Review of the draft prEN5042

© *Rob Hulsebos*

Version 2 January 2026

Introduction

Related to the new (upcoming) EU Machine Directive is the paragraph 1.1.9 about "protection against corruption". It's only about 1/3 page of text, and it doesn't give any details about how to approach the implementation.

> 1.1.9. *Protection against corruption*
>
> The machinery or related product shall be designed and constructed so that the connection to it of another device, via any feature of the connected device itself or via any remote device that communicates with the machinery or related product does not lead to a hazardous situation.
>
> A hardware component transmitting signal or data, relevant for connection or access to software that is critical for the compliance of the machinery or related product with the relevant essential health and safety requirements shall be designed so that it is adequately protected against accidental or intentional corruption. The machinery or related product shall collect evidence of a legitimate or illegitimate intervention in that hardware component, when relevant for connection or access to software that is critical for the compliance of the machinery or related product.
>
> Software and data that are critical for the compliance of the machinery or related product with the relevant essential health and safety requirements shall be identified as such and shall be adequately protected against accidental or intentional corruption.
>
> The machinery or related product shall identify the software installed on it that is necessary for it to operate safely, and shall be able to provide that information at all times in an easily accessible form.
>
> The machinery or related product shall collect evidence of a legitimate or illegitimate intervention in the software or a modification of the software installed on the machinery or related product or its configuration.

But for this there's now the European Norm "EN 50742", which recently had a draft published for public review[1]. This document is my first review of this draft.

[1] This one I found the best readable: https://komport.evs.ee/Default.aspx?s=standardCommenting&doc=19994. Note that you can also buy the draft EN 50742 for about €60, which is better readable in some cases (as the free online viewers do not have high-resolution pictures, or show all the tables).

Summary

The draft EN 50742 is 67 pages in size. It consists of the following chapters:

- Foreword + introduction
- Chapter 1: Scope
- Chapter 2: Normative references
- Chapter 3: Terms and definitions
- Chapter 4: Protection against corruption
- Chapter 5: Process requirements
- Chapter 6: Approach B process requirements
- Chapter 7: Product requirements
- Chapter 8: Approach B product requirements
- Chapter 9: Information for use
- Annex A: examples of logging formats
- Annex B: Threat assessment
- Annex C: Thread modelling for safety systems
- Annex D: List of threats and mitigations
- Annex ZZ: Relationship between this European Standard and the essential requirements of regulation EU 2023/1230 aimed to be covered
- Bibliography

The first 9 chapters form about 1/3 of the content, the annexes 2/3 of the remainder. Note that the annexes are "informative", i.e. they contain examples only, and so in no way enforce you to follow what's written there.

Not everything is written out yet, for example the paragraphs about "Safety Sensor" and "Safety Device with STO safety function"; both mention "This clause is under consideration for a future revision".

Below we will give a short summary of the main chapters.

Foreword

This section mentions that a machine must be safe, and that communication with the machine must not lead to hazardous situations. The manufacturer is to perform a risk assessment according to the standard EN ISO 12100 to identify all potential hazards. Risks should be assessed in terms of impact on functional safety.

The draft EN 50742 provides two approaches to fulfill its requirements. An implementer is free to choose between Approach A or Approach B, depending on personal / company preferences.

- "Approach A" (further described in chapters 5 and 7) is written to facilitate compliance for machinery, but without references to IEC 62443.
- "Approach B" (further described in chapters 6 and 8) is written to facilitate compliance for machinery, referring to IEC 62443 chapters 3-3, 4-1 and 4-2.

The EN 50742 is intended for use by machinery designers, control system manufacturers and integrators, and others involved in the specification, design and validation of an "SCS"[2].

Chapter 4: Protection against corruption

Before choosing the path of Approach A or Approach B, the general process requirements are to be followed:

- A risk assessment according to EN ISO 12100
- Define the security context for the machine

[2] What this abbreviation means is not explained.

- Eliminate all vulnerabilities that can lead to a hazardous situation (examples given: eliminate unnecessary interfaces , or do a redesign)
- If it is not possible to eliminate vulnerabilities, mitigate them
- If it is not possible to eliminate / mitigate all vulnerabilities, provide the user all necessary information to implement compensating countermeasures (examples are given in Annex C).

The next steps are the implementation of either Approach A or Approach B. Both are equally allowed to be followed.

