CEMEP

European Committee of Manufacturers of Electrical Machines and Power Electronics

Towards a Common Cyber Security Product Context for Variable Speed Drives under the EU Cyber Resilience Act (CRA)

A CEMEP White Paper

Foreword

CEMEP is the European Committee of Manufacturers of Electrical Machines and Power Electronics, representing an industry with a market value of more than €28 billion and around 180,000 employees. This paper is intended solely as a technical reference and does not establish mandatory requirements, product specifications, procurement criteria, certification criteria, or common commercial practices. It has been prepared in a dedicated task force by a group of CEMEP members listed hereafter:

- Vassili Jung — ABB
- Maëlle Kabir-Querrec — ABB
- Preben Albrecht — DANFOSS
- Stefan Mahne — DANFOSS
- Sebastian Moebius — INNOMOTICS
- Stephan Musiolik — KEB
- Michael Niehaus — LENZE
- Vincent Amour — SCHNEIDER ELECTRIC
- Rainer Schrundner — SEW-EURODRIVE
- Michael Strauss — SEW-EURODRIVE
- Michael Wiedmann — SEW-EURODRIVE
- Alexander Busch — SIEB & MEYER
- Michael Hegmann — SIEMENS
- Karl-Heinz Schraink — SIEMENS
- Stefan Steinmüller — SIEMENS
- Diego Einloft — WEG
- Bernhard Sattler — CEMEP / ZVEI
- Maximilian Hausmann — ZVEI

Brussels, August 2026 – 1st Edition

Executive Summary

Variable Speed Drives (VSDs) are essential elements of modern industrial systems, and their increasing connectivity makes a clear understanding of their product context critical for addressing cyber security risks under the EU Cyber Resilience Act (CRA). This white paper is intended primarily for system integrators who integrate VSDs into systems, and it is also relevant to manufacturers and operators of VSDs. It is written to be accessible to readers who are not cyber security experts.

This white paper summarizes common characteristics typically found in VSD applications for defining that context: covering the intended purpose, foreseeable use, operational environment, critical assets, and typical deployment conditions of VSDs. It will provide the foundation for consistent, context specific cyber security risk assessments and for defining suitable security requirements.

Effective cyber security will depend on coordinated roles: manufacturers delivering products with well-defined security capabilities, system integrators embedding VSDs into secure architectures, and operators maintaining appropriate physical, network, and organizational controls. The harmonized product context outlined in this paper will support a coherent, risk based, and practicable approach to cyber security for VSDs under the CRA.

Table of Contents

1 Introduction 6

2 Key Concepts Definitions 7

3 What is a Variable Speed Drive? 8

3.1 Definition 8

3.2 Diverse Applications: industrial motors, non-motor systems, utility networks 8

3.3 Functional Description of a VSD 9

3.4 Main Mission of a VSD 9

3.5 Supportive Features 10

3.6 Contribution to Security 10

3.7 Major Communication Interfaces and Security-relevant Elements 11

4 Foreseeable Use of a VSD 12

5 Intended Operational Environment 14

5.1 Physical Accessibility 14

5.2 Network Integration 16

6 Foreseeable Misuse of a VSD 20

7 Assumptions on the VSD's Security Context 21

8 Cyber Security Risk Management 23

8.1 Context Specific Risk Assessment 23

8.2 Establishing a Continuous Risk Management Process 23

8.3 Purpose of Risk Management 23

8.4 Key Areas 23

8.5 Recommended Methodologies 24

8.6 Following the Required Security Context 24

8.7 Continuous Review and Updates 24

9 Conclusion 25

List of Abbreviations

AC	Alternating Current
BDM	Basic Drive Module
CRA	Cyber Resilience Act
DC	Direct Current
HMI	Human Machine Interface
HVAC	Heating, Ventilation, Air Conditioning
I/O	Input/Output
IEC	International Electrotechnical Commission
IP	Ingress Protection
OS	Operating System
OT	Operational Technology
PLC	Programmable Logic Controller
SCADA	Supervisory Control and Data Acquisition
VFD	Variable Frequency Drive
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSD	Variable Speed Drive

1 Introduction

The increasing digitalization of industrial automation and power conversion systems has elevated the importance of clearly defining the product context for Variable Speed Drives (VSDs) under the EU Cyber Resilience Act (CRA). VSDs – also referred to as drives or converters – play a foundational role in industrial operations by providing controlled power conversion to motors and, in certain cases, to non-motoric loads. Although their primary mission remains technical and process-oriented, the connectivity and configurability of modern VSDs introduce cyber security considerations that require systematic treatment.

This white paper describes typical characteristics of the product context of VSDs in relation to cyber security requirements. It aims to harmonize terminology, assumptions, and architectural considerations across manufacturers, integrators, and operators.

The document consolidates typical operational environments, foreseeable use cases, and trust boundaries for VSDs. Recognizing that VSDs are deployed in diverse industrial and infrastructure settings, this white paper is not intended to be prescriptive or exhaustive; rather, its aim is to outline common characteristics found across many VSD deployments so as to foster awareness and support a consistent interpretation of the cyber security implications associated with their integration and operation.

To provide this foundation, we examine:

- the key functions of a VSD and its interactions within the automation environment;
- the range of industrial applications, physical installations, and network integrations in which VSDs operate;
- the key assumptions and expectations defining the intended purpose, reasonably foreseeable use, and intended operational environment under the CRA;
- the trust boundaries, critical assets, and security-relevant interfaces that shape a VSD's exposure to cyber risks; and
- principles and methodologies for context-specific cyber security risk assessment in accordance with IEC 62443-3-2.

This structured approach supports consistent interpretation of cyber security requirements and promotes an aligned understanding across the lifecycle of VSDs.

2 Key Concepts Definitions

Under the CRA, several elements are essential for determining cyber security requirements and risk-management obligations:

- The **intended purpose** means the use for which the product is intended by the manufacturer, including the specific context and conditions of use (cf. CRA Article 3 Section 23).
- The **reasonably foreseeable uses** are uses that, while not necessarily intended, are likely to result from reasonably foreseeable human behavior or technical operations or interactions (cf. CRA Article 3 Section 24).
- The **intended operational environment** is the environment in which the product manufacturer expects the product to be used. It is part of the overall conditions of use that contribute to the product's intended purpose (cf. CRA Article 13 Section 3).
- The **reasonably foreseeable misuse** means the use of a product with digital elements in a way that is not in accordance with its intended purpose, but which may result from reasonably foreseeable human behavior or interactions with other systems (cf. CRA Article 3 Section 25).

To establish a solid foundation for assessing cyber security threats and risks in VSD systems, these contextual elements must first be examined and clearly documented. Doing so captures the assumptions and expectations regarding both the VSD and the conditions under which it will be deployed. This ensures that the risk assessment reflects actual operating conditions, and that the resulting security requirements are truly adequate for the product.

