CAPIEL

european coordinating committee of manufacturers
of electrical switchgear and controlgear

CAPIEL Whitepaper
Cyber security and functional safety interplay

March 25th 2026

1 Purpose of this document

The target audience for this guide is manufacturers of CAPIEL products where the following Acts apply at the point of ”placing on the market”.

It is assumed that the reader is already familiar with the:

- Radio Equipment Directive (RED) 2014/53/EU
- Machinery Regulation (MR) (EU) 2023/1230
- Cyber resilience Act (CRA) (EU) 2024/2847
- EU commission’s ”Blue guide”

The reader should be aware that this guide is not intended to conflict with any of the European Commission’s Guidance or applicable legislation. If in doubt, suppliers must seek their own advice on any issues and must not rely on this document alone.

Several aspects of the Acts are still under discussion by the European Commission, Member States and industry, so it is therefore possible that parts of this document may change as further information becomes available.

2 Landscape of regulations

2.1 Relevant regulations

Since the creation of the digital strategy in the European Union and the advent of Industry 4.0, it has become clear that the ability for devices to be connected and, by consequence, machinery, is the future of manufacturing.

The European Union, in an impressive effort to grant a free and safe market; has addressed cybersecurity threats and the provision of safe and secure connected machinery, putting in place many legislative initiatives such, NIS2 Network and Information Security Directive (EU) 2022/2555, CRA, MR, RED, etc.

But how do all these acts relate to each other and affect manufacturers of products within the CAPIEL consortium? This document aims to help the understanding and how the interplay between the various acts may have an impact on CAPIEL products.

Providing this overview aims to guide manufacturers through the development of their products and help them match the appropriate requirements and standards.

2.2 Relevant regulations

CRA → details requirements on product (with digital elements), throughout their lifetime, provides rules on market surveillance and requirements with regards to threat discovery reaction.

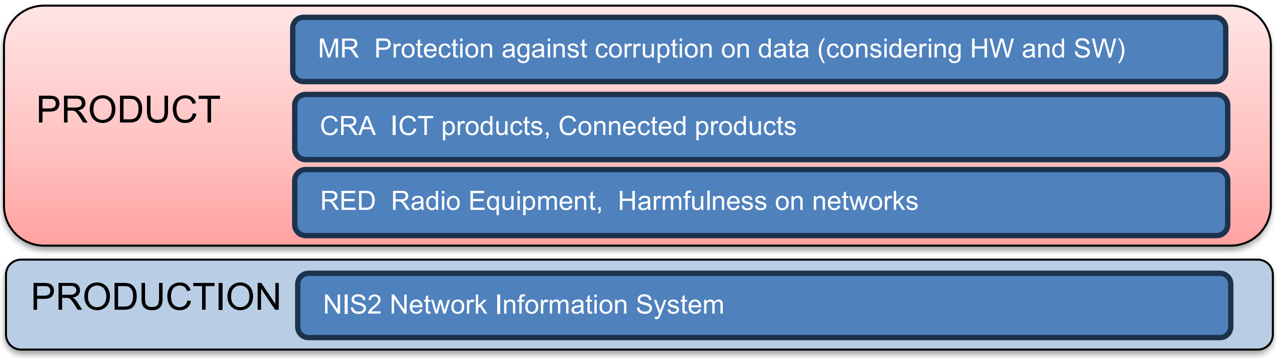
RED → Requirements on products (Radio Equipment) and their influence on existing networks

MR → Machinery or related parts, throughout the entire lifecycle.

CSA → Rules and organizational aspects for the EU certification scheme of ICT (Information Communication Technologies) products /processes and services

NIS2 → Identification of critical sectors (Network information system) and application of related requirements to protect against attacks.

The various legislative Acts providing requirements on products are as follows:



PRODUCT

MR Protection against corruption on data (considering HW and SW)