Chapters 5 and 7 (Approach A)

Chapter 5 "Process requirements" contains only a flowchart named "Risk assessment process including safety and security aspects". There is no explanation of the activities and decision moments in the flow chart, but it doesn't look too difficult.

Chapter 7, "Product requirements", requires all machinery interfaces that are accessible and that can affect the safety of the machine to be identified. They need to be protected using countermeasures and compensating countermeasures. Examples of machine interfaces can be:

- Application protocols
- Wired and wireless interfaces
- Physical ports, USB, card readers, power supply, GPIO
- Embedded human-machine interface

Security measures to be implemented:

- Are selected on a risk-based approach
- Cryptography should use "state-of-the-art" algorithms[3]
- Logging of changes to safety parametrization or configuration parameters, changes to embedded software and application software, parametrization of HMI's (if it can create hazards), and software relevant for displaying safety instructions.
- Collect digital evidence of actions that changes/interrupts the behavior, state or operation of the machine, and deletion of the log file
- Logging requirements (also see Annex A)
- Storage duration requirements for at last 5 years
- Logs shall be protected against tampering.

The chapter then continues with the definition of "SRSL" – Safety Related Security Level SRSL0 .. SRSL3. How exactly this can SRLSx can be determined is described in Annex B (but since this is only an example, alternative methods can be used as well):

SRSL0	To be used for completely isolated safety systems
SRSL1	To protect safety functions when the attack potential is low, where an attack can only occur under specific circumstances
SRLS2	To protect safety functions when the attack potential is significant or critical, where an attack has a high likelihood of occurring or an attack is almost guaranteed to occur. This can be used for connection to untrusted networks, i.e. internet
SRSL3	To protect safety functions when the attack potential is significant or critical, where an attack has a high likelihood of occurring or an attack is almost guaranteed to occur. This can be used for connection to untrusted networks, i.e. internet

[3] The draft EN 50742 refers to a 12-year old ENISA document (with a wrong URL in the bibliography; this is the right URL: https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014), and a reference to a BSI document. Both require quite some background in mathematics and cryptography, which I think is not present in most companies, so how does one choose what is a state-of-the-art algorithm?

The implementation of the security protection requirements depends on the SRSLx that has been chosen. For example, the "authentication requirements":

SRSL0	None
SRSL1	Entities shall be authenticated
SRSL2	Entities shall be authenticated
SRSL3	Entities shall be uniquely authenticated

The same follows for "authorization requirements", the "software and information integrity", "integrity of boot process", "information exchange integrity", "input data validation", "physical tampering", and "authenticity of safety-related application software and safety-related embedded software".

Finally, there must be functionality to identify software versions and configuration information, available on demand, and in human-readable form, either built-in or via an external tool.

Chapters 6 and 8 (Approach B)

Chapter 6 "Process Requirements" consist only of a single sentence, namely that EN IEC 62443-4-1 shall apply. This still means a lot of work if there is nothing. But if an organization already works according to the 4-1, it is an easy win.

In chapter 8, the requirements for a *machinery system* are listed:

Foundational Requirement (FR)	Security Level	Security Requirements
FR 1 – Identification and authentication control (IAC)	SL-C2	SR1.1
FR 2 – Use control (UC)	SL-C2	SR2.1, SR2.8, SR2.9
FR 3 – System integrity (SI)	SL-C2	SR3.1, SR3.4, SR3.5, SR3.6
FR 4 – Data confidentiality	None	None
FR 5 – Restricted data flow (RDF)	SL-C1	SR5.1
FR 6 – Timely response to events (TRE)	SL-C1	SR6.1
FR 7 – Resource availability (RA)	SL-C2	SR7.1, SR7.2

Here we see the familiar 62443-style of chapter 3-3, choosing an SL-C (Security Level Capability) of 1 and 2, and only 12 (of the 51) Foundational Requirements need an implementation.

There are also requirements for a *machinery component*:

Foundational Requirement (FR)	Security Level	Security Requirements
FR 1 – Identification and authentication control (IAC)	SL-C2	CR1.1, CR1.2
FR 2 – Use control (UC)	SL-C2	CR2.1, CR2.6, CR2.8, CR2.9, CR2.12, EDR 2.13
FR 3 – System integrity (SI)	SL-C2	CR3.1, CR3.4, CR3.5, CR3.6, EDR3.2, EDR3.11, EDR3.14
FR 4 – Data confidentiality	None	
FR 5 – Restricted data flow (RDF)	SL-C1	CR 5.1
FR 6 – Timely response to events (TRE)	SL-C1	CR 6.1
FR 7 – Resource availability (RA)	SL-C2	CR 7.1, CR7.2

This table follows the familiar 62443-style of chapter 4-2.