Aligned with IEC 62443-4-1 (Practice 2), documenting these assumptions and expectations about the product's security context – for example, network placement, isolation/segmentation, physical protection, and expected external safeguards – enables manufacturers to implement appropriate built-in controls and integrators/operators to provide any required external or supporting measures at system level. This alignment supports a coherent, defense-in-depth design and enables verification and validation under conditions that faithfully represent real-world deployments.

3 What is a Variable Speed Drive?

3.1 Definition

A VSD is an electronic device that controls an electric load by varying the frequency and voltage of the power supplied to it.

A more formal definition can be found in the IEC 61800-2 standard which defines a Basic Drive Module (BDM) as an electronic power converter and related control, connected between an electric supply and a motor (the load). A BDM can transmit power from the electric supply to the motor and may be capable of transmitting power from the motor to the electric supply. Furthermore, a BDM controls some or all of the following aspects of power transmitted to the motor and motor output: current, frequency, voltage, speed, torque, force.[1]

In this white paper, we predominantly use the term VSD. VSDs are sometimes known as Variable Frequency Drives (VFDs). This white paper covers many types of VSD, including servo drives, and BDM. It also can be applied to other similar power electronic converters.

3.2 Diverse Applications: industrial motors, non-motor systems, utility networks

VSDs serve a wide range of industrial purposes, primarily by controlling the position, speed and torque of electric motors to match actual load requirements. This functionality improves energy efficiency (especially in systems like Heating, Ventilation, Air Conditioning (HVAC) and pumps) by reducing unnecessary power consumption. VSDs also help extend equipment lifespan by enabling smooth starts and stops, minimizing mechanical stress. Typical motor applications include industrial automation (e.g., conveyors, mixers, extruders), industrial motion control, HVAC systems (fans, blowers, compressors), water and wastewater treatment (pumps), and elevators and escalators. Beyond motor control, VSDs are also used in non-motor applications like precision heating and electrolysis. In these cases, the VSD does not regulate a motor but instead controls the electrical power delivered to heating elements or electrolytic cells with high accuracy, making it a versatile tool in both process and energy-intensive industries.

Specific VSDs are also used purely to convert electricity and transfer it from one grid to another with different characteristics. They are used for instance in renewable energy systems such as wind turbines or solar generation. Although this paper may be partially applicable to such use cases, it primarily focuses on industrial applications, encompassing both motor-driven and non-motor systems. Indeed, the energy domain is quite specific with its own regulations and standards that may deviate from generic industrial ones.

---

[1] International Electrotechnical Commission (IEC) 61800-2, 3.4

3.3 Functional Description of a VSD

Figure 1 gives a functional representation of a VSD with its in- and outflows of control and monitoring data (green) and energy (blue). Upstream, data is supplied by an optional external and/or internal control, including Programmable Logic Controllers (PLCs) or supervisory management systems, whereas downstream it may be obtained from sensors associated with the load.

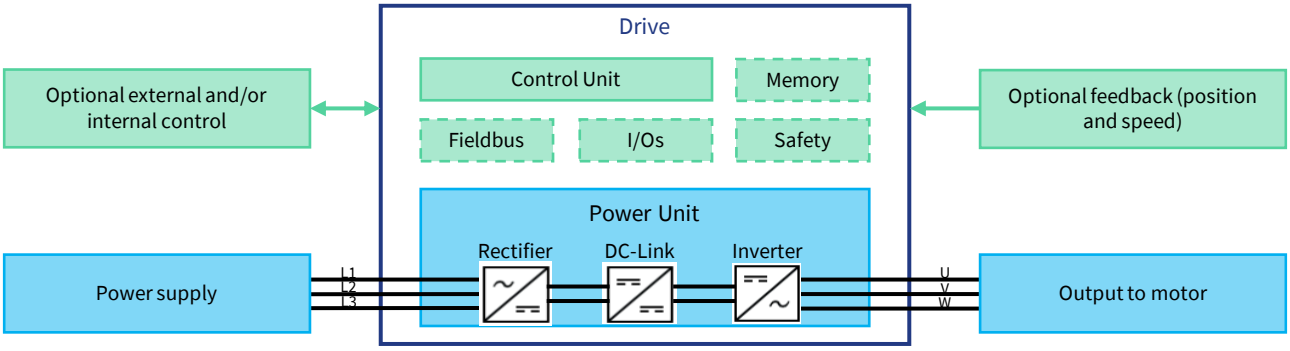


Figure 1: Functional View of a Drive Module

A drive module typically has two main parts: the power unit and the control unit with its optional modules. Such modules may be physically pluggable units or may be integrated in the control unit depending on models. The power unit is the electrical circuit that actually converts and delivers electrical energy. The control part may consist of:

- one or more control units where the firmware runs,
- optional modules for communication (digital – fieldbus, or analog Inputs/Outputs (I/O)) or providing safety features,
- optional modules for feedback encoders (speed or position),
- an optional pluggable memory extension unit,
- an optional user interface

A VSD can be designed either as a single-drive system, where one rectifier converts Alternating Current (AC) to Direct Current (DC) and one inverter converts DC back to AC, or as a multi-drive system, where a shared rectifier supplies DC power to several inverters. Depending on the setup, conversions between AC/DC, DC/DC, or DC/AC are all possible.

3.4 Main Mission of a VSD

As explained in section 3.1 and section 3.2, the main mission of a VSD is to convert energy between a power supply and a load, and to do it by applying adequate control. To perform its mission, a VSD should:

- Enable a fine control of the energy transferred to the load for reduced mechanical stress and optimized energy efficiency.
- Optimize uptime and limit maintenance needs on the VSD-based system for enhanced productivity.
- Support electrical safety functionalities.

3.5 Supportive Features

A VSD incorporates a range of digital functionalities to fulfilling its primary purpose depending on the applications. These may include:

- **System Communication**: Interfacing with other components in the industrial ecosystem – such as VSDs, PLCs or other control systems, and edge gateways – via analog I/O, fieldbus networks, or industrial Ethernet protocols.
- **Command Processing**: Receiving and executing control commands (e.g., start, stop, direction) as well as motor position, speed and torque references.
- **Data Management**: Storing, processing, and providing access to parameters, measurements, and event data for internal and external entities.
- **Global Time Synchronization**: Maintaining alignment with external reference to support synchronized time to one source.
- **Event Logging**: Recording operational events and making logs accessible to external systems.
- **Backup and Restore**: Supporting configuration backup and restoration for operational continuity.
- **Firmware Update**: Updating the VSD's embedded software to fix issues, enhance security, improve performance, or add new features.
- **User Management**: Enabling secure user access and role-based permissions.
- **Local Interface Communication**: Connecting through local ports to external tools (e.g., configuration software, keypads, panels, or web servers) for parameterization, firmware updates, or manual control (including command overrides, alarm acknowledgment, and system start/stop).
- **Application Support**: Allowing execution of programs and applications (e.g., IEC-compliant programs).
- **Functional Safety**: Ensuring the system detects, controls, or mitigates hazardous conditions to maintain or transition to a safe state. Cyber security aspects of functional safety, e.g. from the EU Machinery Regulation 2023/1230, are out of scope for this paper.