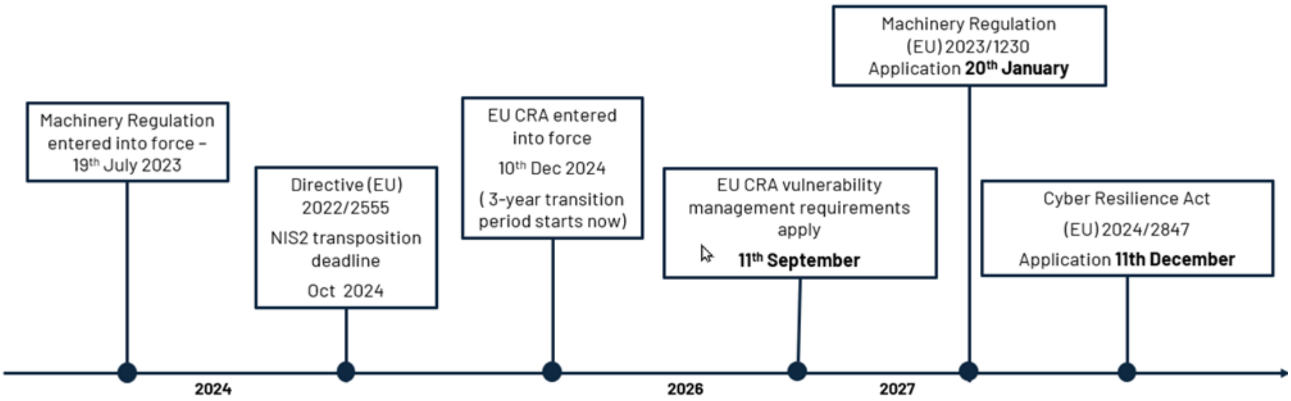
CRA ICT products, Connected products

RED Radio Equipment, Harmfulness on networks

PRODUCTION

NIS2 Network Information System

Figure 1

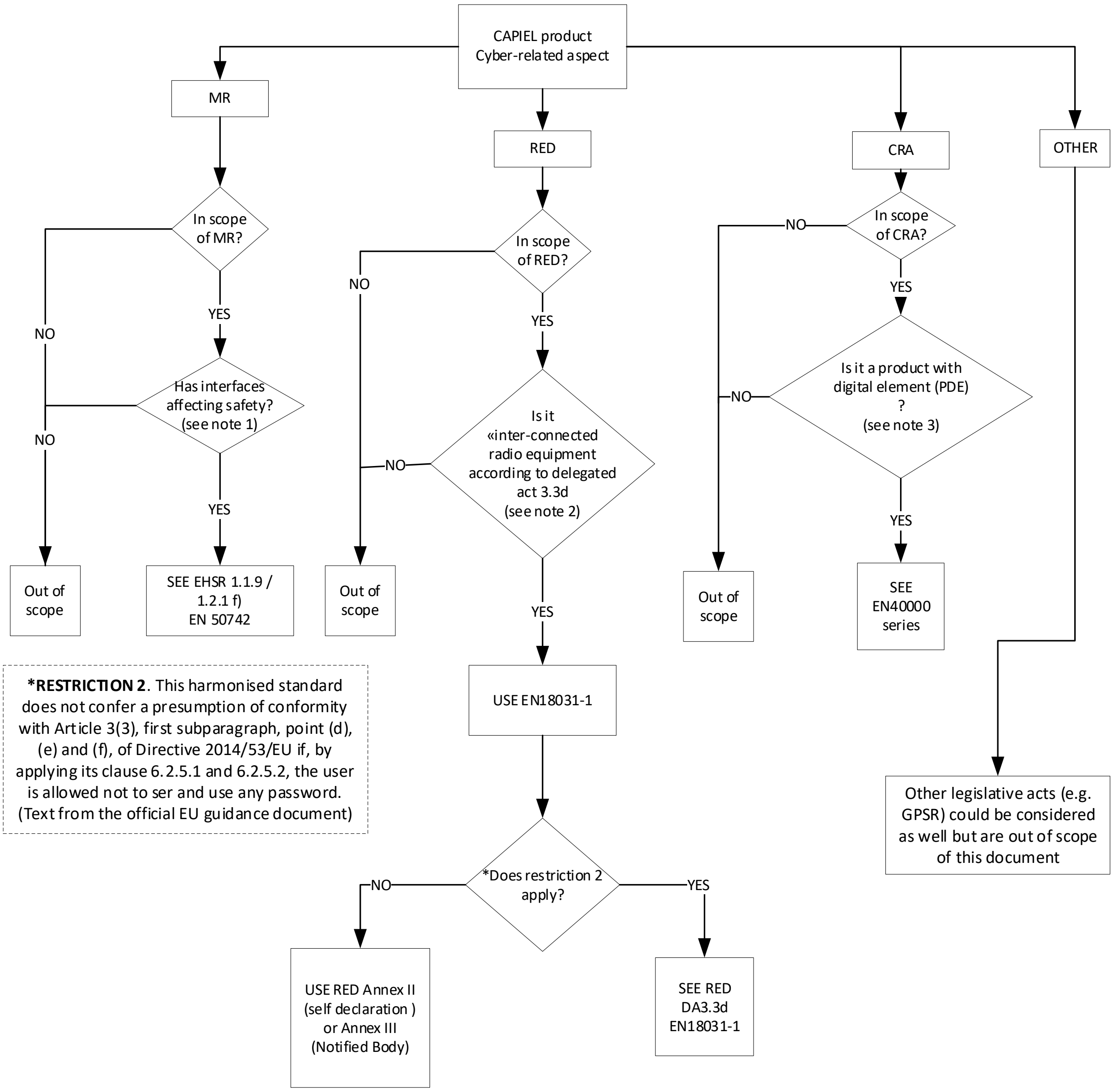


Machinery Regulation entered into force - 19th July 2023
Directive (EU) 2022/2555 NIS2 transposition deadline Oct 2024
EU CRA entered into force 10th Dec 2024 (3-year transition period starts now)
EU CRA vulnerability management requirements apply 11th September
Machinery Regulation (EU) 2023/1230 Application 20th January
Cyber Resilience Act (EU) 2024/2847 Application 11th December
2024
2026
2027

Figure 2

2.3 Explanation of the actual process

The below flowchart in figure 3 describes the process for complying with the various cyber-security requirements which may apply to a CAPIEL product.