A machinery component may have a lower SL-C than required in the table above if it is part of a machinery system, if the machinery system can provide compensating countermeasures. This must be properly documented: which requirements are not fulfilled by the component, and which compensating countermeasures must be implemented at the system level.

Finally, there must be functionality to identify software versions and configuration information, available on demand, and in human-readable form, either built-in or via an external tool. Persistency of audit records shall be at least 5 years (both requirements are the same as mentioned in Approach A).

Annex A: Examples of logging formats

Describes two examples of logging formats: CLF (Common Log Format), and Syslog. But note that you do not have to use this, these are examples only.

Annex B: Threat assessment

This chapter serves to objectively determine a "Safety-Related Security Level" (SRSL). Its value is derived from an "Exposure Level" (EL), "Attacker Capability Score" (AC), "Window of Opportunity Score" (WoO), according to the formula:

Attack Potential Score = (EL * WoO) + AC

Which then translates to an "Attack Potential" AP0..AP5, as listed in this table:

Attack Potential Score	Label	Description	Interpretation
0–5	AP0	Very Low	Minimal attack potential; highly unlikely to occur
5.1–10	AP1	Low	Low attack potential; can occur under very specific circumstances
10.1–15	AP2	Medium	Moderate Attack Potential; Has a reasonable likelihood of occurring
15.1–20	AP3	High	Significant Attack Potential; Has a high likelihood of occurring
> 20	AP4	Very High	Critical Attack Potential; An attack is almost guaranteed to occur,

The AP value is then mapped to the Severity Level (see chapter 5 on how this decides the implementation of some measures):

		Attack Potential (AP)				
		AP0	AP1	AP2	AP3	AP4
Severity Level	low/e.g. reversible	SRSL0	SRSL1	SRSL1	SRSL2	SRSL3
	high/e.g. non reversible	SRSL0	SRSL1	SRSL2	SRSL3	SRSL3

Annex C: Threat model for safety systems

This is the largest chapter in the EN 50742 (35 pages!). It gives examples of a process to determine appropriate and adequate countermeasures to protect a machine against corruption. It describes the steps to be executed to determine appropriate and adequate countermeasures for protection against corruption. Four examples are used:

- Simple form-filling machine
- Wireless controller for loading crane
- Safety sensor[4]
- Safety sensor with STO safety function sensor (idem)

[4] However, there is no description for it, it is "under consideration for a future revision"

The chapter then describes the steps to be taken for each of these 4 examples:

- Determine assets that have an implication on safety
- Determine the security context
- Draw a data flow diagram (detailing all communication and elements)
- Determine trust boundaries: areas at a similar level of trust, which should be isolated from other areas at a different level of trust)
- Determine where corruption can cause adverse effects (according to EN ISO 12100).
- Finally, all safety-related threats that have been found are to be written down in a table. Per threat, classify it by assigning the preconditions for exploitation, and map it to a set of defined standard threats (as listed in annex D).

Annex D: List of threats and mitigations

This chapter describes how to counter threats via mitigations, and (if not practically reasonable) via compensating countermeasures. Some mitigations that are mentioned: input validation, least privilege principle, secure defaults, immutable application code, read-only memory, separate memory for execution and data, and the Kerckhoff principle for encryption.

The first table lists 16 common threat types, and possible mitigations. For example, for threat "attacker has access to the wireless network" a possible mitigation is "CCM3: Encryption of wireless protocol".

It also has a table listing 20 common threat types, and possible mitigations (in some cases). For example, for threat "manipulation via physical means" a possible mitigation is "Allow physical access only with a special key – not via readily available tools such as screwdrivers".

Conclusion

This draft EN 50742 is far from complete. But that's what a draft is intended for. Let the discussion start!

One thing I wonder is whether those *not* working in cybersecurity will be able to implement its requirements. And those working in cybersecurity know nothing about safety.

Note the clock is ticking, only one year to go before the Machinery Directive comes into effect. Hopefully the final draft EN 50742 will be published soon. Perhaps another draft version will be published first.

But as of today (January 2026) you have no official guidance on what to *do*. Personally I'd bet on an implementation following the IEC 62443, or "Approach B". This standard already exists and there is a lot of knowledge in the market. You could already start with it today!

History:

2 January 2026	Version 1