3.6 Contribution to Security

Depending on the operational environment, a VSD may also play a role in enhancing cyber security. This can affect both its primary mission and supporting functions, and may include:

- Contribute to managing cyber risks that could impact functional safety.
- Contribute to managing cyber risks that could affect the environment accidentally or deliberately.
- Help to protect against compromise of integrity of the industrial process and data.
- Log security-relevant changes for forensic purposes and to support non-repudiation.

3.7 Major Communication Interfaces and Security-relevant Elements

Major security-relevant elements are components, data sets, and operational functions whose availability, integrity, and confidentiality can play a major role in the correct and reliable operation of a VSD system. Compromise, malfunction, or loss of any of these elements can prevent the VSD from performing as intended, degrade system safety, or disrupt production.

3.7.1 Major Communication Interfaces of a VSD

A VSD has the following major communication interfaces:

- **Communication between the control system and the VSD**: Reliable communication is essential to ensure correct command execution and prevent unauthorized or unintended control actions.
- **Communication between configuration tools and the VSD via local ports or the network**: The engineering interfaces provide direct access to configure or reprogram the VSD. Such channels can be exploited for unauthorized parameter changes or malicious reprogramming if not properly secured, making their protection essential to maintaining the integrity and safe operation of the VSD.

3.7.2 Major Security-relevant Elements of a VSD

The following security-relevant elements of a VSD (covering both functional and data-related elements) can play a major role for maintaining secure and stable VSD operation:

- **User authentication**: These ensure that only authorized personnel can access, modify, or control the VSD. If certain interfaces lack built-in authentication, this requirement shifts to the surrounding operational environment.
- **VSD configuration**: Parameter sets and operational settings define how the VSD controls the load and interacts with the system. Unauthorized changes can impair process quality, damage equipment, or lead to unsafe behavior.
- **Firmware and firmware update**: Firmware provides the functionalities required for the VSD to operate. Firmware whose integrity is compromised, or firmware that is outdated, can introduce vulnerabilities or prevent the process from functioning as intended.
- **Access to customer sensitive information**: This may include customer-specific applications, authentication credentials, and measurement data collected by the VSD. Exposure or manipulation of this information can lead to privacy breaches or misuse of intellectual property.
- **Event logs and optional audit logs**: Logs provide traceability for operational and security events. Loss or manipulation of audit data limits the ability to detect incidents and investigate anomalies. If certain interfaces lack built-in audit logs, this requirement shifts to the surrounding operational environment.

The impact of these elements on the secure and stable operation of the VSD must be systematically assessed for each specific application as part of a risk analysis.

4 Foreseeable Use of a VSD

The VSD needs to be integrated with diverse industrial equipment to build an industrial application. Figure 2 gives an overview of the VSD system, it shows how the VSD interfaces with other components like:

- **Configuration tools** intended to be connected to the VSD for a time limited to the configuration and the software update. Such tools are typically running on work engineering stations (e.g., a Windows computer) over Ethernet or via local interfaces like e.g. USB.
- **A local Human Machine Interface (HMI)** such as a control panel, through Ethernet, USB or Serial. It may itself be used to connect to mobile apps via Bluetooth or Wi-Fi connection or configuration tools.
- **Industrial components and processes** such as PLCs or other control management systems via classical fieldbuses or industrial Ethernet protocols.
- **An edge gateway**, via Ethernet or Serial, that may provide cloud connectivity for monitoring and/or control.
- **Encoders and other sensors** via I/Os, fieldbuses or industrial Ethernet protocols.
- **Other VSDs**. VSDs can be controlled in a leader-follower configuration. The leading VSD gives control instructions to follower VSDs. This setup synchronizes multiple motors using either analog or digital communication.

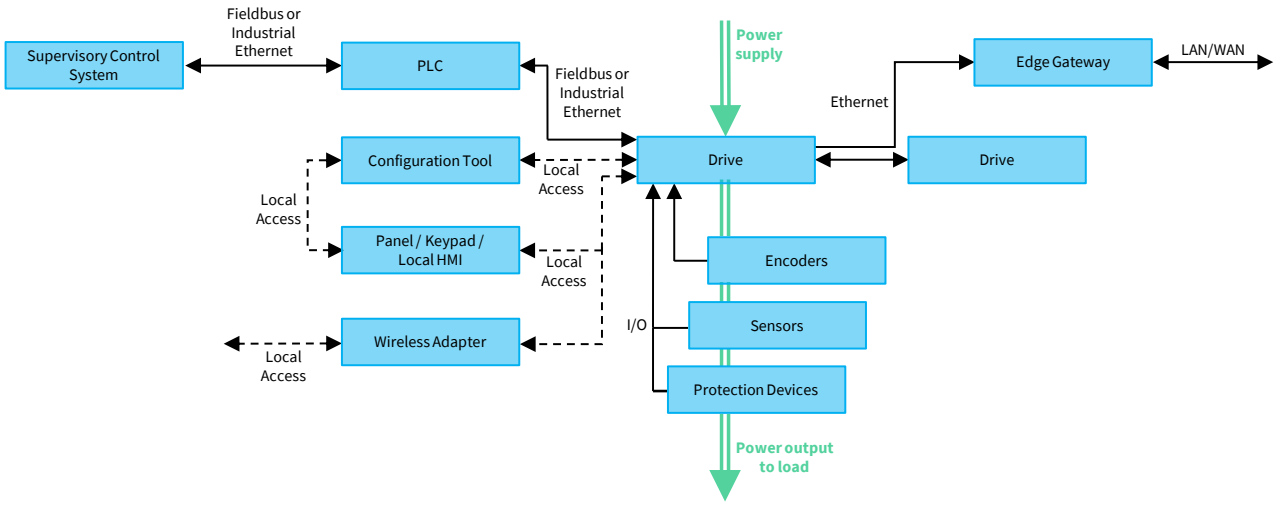


Figure 2: Functional Representation of the VSD's Ecosystem

To support integration into a wide range of industrial applications, VSDs can be deployed in various configurations depending, for example, on the physical layout and control system architecture. While standalone VSDs operate independently without network integration, other configurations leverage connectivity for advanced control and monitoring.

Standalone VSD:

These VSDs function without a central control system and are typically mounted on a wall near the motor or housed in a local enclosure. They are suited for simple applications where local control via a keypad, analog input, or basic I/O is sufficient.