CAPIEL product
Cyber-related aspect
MR
RED
CRA
OTHER
In scope of MR?
NO
YES
Has interfaces affecting safety? (see note 1)
NO
YES
Out of scope
SEE EHSR 1.1.9 / 1.2.1 f) EN 50742
In scope of RED?
NO
YES
Is it «inter-connected radio equipment according to delegated act 3.3d (see note 2)
NO
Out of scope
YES
USE EN18031-1
*Does restriction 2 apply?
NO
YES
USE RED Annex II (self declaration) or Annex III (Notified Body)
SEE RED DA3.3d EN18031-1
In scope of CRA?
NO
YES
Is it a product with digital element (PDE) ? (see note 3)
NO
YES
Out of scope
SEE EN40000 series
Other legislative acts (e.g. GPSR) could be considered as well but are out of scope of this document

***RESTRICTION 2**. This harmonised standard does not confer a presumption of conformity with Article 3(3), first subparagraph, point (d), (e) and (f), of Directive 2014/53/EU if, by applying its clause 6.2.5.1 and 6.2.5.2, the user is allowed not to ser and use any password. (Text from the official EU guidance document)

Figure 3 – Action map comparing the product cybersecurity requirements.

Once the applicable legislative acts have been identified, the steps for analysing the product can be summarised as follows:

- **Machinery Regulation [MR]:**

    1. Assess whether your product has moving parts or is a safety component and within the scope of the Machinery Regulation [MR].
    2. Assess whether it can exchange information directly or indirectly with the internet?
    3. If it can, check that it is not listed in annex I and subject to third party assessment, then

4. If the category of equipment allows for internal production control (module A) conformity assessment, set out in Annex VI, see ESHR 1.1.9 & 1.2.1(f) and use a standard providing a method of compliance such as EN 50742.

- **Radio Equipment Directive [RED]:**

1. Assess whether your equipment receives or transmits radio waves and is therefore within the scope of the RED.
2. Assess whether your product can exchange information directly or indirectly with the internet, according to delegated act 3.3(d).
3. If it can, 3.3d applies: (d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service.
4. Use the module A, internal production control conformity assessment procedure described in Annex II of the RED (2014/53/EU), by using a standard meeting the EHSR's such as EN 18031-1, making sure that a password is mandatory which can be defined by the end-user (see restriction 2 in the OJEU).

Note that the RED Delegated acts 3.3 d), e) and F) will be repealed on Dec 11th, 2027, when the CRA comes into effect.

- **Cyber Resilience Act [CRA]:**

1. Assess whether the equipment has digital elements according to the scope of CRA.
2. Undertake and document an assessment of the cybersecurity risks associated with a product with digital elements.
3. Take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product.
4. Minimise cybersecurity risks, prevent incidents and minimise their impact.
5. Documentation regarding the measures and countermeasures to be adopted.

Other directives may apply such as the LVD (Low Voltage Directive), but this is not within the scope of this paper since our main focus is the interaction between Cybersecurity aspects of the various Directives and Regulations.

This paper focuses on cyber-security aspects only and the different approaches adopted by the above Acts.

Other non-cybersecurity related requirements apply to the CAPIEL product simultaneously but are not part of this analysis e.g. LVD (Low Voltage Directive) 2014/35/EU and EMCD (Electromagnetic compatibility Directive) 2014/30/EU.

3 Useful definitions

The legislative acts that are referred to within this document requires a shared and defined vocabulary to get a common understanding.

The following table lists various definitions to help readers understand the MR, CRA, RED

Act	Term	Definition
CRA	**Product with Digital Elements (PDE)**	a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately
	Cybersecurity	as defined in Article 2, point (1), of Regulation (EU) 2019/881 “on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) EU cybersecurity; *(1) ‘cybersecurity’ means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.*
	Software	the part of an electronic information system which consists of computer code
	Hardware	a physical electronic information system, or parts thereof capable of processing, storing or transmitting digital data
	Component	software or hardware intended for integration into an electronic information system
	Connectivity Capability	the ability to exchange information and data
MR	**Safety component**	means a physical or digital component, including software, of a product within the scope of this Regulation, which is designed or intended to fulfil a safety function and which is independently placed on the market, the failure or malfunction of which endanger the safety of persons, but which is not necessary in order for that product to function or for which normal components may be substituted in order for that product to function
	Safety function	means a function that serves to fulfil a protective measure designed to eliminate, or, if that is not possible, to reduce, a risk, which, if it fails, could result in an increase of that risk
	Cybersecurity	measures to protect a machine control system against unauthorized access or attack that can result in a hazardous situation (from ISO 12100 clause 3.40)
	Corruption	accidental or illegitimate modification of machinery data potentially resulting in hazardous situations. (from prEN 50742 clause 3.5)
RED	**Internet-connected radio equipment**	radio equipment that can communicate by itself over the internet, whether it communicates directly or via any other equipment. See Orgalim DigitalEurope industry interpretation document once published

4 Requirement overlap examples

Increased connectivity of products present in a plant, brings in the possibilities of overlapping of different Directives and Regulations; in other words, the very same equipment may now fall under the scope of several Acts.

The CRA has in scope a "product with digital element" and is aimed at covering a very wide range of products; MR has in scope machinery or related parts, and the RED DA 3.3 d) has in scope radio equipment capable of communicating over the internet.

This implies a need to pay particular attention where a product may fall under different regulations at the same time.

4.1 Safety PLC

The following figure 4 is a safety PLC for which all the main characteristics have been identified (boxes) and are linked to the applicable Act with arrows.

