Article 3.3(d), IEC 62443-4-1, IEC 62443-4-2, and CRA guidelines. The following hardware requirements are fulfilled in the DrivePro® Remote Monitoring solution:

- All gateway devices are:

  1. x86-64 architecture 7th Generation Intel® Core™ i5-7300U Processor, Single Socket FCBGA 1356, or
  2. ARM Cortex-A53 Industrial gateway device

- All gateway devices support standard protocols for data handling and transfer such as WEB UI, FOTA, CLI, SSH, SMS, Call, TR-069, MQTT, SNMP, JSON-RPC, MODBUS, RMS
- Supports RS-485, RS-232, Ethernet and RJ45
- The built-in security mechanism of the devices has DDOS prevention (SYN flood protection, SSH attack prevention, and HTTP/HTTPS attack prevention)
- Physical attack protection and tamper-proofing are achieved in the devices with port scan prevention (SYN-FIN, SYN-RST, X-mas, NULL flags, FIN scan attacks)
- The devices are CE-marked with RED (2014/53/EU) and other EU directives such as LVD (2014/35/EU), EMDC (2014/30/EU), and EU ROHS2 Directive (2011/65/EU)
- A built-in NXP processor mechanism handles the secured boot process
- A built-in NXP processor mechanism handles firmware-controlled root-of-trust. TPM2.0 is available.
- No parts in the devices can be categorized as vendor-managed third-party components

The preceding points ensure that security-by-design is implemented in the solution as per RED EN 18031-1 Article 3.3 (d) and complements IEC 62443.

2.2.2 Software

The Danfoss DrivePro® Remote Monitoring solution uses secure and standard software development practices to ensure that the gateway software meets the requirements of IEC 62443 and CRA guidelines. The following are the best practices used in the solution:

Secure LINUX as OS

DrivePro® Remote Monitoring solution uses base OS for firmware development such as Debian 12, released in June 2023. Debian 12 contains advanced security features such as AppArmor for application confinement, Secure Boot support, hardened compiler flags, Stack protector, and other memory protection mechanisms. The LTS version of Debian 12 will receive security updates for more than 5 years, ensuring long-term security coverage. Further derisking mechanisms use the gateway vendor's original OS for which patch management is regularly performed by the vendor.

Firmware update

Firmware update of the DrivePro® Remote Monitoring solution is comprehensive and fast. The gateway device regularly verifies the integrity and authenticity of the downloaded firmware. An A/B update schema is used, which ensures that if the update on the inactive partition fails to validate correctly, the device can roll back to a known, functioning state.

Security hardening

Security hardening practices are implemented in the DrivePro® Remote Monitoring solution using a secure development process,. This process includes:

- Secured configuration management
  a. Detailed documentation is provided on secure configuration and integration of the gateway
  b. Guidelines are provided on interfaces with other subsystems such as drives or SaaS platform, product configurations, and use of security-related tools such as firewalls, PKI, Wireshark, or tcpdump, when necessary.

- Removal of unnecessary components

Unnecessary services, applications, protocols, accounts, and other components are removed. Only trusted web servers are used in the solution. Wireless network services are avoided unless necessary. Physical media such as flash drives, file sharing, libraries, and functionality are avoided unless necessary. Remote access and control applications are not activated for the gateway device. Default guest and administrator accounts are disabled. Accounts which are non-responsive for more than 30 days are deactivated. OS updates and application software updates are done frequently. With toolbox like thin-edge, independent package management on a gateway device is not needed.

- Access control

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. Such manipulation may result in incorrect operation of the DrivePro® Remote Monitoring solution and damage to the installed equipment.

It is important to:

- Develop guidelines for password renewal. Do not keep the same password for a longer period. This requirement 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 deploy 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 change critical data in the equipment. When updating passwords, consider the following guidelines:

a. Do not assign passwords that can be easily guessed, for example, simple number combinations like 1111 or 1234

b. Assign, if possible, passwords with the required maximum length. Maximum-length passwords make it more complicated to gain unauthorized access.

2.2.3 Network and Communication

The DrivePro® Remote Monitoring solution offers Network and Communication security to ensure that the network is compliant to cybersecurity norms. This compliance minimizes the risk of attacks, 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. The following best practices are implemented in the solution:

a. Network firewall rules and configuration

- The principle of least privilege is followed as per IEC 62443
- All gateway devices, servers, switches, or any other devices in the network implement secure NTP to ensure accurate time across all devices
- Firewalls are deployed in the edge network
- An inventory of all devices and assets on the network is maintained
- The allowed ports for the solution are 443 (HTTPS), 8883 (MQTTS) and 22 (SSH). All other unused ports are disabled to prevent unauthorized access

b. Create the connection so that the drive connects only to the gateway point-to-point or via switches

c. Encrypted protocols like TLS/SSL are used for sensitive data transmission, if necessary

d. Only the latest firmware is used in all gateway devices, servers, switches, or any other devices in the network

e. To prevent physical layer attacks, the network equipment is kept in restricted-access rooms, or in lockable cabinets

f. Certificates

- X.509 certificates for trusted network are used in both the cloud and on-premise deployment of DrivePro® Remote Monitoring solution
- Danfoss PKI is recommended for Device certificates


DRIVE OVERVIEW
Live Metrics
FC-102
Drive Status History
Unknown
Fault
Running
Ready

Cybersecurity in DrivePro® Remote Monitoring

2.3 IOT platform

Danfoss has partnered with Cumulocity GmbH to equip the DrivePro® Remote Monitoring solution with strong cybersecurity practices and methods. In this way, we help our customers to enjoy all the features of a resilient and security hardened platform for handling their data. Cumulocity brings the following cybersecurity best practices to DrivePro® Remote Monitoring:

Tenant Isolation

Tenant Isolation includes Data & Resource Isolation. Security controls ensure tenants' data is stored securely to prevent unauthorized access or data leakage.