Centralized VSD:

In this configuration, VSDs are installed close to the main control system, usually in a central cabinet or electrical room with restricted access. This setup simplifies maintenance and environmental control (temperature, dust, moisture). Centralized integration is ideal for environments with limited machine space or applications that demand centralized monitoring and maintenance.

Decentralized VSD:

Here, VSDs are mounted near or directly on the motor in the field and communicate with the control system via industrial networks such as fieldbus or industrial Ethernet. This approach reduces motor cable length and installation costs while improving flexibility and scalability – making it well-suited for modular production lines and large systems like conveyors or packaging lines. It does, however, require robust communication protocols.

5 Intended Operational Environment

As Operational Technology (OT) components, VSDs often operate in harsh environments with electrical, thermal, mechanical, energy-related, and dust-related hazards, as described in IEC 61800-5-1. Therefore, Ingress Protection (IP)-rated enclosures or other protective measures for physical access protection are usually required.

Some environmental factors also affect cyber security. In particular, cyber security depends on managing both physical access to the device and digital access through its network connections. These access paths are central to evaluating cyber security risks for VSDs and are discussed in the following sections.

5.1 Physical Accessibility

In general, there are three levels of physical accessibility to the VSD system: public, limited and controlled.

1. **Public** environments are places where non-specialists or even the general public could be nearby.
2. For environments with **limited** accessibility, there are security measures like, for example, a fence, video surveillance, and entrance controls that restrict access to selected people. Examples are company premises that contain many not so critical buildings like a canteen or a general office building.
3. In **controlled** environments, access is even more limited to trustworthy people than in environments with limited accessibility, and additionally there may be more surveillance measures in place. An example for this may be a production building in a company's premise: For entering the production building, people must use an additional card reader that restricts access to trustworthy and skilled people only. If there are any visitors, then they must be escorted by a trustworthy and skilled person.

VSDs are typically installed in controlled environments with strict access control, ensuring that only skilled and trusted personnel can reach the equipment. Examples include controlled industrial areas, such as container terminals, process automation facilities, or production buildings, and locked machines, switchboard cabinets or dedicated cabinet rooms accessible only to authorized personnel with the appropriate keys or permissions.

Figure 3 and Figure 4 illustrate these examples for VSDs that are used in production buildings:

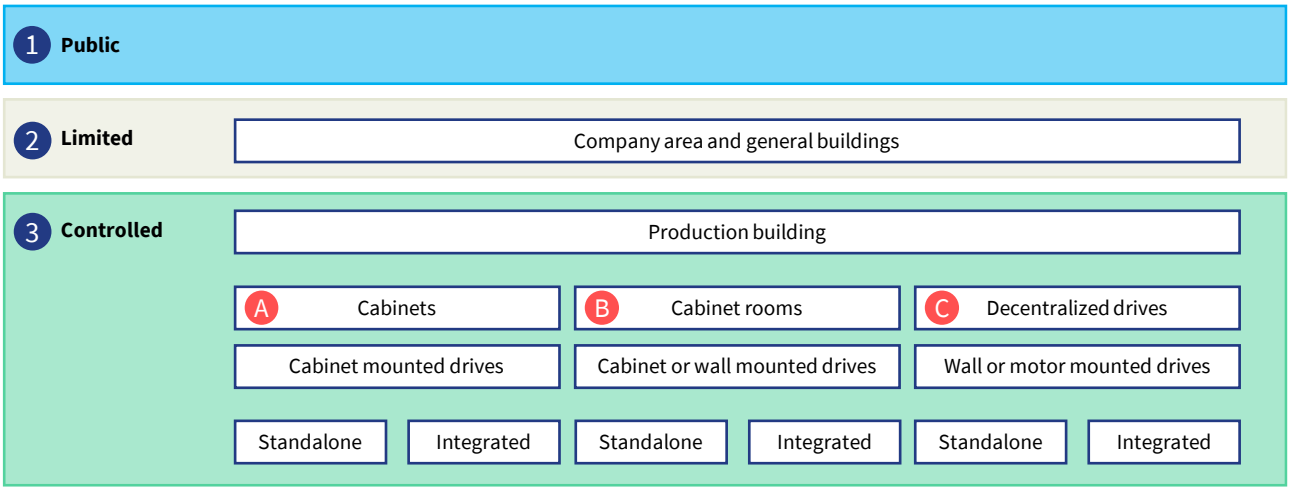


Figure 3: Physical environment for the usage of converters in production buildings (hierarchy)