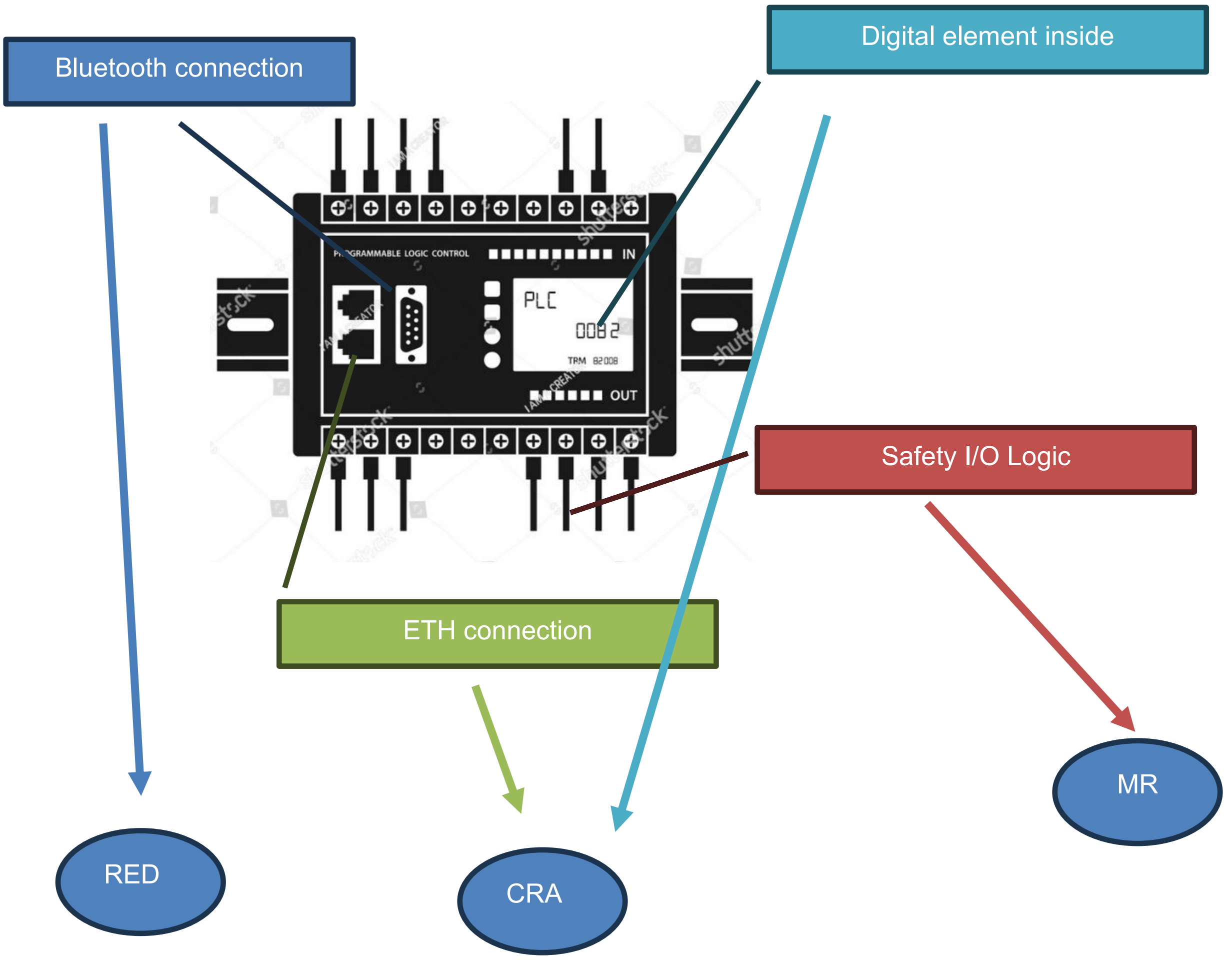


Figure 4 – Typical safety PLC

Rationale;

- A safety PLC has safety I/O and Logic to perform safety-related tasks thus it falls under the MR (art. 3 definition for safety-related function),
- It has connectivity capability via ETH interfaces, so it falls under the CRA,

- It has a Bluetooth connection (radio), only to display statuses, but as a consequence it falls under the RED.

According to the flowchart in figure 2, to fully address the requirements for cyber security the following standards have to be considered:

- EN 50742 for compliance to the MR;
- Upcoming standards under development for the compliance to the CRA, (e.g. EN40000-1) and finally
- EN 18031-1 for the compliance to the RED DA3.3 (d).

4.2 Safety relay

The following figure 5 relates to a simple safety relay.

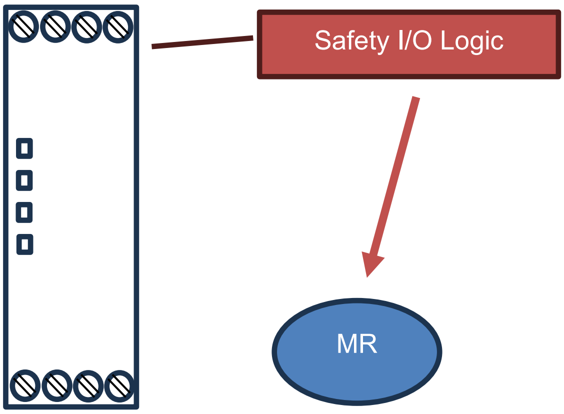


Figure 5 – Typical Safety relay

Rationale:

- Has the ability to perform a safety function, therefore it is within the scope of the MR.
- It is a stand-alone unit without radio capability/interfaces so not within the scope of the RED directive.
- May contain digital elements capable of processing and transmitting digital data (receives digital Inputs form the Input actuator via wire and provides digital outputs e.g. to the contactors via wire) however it is not possible to access the internal firmware after installation therefore the CRA is not applicable.