Authentication and Authorization

Strong Authentication enables the platform users to access the services using multi-factor authentication. It also enables tenant administrators to configure secure authentication using Single Sign-on mechanisms such as OAuth2 and OpenID connect.

Access Control Roles and permissions can be defined for different "User types" within each tenant using Role-Based Access Controls. RBAC enables tenant administrators to define their own roles with customized permissions. Explicit device permissions can be achieved through Inventory Roles such as principle of least privilege and granular access control.

Secure Communication

Data Encryption: Securing the data in motion by encrypting all communications between devices, the platform, and tenants

Mutual TLS (mTLS): Mutual TLS used for device authentication, ensuring both client and server authenticate each other

Secure Device Management

Device Onboarding: Secure onboarding processes for device provisioning and authentication
Firmware Updates: Secure Firmware-over-the-air (FOTA) updates for devices.

Auditing

Comprehensive Logging
Detailed logging of all access information and administrative actions.
The logs are stored securely and can be used for auditing and forensic analysis.

Data Protection and Privacy

Data Minimization
Only the necessary data needed for platform operation is collected, anonymizing or pseudonymizing data where possible.

Identity Management

Cumulocity has its own local user data store. Cumulocity provides an SSO functionality that allows a user to login with a third party auth server configured in their tenant space.

Security Configuration

Cumulocity comes with a rich set of configurations that enables you to deploy the instance or configure the tenant in a secure fashion. Security hardening guidelines for Cumulocity provide some of the best practices that can be used for reference to deploy and configure Cumulocity cloud and edge in a secure fashion, as per information security standards.

Data-at-rest

The Customer data is encrypted in motion/flight and at rest. Data at rest is stored on encrypted disk volumes. Keys are managed by the hyperscaler KMS. The encryption algorithm used is AES-256. Compatible hyperscalers providing the infrastructure for Cumulocity are Azure, AWS and in China, Alibaba and Tencent.

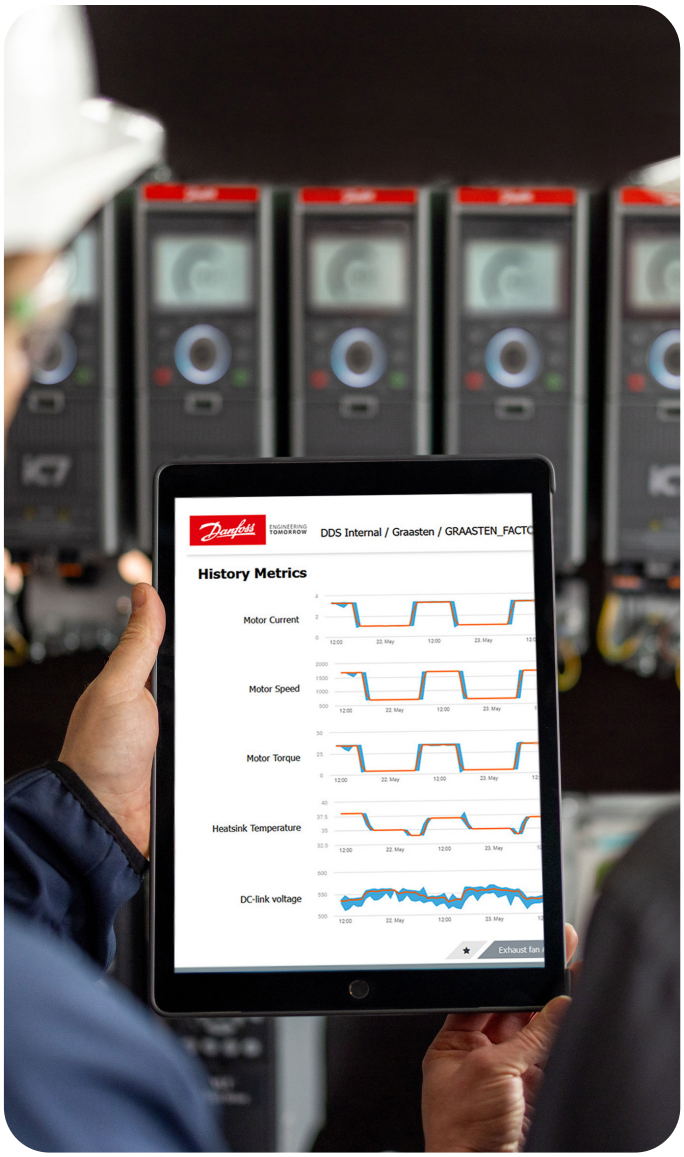
Data-in-Transit

For data-in-transit, data can be encrypted. The encryption depends on the type of traffic or device. For example, Cumulocity IoT can encrypt REST and MQTT via TLS. The exact version of the protocol used for a connection depends on the negotiation between platform and device or user browser. Cumulocity IoT uses state-of-the-art encryption protocols and ciphers for data in flight. TLS protocols and ciphers are under constant monitoring to identify weaknesses.

Continuous security monitoring

A dedicated SOC team monitors Cumulocity public cloud instances on a continuous basis. This team continuously investigates the alerts from all the security monitoring tools deployed on the platform.

The Cumulocity platform is graded A+ by SSL labs regarding Transport layer security. Learn more about the security aspect of the Cumulocity IoT platform on their website1.



References

1. https://cumulocity.com/docs/concepts/security/
2. https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

Contact us

Contact your local Danfoss experts

Learn more about DrivePro® Services

BE523146459201en-000101