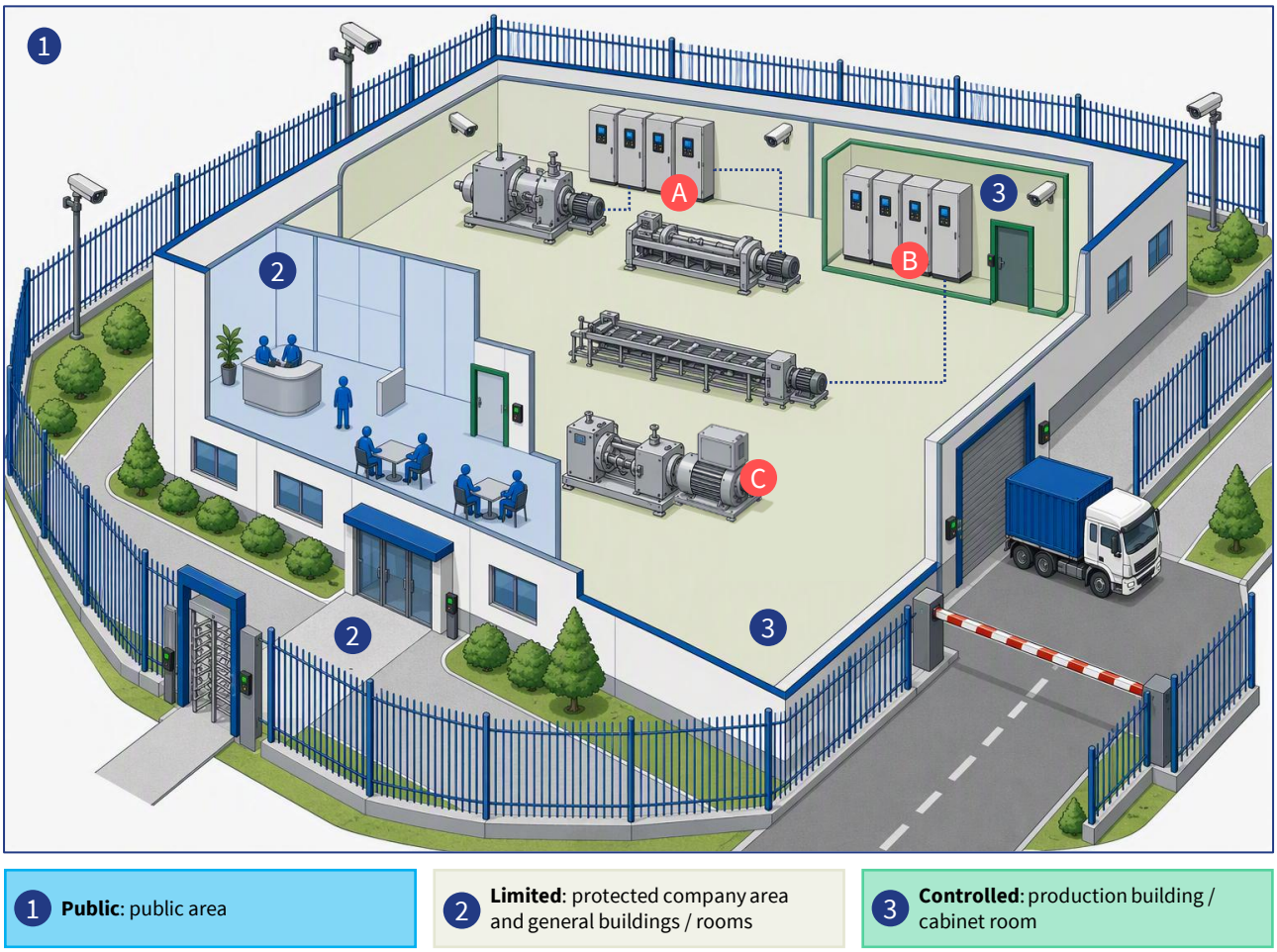


Figure 4: Physical environment for the usage of converters in production buildings (Image generated with AI).

Beyond selecting an appropriate installation area, additional measures may be required to further restrict and control physical interaction with the VSD, depending on the assessed risk, like one or many of the following:

- Installing VSDs in securely locked machines or cabinets Ⓐ, Ⓑ with limited access to the keys for authorized personnel only.
- Installing VSDs in cabinet rooms Ⓑ with suitable access control and monitoring mechanisms. In such an electrical room the access to the converters including their local user interfaces or engineering interfaces is limited by the access control to the room.
- Using video surveillance.
- Locking or unmounting removable operator panels.
- Using alarm switches, that triggers an alarm when the machine or switchboard cabinet is opened.

When a VSD is monitored or controlled remotely – whether from a central control room or through Supervisory Control and Data Acquisition (SCADA) systems – physical access control must be enforced at both ends: on the control infrastructure and directly at or near the VSD itself. Effective remote access management also depends on secure integration into the surrounding automation network; the key considerations for this are discussed in the following section on Network Integration.

For decentralized or wall-mounted VSDs, especially those mounted directly on the motor Ⓒ or positioned close to the motor on the machine or a nearby wall, there are limited options to establish an additional physical trust boundary such as a locked cabinet. Depending on the risk, users may therefore need to apply additional protective measures, for example:

- locking the HMI with a dedicated physical lock, configuring it as read-only, or removing and storing it in an access-restricted location,
- locking, disabling, or restricting engineering interfaces so they are accessible only with a dedicated tool.

If the VSD or its user interface supports a wireless protocol, its effective wireless range becomes part of the physical access exposure. Because wireless communication can extend far beyond the immediate vicinity of the VSD, it may – in line with the assessed risk – be necessary to disable the wireless interface entirely or enable it only temporarily during commissioning or diagnostics.

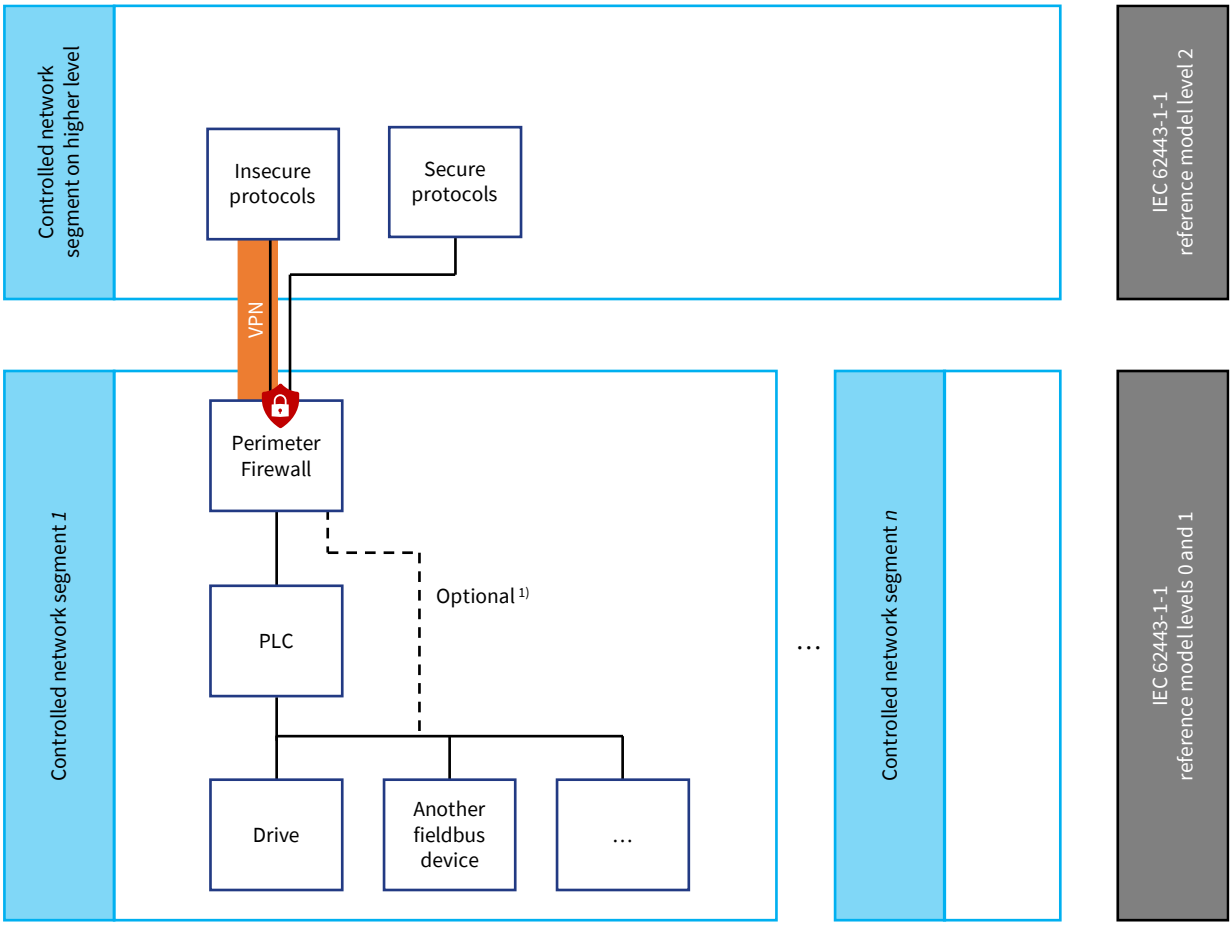
5.2 Network Integration

5.2.1 Introduction and General Network Integration

Besides standalone VSDs with no network integration, VSDs are typically deployed within controlled network segments. In such segments, the perimeter firewall protecting the relevant network area shall be configured according to the default-deny principle – blocking all inbound and outbound traffic by default. Exceptions may be permitted based on a risk analysis, but only for secure, manufacturer-approved protocols and only to devices that are explicitly intended to communicate with the VSD.