According to the flowchart in figure 3, to fully address the requirements for cybersecurity the following needs to be considered:

- EN 50742 for compliance to the MR only
- The Cybersecurity requirements explained under the EHSR 1.1.9 and 1.2.1 (f) of MR can be limited to logging only, if available, since the unit has no connectivity capability.

4.3 Switchgear

The following figure 6 shows switchgear for which all the main characteristics have been identified (boxes) and are linked to the applicable Act with arrows.

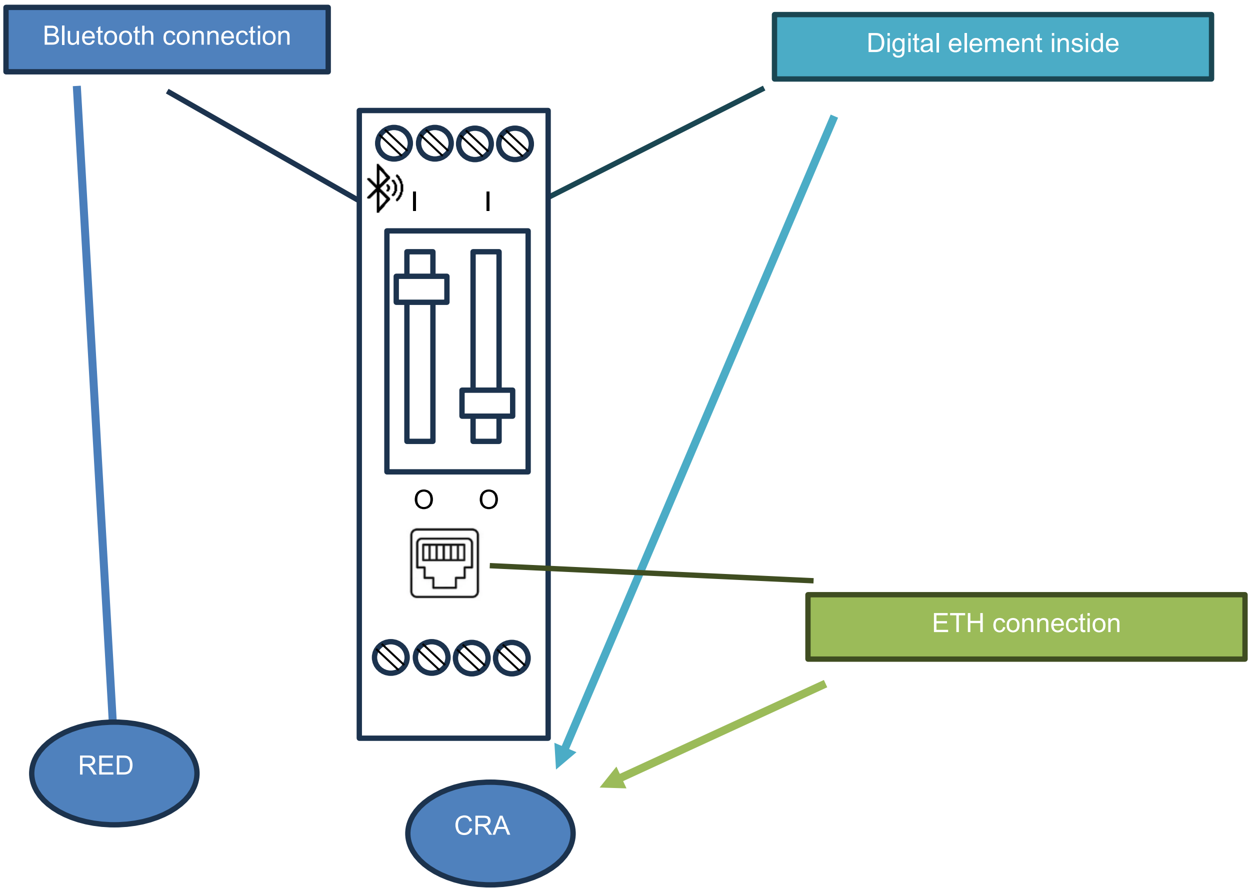


Figure 6 – Example of simple Switchgear

Rationale;

- it has connectivity capability and digital elements to control via an interface, so it falls under the CRA,
- It has a Bluetooth interface to send out only status data thus it falls under the RED
- It has no specific nor dedicated I/O or logic capable to perform safety-related functions thus it does not fall under the MR

NOTE: LVD safety requirements are included under the RED provisions (art 3.1 a) too.

According to the flowchart in figure 3, to fully address the requirements for cyber security the following standards must be considered:

- EN standards under development for the CRA (e.g. EN 40000 series)
- EN 18031-1 for the RED DA 3.3 d)

4.4.1 Limit switch (non safety-related)

The following figure 7.A shows a limit switch for which all the main characteristics have been identified (boxes) and are linked to the applicable Act with arrows.

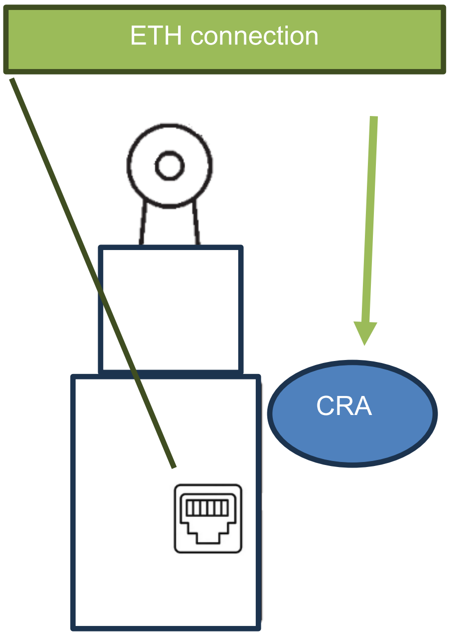


Figure 7.A

Rationale;

- It is not within the scope of the MR since it has no capability to host safety function,
- It has connectivity capabilities, so it is in the scope of the CRA
- It has known vulnerabilities disclosed by the manufacturer.

This falls under the CRA solely and known vulnerabilities have to be treated by the end user, according to the manufacturer's instructions.

According to the flowchart in figure 2, to fully address the requirements for cyber security the following standards have to be considered:

- The EN standards under development for the CRA (e.g. EN 40000 series)

4.4.2 Limit switch (safety-related)

The following figure 7.B shows a limit switch for which all the main characteristics have been identified (boxes) and are linked to the applicable Act with arrows.

It is also used to perform a safety function of the machine.

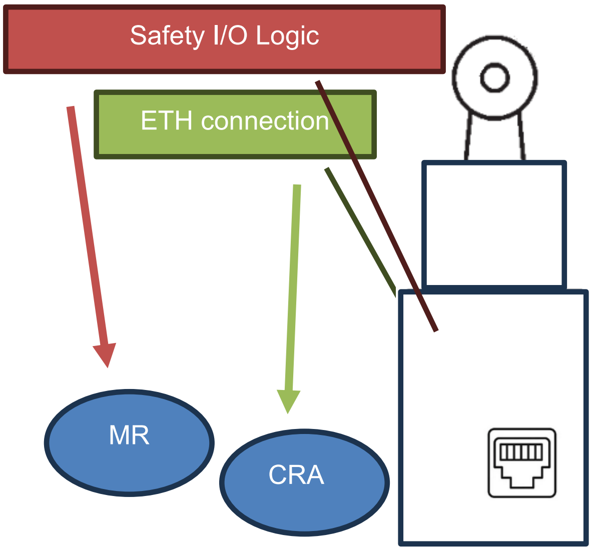


Figure 7.B

Rationale;

- It is within the scope of the MR since it is part of a safety function for the machinery,
- It has connectivity capabilities, so it is in the scope of the CRA
- It has known vulnerabilities disclosed by the manufacturer.

It is in the scope of both the CRA and the MR, the known vulnerabilities have to be treated by the end user, according to the manufacturer's instructions.

According to the flowchart in figure 2, to fully address the requirements for cyber security the following standards have to be considered:

- The EN standards under development for the CRA (e.g. EN 40000 series)
- EN 50742 for the MR

4.5.1 Power Drive System (without safety functions)

The following figure 8 shows a power drive system (PDS) for which all the main characteristics have been identified (boxes), and are linked to the applicable Act with arrows.