If communication across the perimeter is required using other protocols or involving external devices, such access shall be treated as a controlled exception and secured through measures such as a Virtual Private Network (VPN) tunnel with strong authentication, restrictive firewall rules, and/or properly configured Virtual Local Area Networks (VLANs).

These principles are illustrated in Figure 5. They apply independently of the VSD type (e.g., centralized or decentralized) and whether the VSD is connected directly or indirectly to a controlled segment at a higher network level. The notion of network level refers to the industrial reference model structured into logical levels – from Level 0 for the physical process up to Level 4 for enterprise functions – based on the IEC 62443-1-1 reference architecture.



1) IP-based devices may be optionally connected directly to the perimeter firewall

Figure 5: General network integration of VSDs

5.2.2 Cloud Integration

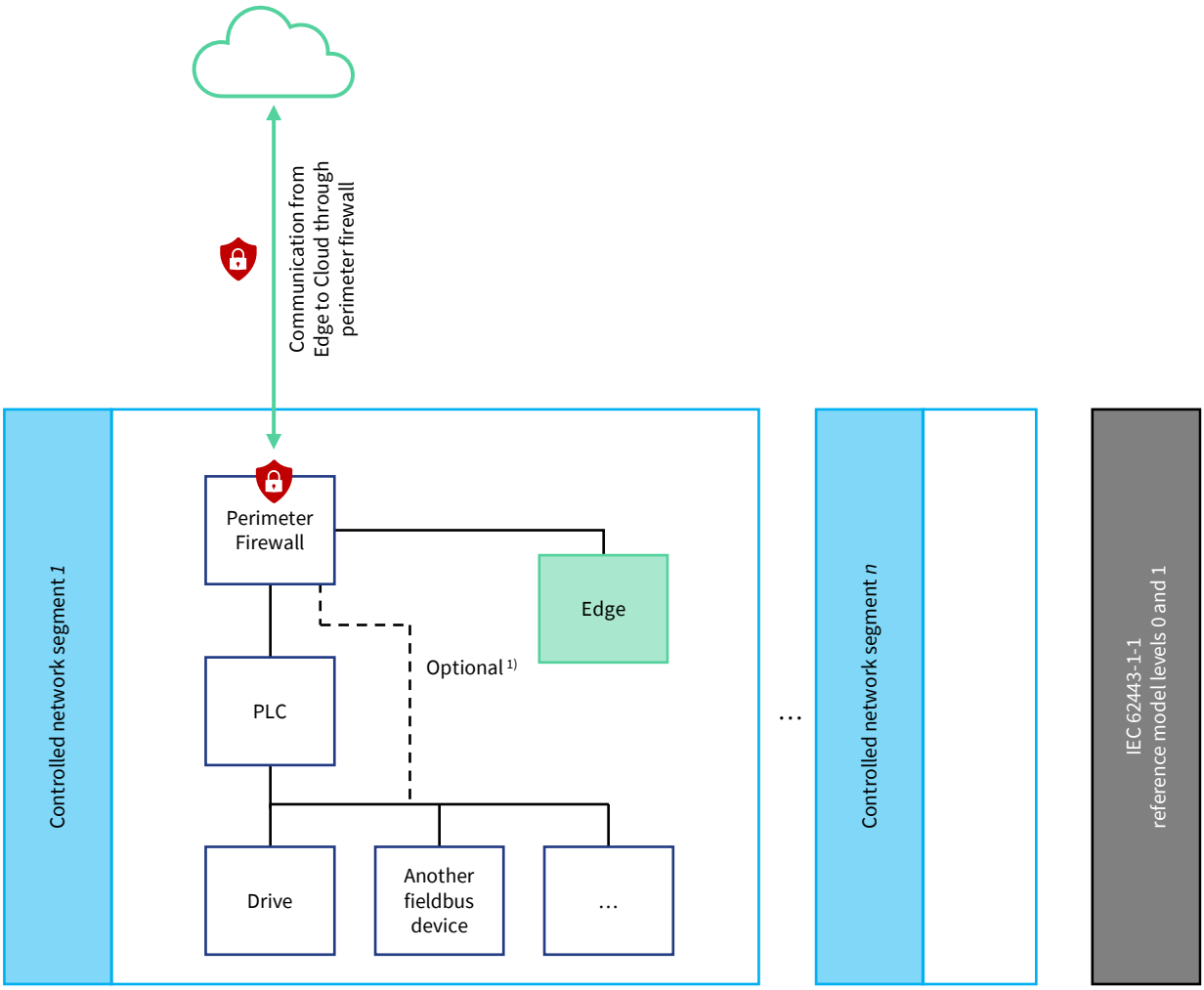
VSDs are not directly connected to cloud services. Instead, cloud access occurs indirectly through an intermediate device – such as an edge device, HMI, or PLC – that exchanges data with the VSD. This intermediary typically collects operational data from the VSD, aggregates and/or preprocesses it, and then forwards the relevant information securely to the cloud. Conversely, any commands or configuration actions originating from cloud applications are routed back through the same intermediary, which enforces the appropriate safeguards before forwarding them to the VSD.

Depending on the overall architecture, these intermediate devices may operate within the same controlled network segment as the VSD, or within a controlled network segment at a higher network level, consistent with the IEC 62443 reference architecture.

Cloud Integration via Device in the Same Controlled Network:

In the scenario illustrated in Figure 6, cloud connectivity is provided through an edge device that resides within the same controlled network segment as the VSDs, either continuously or only when temporarily enabled (e.g., during diagnostics or maintenance). The edge device communicates with multiple components in the network and acts as the secure intermediary for forwarding information to cloud services.

To safely bridge the controlled network with cloud environments, the cloud environment and the edge device must implement appropriate perimeter protections, authenticated communication channels, and other network security measures that ensure data transfer occurs in a controlled, protected, and well-governed manner. This architecture maintains the isolation of the production network while enabling cloud-based monitoring, analytics, or lifecycle-management functions.