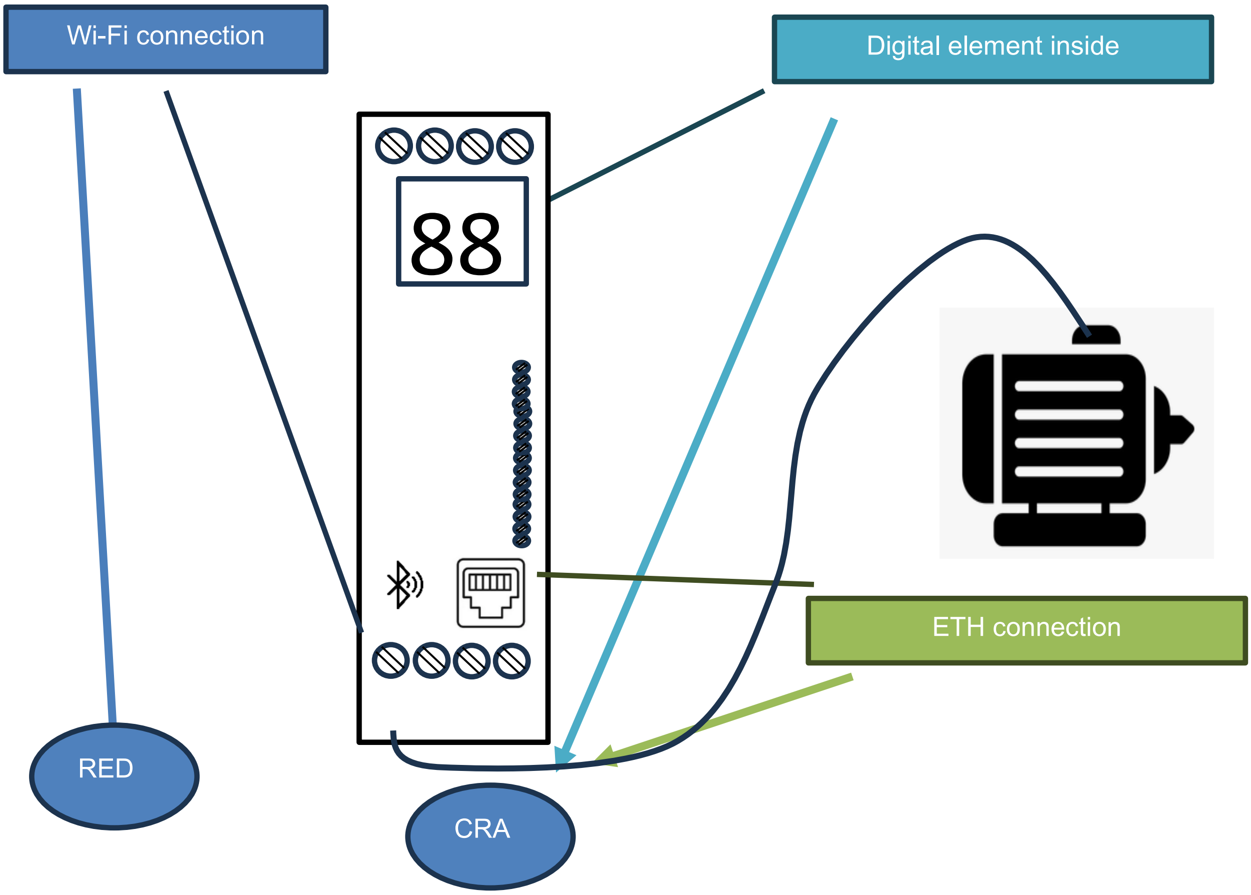


Figure 8 – Typical PDS

Rationale:

- The PDS had a fieldbus connection that makes it possible to have a remote connection, thus it falls under the CRA
- It also has a Wi-Fi interface for status monitoring, and thus it also falls under the RED.

According to the flowchart in figure 3, to fully address the requirements for cyber security the following standards have to be considered:

- The upcoming standard under the CRA (E.g. EN40000 series)
- EN18031-1 for the RED DA 3.3 D)

4.5.2 Power Drive System (with embedded safety function)

The following figure 9 shows a power drive system (PDS) for which all the main characteristics have been identified (boxes) and are linked to the applicable Act with arrows.

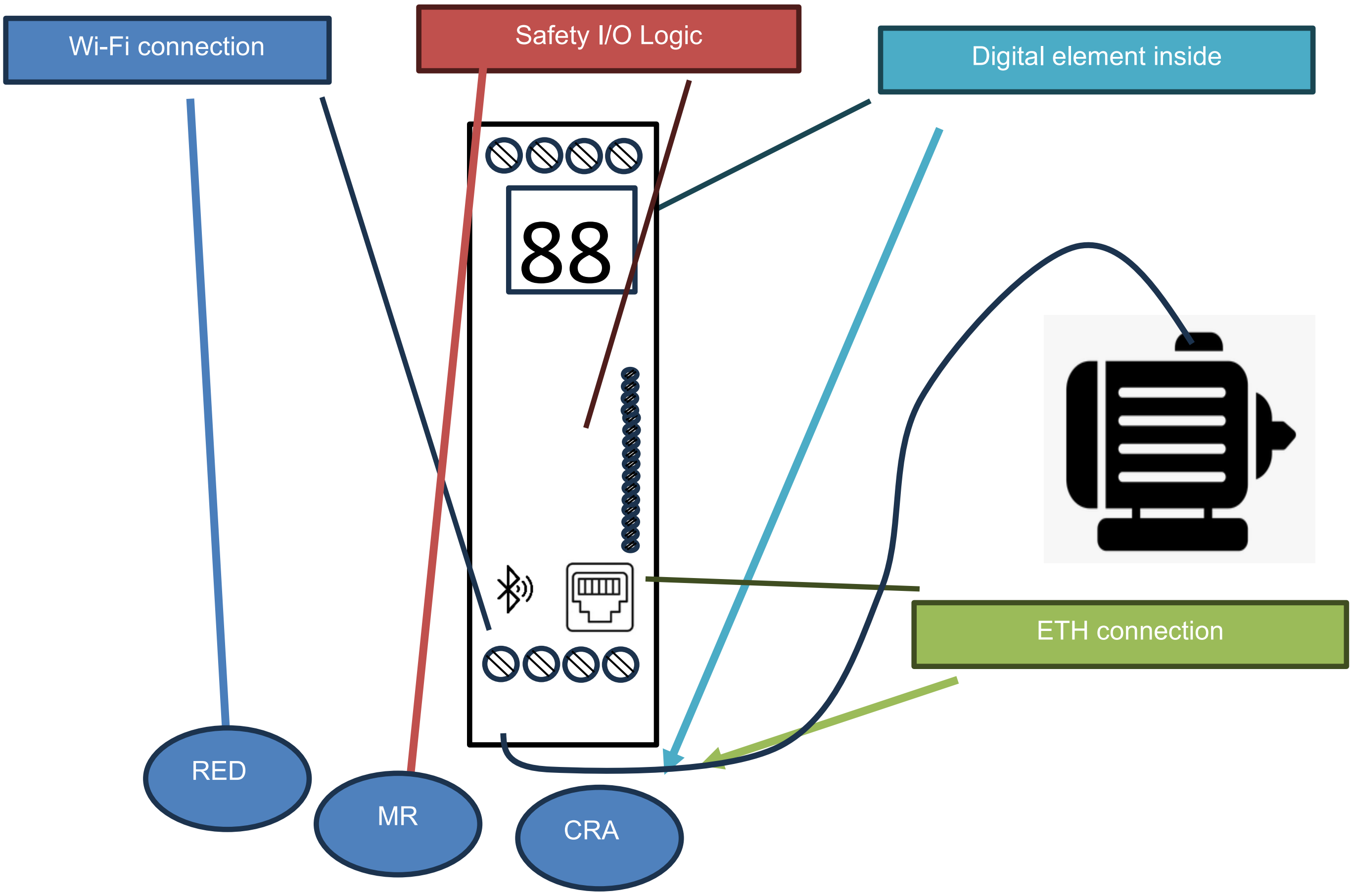


Figure 9 – Typical PDS with embedded safety function

Rationale:

- The PDS has a fieldbus connection that makes it possible to have remote connections; thus it is in the scope of the CRA.
- It also has a Wi-Fi interface for status monitoring, and thus it is also in the scope of RED.
- It also has embedded safety functions (e.g. STO) and is therefore also in the scope of MR.

According to the flowchart in figure 2, to fully address the requirements for cyber security the following standards have to be considered:

- The upcoming standards under the CRA (e.g. EN 40000 series)
- EN18031-1 for the RED Delegated Act 3.3(d)
- EN 50742 for the MR

Note: The user of the PDS may not use the embedded safety function. This does not affect the analysis that the manufacturer of the PDS has to complete to claim compliance for the product.

4.6 Summary table

The following table summarizes the rationale used in the examples and describes cyber requirements only; dedicated product requirements would also apply in addition to the below.

The table is designed to help and guide product manufacturers to navigate cybersecurity requirements across the various applicable Acts.

Possible interplay for different type of products

	SAFETY PLCs	SAFETY RELAY	SWITCHGEAR (not safety related)	LIMIT SWITCH (not safety related)	Limit switch (safety related)	POWER DRIVE SYSTEM (no embedded safety function)	POWER DRIVE SYSTEM (embedded safety function)
MR applies It is a Machinery according Art. 3 definition? See Note 1	YES It is a safety related component according Art 3 definitions	YES It is a safety related component according Art 3 definitions	NO	NO	YES It is part in a safety function for the machinery	NO	YES It has embedded safety functions (e.g. STO)
MR applies Cyber security requirements It has connectivity capability?	YES It has connection available for configuration	NO Purely passive electronics*	NO	NO	YES It has connection available for status feedbacks	NO	YES It has connection available for operation
RED applies It has radio connection capability? See Note 4	YES It has a radio connection to show off statuses.	NO	YES It has radio connection capabilities (e.g. Bluetooth)	NO	NO	YES It has radio connection capabilities (e.g. Wi.fi/ Bluetooth) for status monitoring	YES It has radio connection capabilities (e.g. Wi.fi/ Bluetooth) for status monitoring
CRA applies See Note 2 and 3	YES It has connection available for configuration	NO Due to the absence of connectivity.	YES Controllable via cloud application	YES It has connection available for status feedbacks	YES It has connection available for status feedbacks	YES It has connection available for operation	YES It has connection available for operation

NOTE 1. Machinery Regulation (EU) 2023/1230, Annex III clause 1.1.9, includes any connection of any nature (physical, logical and indirect) capable of exchanging data with an external system. The Machinery Regulation focuses on connections that can compromise safety.

An example is a connection from a machine to external systems such as building networks, cloud services, or service tools. The connectivity can exist through equipment permanently available on site, or equipment temporarily brought to the location during the installation, operation and maintenance, or decommissioning steps. Another example of machinery not to be considered is a simple drilling machine without any external connection e.g. no remote control or interfaces where no secrets (e.g.

password, encryption keys) can be extracted over the power supply line and where higher order attacks e.g. side channel attacks, are not considered.

NOTE 2. According to the Cyber Resilience ACT 2024/2847 a product with Digital element is identified as “a software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately” where the “data processing solutions” is intended as the software whose absence prevent the product with digital elements from performing one of its functions.

NOTE 3 See the “Orgalim / DigitalEurope guidance on internet-connected radio equipment” document when published.

NOTE 4. See “Applicability of the Radio Equipment Directive (RED) 2014/53/EU to CAPIEL Products “ guide.

5 Bibliograpy

EN ISO 12100

EN 40000 series

EN 18031-1

prEN 50742

Radio Equipment Directive (RED) 2014/53/EU

(EU) 2022/30 supplementing Directive 2014/53/EU delegated act

Machinery Regulation (MR) (EU) 2023/1230

Cyber resilience Act (CRA) (EU) 2024/2847

EU commission’s ”Blue guide”

6 History of this document

Stage	Revision	Date	Remark
Initial draft	0.1	2025-11-12	Internal CAPIEL review
Minor revision	0.2	2025-12-23	Internal CAPIEL review
Release of document	1.0	2026-03-26	Publication on CAPIEL website

Contact

Paolo Viviani
Email: paolo.viviani@omron.com

Lars-Magnus Felth
Email: lars-magnus.felth@se.abb.com

David Main-Reade
Email: dreade@rockwellautomation.com

Andrew Evans
Email: andrew.evans@gambica.org.uk

CAPIEL – European Coordinating Committee of manufacturers of electrical switchgear and controlgear - 17 rue de l’Amiral Hamelin - 75016 PARIS – France

EU Transparency Register ID: REG 498106892228-27 • www.capiel.eu

Date: 25.03.2026