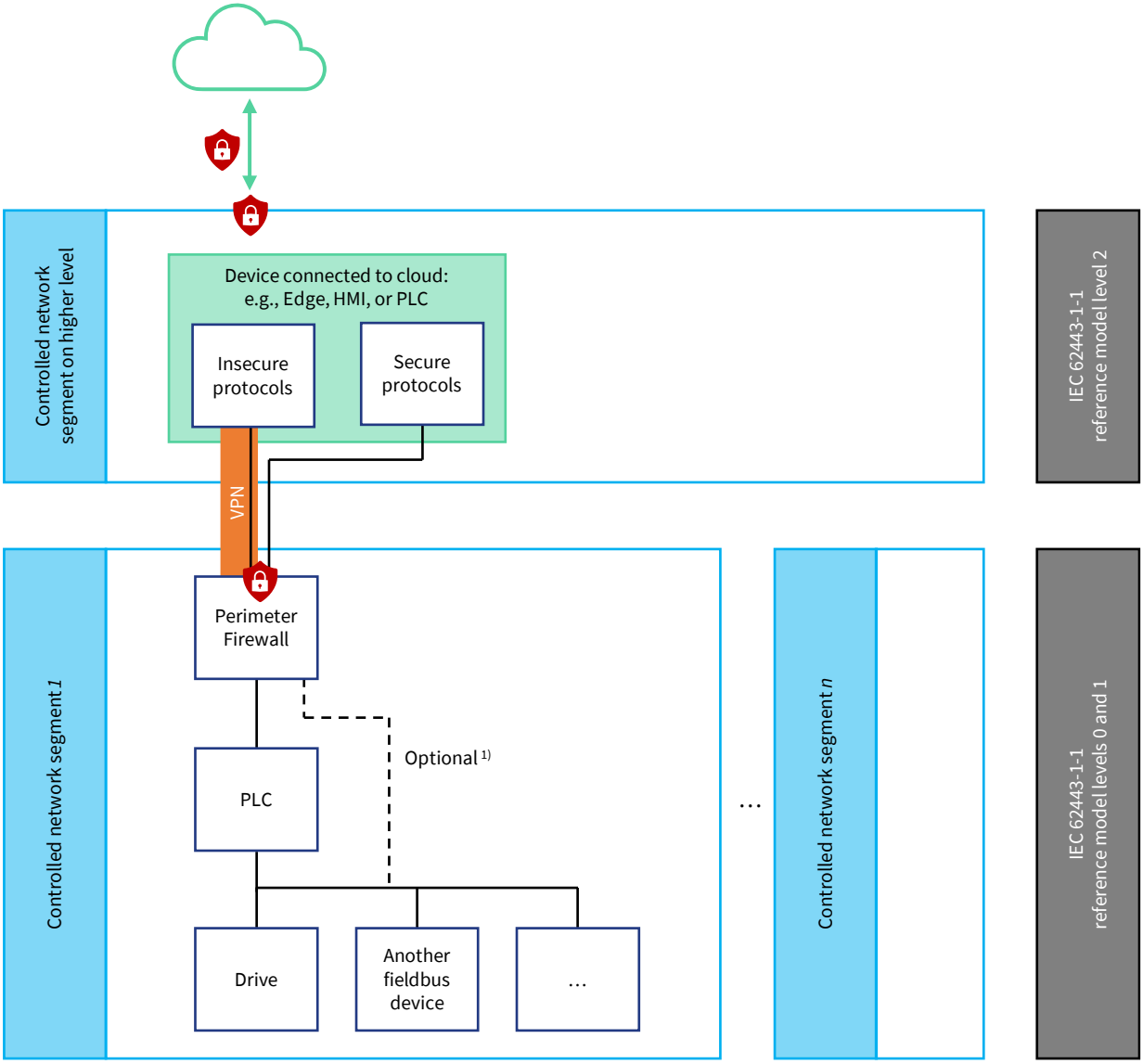
1) IP-based devices may be optionally connected directly to the perimeter firewall

Figure 6: Cloud integration via device in the same controlled network

Cloud Integration via Device in a Higher Network Layer:

In the scenario illustrated in Figure 7, cloud connectivity is provided through a higher-level device, typically an HMI system, a dedicated PLC, or an edge device, that communicates with multiple lower-level networks using secure, authenticated protocols. This higher-level device aggregates data originating from the VSDs and other field components before forwarding it to cloud services in a controlled manner.

Depending on the outcome of the risk analysis, the VSDs may communicate with such higher-level devices either through a secure VPN link terminating at the network perimeter firewall, or via secure communication protocols that incorporate proper authentication and additional protections such as security-event monitoring and controlled data flows. Alternatively, a PLC or edge device located within the controlled network segment may serve as the secure intermediary between the higher-level system and the VSD. In this role, it ensures that cloud-bound communication remains protected, traceable, and consistent with the VSD's intended deployment context.



1) IP-based devices may be optionally connected directly to the perimeter firewall

Figure 7: Cloud integration via device in a higher-level network

6 Foreseeable Misuse of a VSD

Foreseeable misuse of a VSD mainly stems from predictable human actions or integration practices – such as leaving default passwords, bypassing recommended configuration workflows, or using the VSD under conditions that differ from those normally expected for proper integration and operation. While such deviations can lead to consequences such as incorrect torque or speed, operational downtime, or mechanical stress on the equipment, commonly implemented electrical and functional safety protections – such as those described in IEC 61800-5-1 – typically limit or prevent hazardous outcomes at the VSD level (and/or at the control level that the VSD receives commands from). Some misuse scenarios cannot be fully mitigated by product-embedded controls and instead require appropriate engineering practices, user competence, and adherence to established procedures. Likewise, ensuring that the system-level integration, network environment, and physical access conditions reflect the intended operational environment is essential to prevent misuse that originates outside the VSD. When manufacturers, machine builders, integrators, and users follow industry best practices, such as those described in this white paper, throughout the development, installation, configuration, and operation of VSDs, foreseeable misuse at the VSD level can be effectively addressed. However, broader risks may still emerge at the system level, where both the range of actions and the potential impact extend beyond the VSD itself.

7 Assumptions on the VSD's Security Context

The following is a consolidated list of assumptions that define the product context as relevant to assessing the cyber security risks of VSDs. Some of these assumptions were introduced earlier in the white paper, while others are added here to complete the contextual basis required for a consistent and industry aligned risk assessment.

The assumptions described in this section are not mandatory requirements and do not define a technical standard. They represent common characteristics observed in many industrial VSD deployments and are intended solely as a reference framework for risk assessment activities.

1) Intended Purpose & Use:

- A VSD's primary mission is controlling power conversion; digital features support this mission.
- Commissioning, operation, maintenance, troubleshooting, and decommissioning are performed by skilled personnel using vendor-approved tools and procedures.

2) Physical Environment:

- Industry standard electrical and functional safety protections – for example having appropriate enclosures or other protections as applied through common engineering practice – are in place to ensure that hazardous physical consequences are prevented or limited even in the event of cyber induced misuse or malfunction.
- Default installations are in controlled industrial and commercial environments (restricted buildings/rooms, locked cabinets/panels). Some deployments may occur in limited access areas, and exceptional cases may be in public proximity locations; in those cases, additional physical protection (e.g., locked enclosures) is required to provide a controlled environment.
- If wireless interfaces are present (e.g., Bluetooth/Wi-Fi on HMI/panel), their effective range is part of the physical exposure. So wireless is disabled by default or enabled only temporarily for commissioning/diagnostics, with protections appropriate to risk.

3) Engineering Access & Local Interfaces:

- Configuration tools (engineering workstations, panels, local HMIs) provide direct configuration access and are assumed to be used intermittently (commissioning/ maintenance) by authorized, skilled users.
- Engineering workstations are trusted endpoints, managed by the operator. They shall be hardened systems according to best practices (Operating System (OS) without any known vulnerability, anti-malware, least privilege…).

4) Network Environment:

- Network connected VSDs operate in protected, controlled network segments with default deny rules for the perimeters.
- Exceptions are limited to secure, manufacturer approved protocols.
- VSDs are not directly Internet exposed.
- Cloud connectivity occurs only via intermediaries (e.g., via edge device, HMI, PLC, user tools) implementing their own security controls.

5) Lifecycle & Maintenance:

- Vendors have a vulnerability management process and provide security patches based on risks throughout the product's supported lifetime.
- Vendor-supported firmware update mechanisms and configuration backup/restore are available and used.
- Throughout the product's supported lifetime, operators are expected to apply available security updates in a timely manner.

6) Roles & Responsibilities:

- Only authorized and skilled personnel access or modify the VSD.
- Manufacturers provide guidance for secure integration and use of the VSD as well as security updates; system integrators ensure secure integration; operators ensure physical security, network segmentation, and monitoring.
- All parties involved implement a cyber security risk management system.

7) Risk Assessment:

- The cyber security risk assessment considers adversaries who may gain network level access to the controlled segment or local physical access, consistent with how accessible the installation is in practice (public, limited or controlled).

8) Supply Chain:

- Vendors are expected to apply established industrial practices to mitigate supply chain risks throughout the product lifecycle.
- Machine builders, system integrators, and operators are expected to procure VSDs, components, and accessories exclusively from trusted and reputable sources, following established supply-chain assurance practices.

8 Cyber Security Risk Management

8.1 Context Specific Risk Assessment

The cyber security posture of a VSD deployment is determined not only by the product's built-in security capabilities but also by how it is integrated into a broader machine or plant environment.

Each installation presents a distinct operational context; therefore, vendors, machine builders, plant builders, and operators shall each perform a risk assessment at their respective levels – vendors applying a more generic assessment because their products may serve diverse use cases, while plant builders and operators evaluate the specific risks associated with their installation and plant environment.

This ensures that cyber security controls reflect the actual operational, environmental, and network conditions of the system.

8.2 Establishing a Continuous Risk Management Process

Effective cyber security for VSD installations requires a structured and continuous risk management process. Such a process must adapt to evolving threats, system modifications, and changes in operational requirements. The risk assessment is a central activity within this process and should be revisited at defined intervals throughout the VSD lifecycle, as well as whenever system changes, new vulnerabilities, or altered operational conditions necessitate an updated evaluation.

8.3 Purpose of Risk Management

The risk assessment supports several key objectives. These may include but are not limited to:

- Identifying cyber security threats relevant to the specific operational context
- Assessing potential impacts on data confidentiality and integrity, safety, production continuity, and business operations
- Determining security measures proportional to the identified risks
- Defining the security context required for the VSD and its environment
- Demonstrating compliance with regulatory and industry requirements

8.4 Key Areas

A complete and context aware risk assessment for VSD installations typically includes analysis of:

- **System architecture**: Network topology, segmentation, communication routes, and any remote access interfaces
- **Operational criticality**: The consequences of compromised operation, including safety hazards, production losses, or process degradation
- **Physical and logical access**: The conditions under which personnel may access the VSD locally or remotely, and how such access is controlled
- **Supply chain considerations**: Hardware, firmware, and software provenance; update, patching, and replacement mechanisms; and maintenance workflows.

8.5 Recommended Methodologies

Industry standards provide structured and widely accepted processes for assessing cyber security risks in industrial automation and control systems. For example, IEC 62443-3-2 defines a system-level security risk assessment process from the perspective of the asset owner, supporting the identification of assets, the partitioning of the system under consideration into zones and conduits, the evaluation of risks, and the derivation of system-level security requirements. For product-related aspects, IEC 62443-4-1 includes threat-modelling activities, but does not fully address product security risk assessment. Organizations may therefore apply suitable techniques to establish and maintain product security risk assessment processes across the product lifecycle, such as STRIDE, attack-tree analysis, or other risk-analysis methods, in line with their engineering practices. Together, these processes support the derivation of consistent, repeatable, and context-appropriate security requirements for VSD deployments.

8.6 Following the Required Security Context

Based on the outcomes of the risk assessment, the required security context for a VSD installation is established and maintained. This may include:

- Implementing appropriate network segmentation and access controls
- Applying suitable authentication and authorization mechanisms
- Ensuring secure configuration aligned with operational needs
- Enabling and appropriately configuring monitoring, logging, and event handling proportional to risk level
- Maintaining timely patch management and regular application of security updates

8.7 Continuous Review and Updates

Risk assessments are not static. They are reviewed and updated when the system or its operational environment changes.

Updates occur, for example, when:

- System or network architectures are modified,
- New vulnerabilities or relevant threat scenarios emerge,
- Security incidents occur within the installation or become evident in the wider industry, or
- Operational requirements or process conditions change.

In addition to event-driven updates, periodic reviews form part of the continuous risk management process. As a baseline, such reviews take place at least annually, while recognizing that vulnerability management processes require ongoing assessment of newly disclosed vulnerabilities and their potential impact.

9 Conclusion

This white paper summarizes common assumptions and deployment characteristics for understanding the product context of VSDs in relation to cyber security under the CRA. By clarifying the intended purpose, foreseeable use, operational environment, system interactions, and security-relevant elements of VSDs, it provides a structured foundation for context-specific and risk-based cyber security assessments. Rather than prescribing specific solutions, it supports a consistent and shared understanding that can be adapted to the wide range of industrial applications in which VSDs are deployed.

Ensuring effective cyber security for VSDs requires a coordinated effort across all stakeholders. Manufacturers define the security capabilities of the product and its intended context, system integrators embed VSDs into secure architectures, and operators establish and maintain the necessary physical, network, and organizational controls in their specific environment. Only through this shared responsibility, combined with continuous risk assessment and lifecycle management, can a robust and sustainable cyber security posture be achieved for VSD deployments.

CEMEP – European Committee of Manufacturers of Electrical Machines and Power Electronics

Moulevard A. Reyers 80, 1030 Brussels, Belgium
+32 4 873 284 84 – policy@cemep.eu – www.cemep.eu