



# SLOVENSKI STANDARD

## oSIST prEN 50742:2026

---

### Varnost strojev - Zaščita pred degradacijo

Safety of machinery - Protection against corruption

Sécurité des machines - Protection contre la corruption

Ta slovenski standard je istoveten z: prEN 50742:2025

---

#### ICS:

03.100.02	Upravljanje in etika	Governance and ethics
13.110	Varnost strojev	Safety of machinery

**oSIST prEN 50742:2026**

**en,fr,de**



EUROPEAN STANDARD  
NORME EUROPÉENNE  
EUROPÄISCHE NORM

**DRAFT**  
**prEN 50742**

December 2025

ICS 13.110

English Version

**Safety of machinery - Protection against corruption**

To be completed

To be completed

This draft European Standard is submitted to CENELEC members for enquiry.  
Deadline for CENELEC: 2026-02-27.

It has been drawn up by CLC/TC 44X.

If this draft becomes a European Standard, CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

This draft European Standard was established by CENELEC in three official versions (English, French, German).  
A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.



European Committee for Electrotechnical Standardization  
Comité Européen de Normalisation Electrotechnique  
Europäisches Komitee für Elektrotechnische Normung

**CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels**

1	Contents	Page
2	European foreword.....	3
3	Introduction .....	4
4	1 Scope .....	5
5	2 Normative references .....	5
6	3 Terms and definitions .....	6
7	4 Protection against corruption .....	8
8	4.1 General.....	8
9	4.2 Connection of machinery.....	8
10	4.3 General process requirements.....	8
11	5 Process requirements .....	10
12	5.1 Introduction .....	10
13	6 Approach B process requirements.....	10
14	7 Product requirements .....	11
15	7.1 Interfaces .....	11
16	7.2 Security measures .....	11
17	7.2.1 General.....	11
18	7.2.2 Cryptography .....	11
19	7.3 Information collection .....	12
20	7.3.1 Types of interventions .....	12
21	7.3.2 Intervention evidence to be collected .....	12
22	7.3.3 Logging requirements.....	12
23	7.3.4 Storage duration requirements .....	13
24	7.3.5 Storage protection requirements.....	13
25	7.4 Protection measures against corruption .....	13
26	7.4.1 General.....	13
27	7.4.2 Safety-related Security levels.....	13
28	7.4.3 Security protection requirements .....	14
29	7.5 Identification of software versions and configuration.....	16
30	8 Approach B product requirements .....	17
31	8.1 General.....	17
32	8.2 Machinery systems.....	17
33	8.3 Machinery components.....	17
34	8.4 Identification .....	18
35	8.5 Persistency.....	18
36	9 Information for use .....	18
37	Annex A (informative) Examples of logging formats.....	19
38	Annex B (informative) Threat assessment.....	20
39	Annex C (informative) Threat modelling for safety systems .....	25
40	Annex D (informative) List of threats and mitigations.....	62
41	Annex ZZ (informative) Relationship between this European Standard and the essential requirements of Regulation (EU) 2023/1230 aimed to be covered .....	66
42		
43	Bibliography .....	67

## 44 European foreword

45 This document (prEN 50742:2025) has been prepared by CLC/TC 44X "Safety of machinery: electrotechnical  
46 aspects".

47 This document is currently submitted to the Enquiry.

48 The following dates are proposed:

- latest date by which the existence of this (doa) dav + 6 months  
document has to be announced at national level
- latest date by which this document has to be (dop) dav + 12 months  
implemented at national level by publication of  
an identical national standard or by  
endorsement
- latest date by which the national standards (dow) dav + 36 months  
conflicting with this document have to be (to be confirmed or  
withdrawn modified when voting)

49 This document has been prepared under a standardization request addressed to CENELEC by the European  
50 Commission. The Standing Committee of the EFTA States subsequently approves these requests for its  
51 Member States.

52 For the relationship with EU Legislation, see informative Annex ZZ, which is an integral part of this document.

iTeh Standards  
(<https://standards.iteh.ai>)  
Document Preview

[oSIST prEN 50742:2026](https://standards.iteh.ai/catalog/standards/sist/07a63742-502d-4d13-bdb9-17a86e07b9f8/osist-pren-50742-2026)

<https://standards.iteh.ai/catalog/standards/sist/07a63742-502d-4d13-bdb9-17a86e07b9f8/osist-pren-50742-2026>

## 53 Introduction

54 Machinery must be safe in order to prevent injuries and loss of life.

55 The communication with the machine must not lead to hazardous situations.

56 The manufacturer performs a risk assessment according to EN ISO 12100 to identify all potential hazards.

57 Vulnerabilities can lead to a corruption of the control system of the machine and hazards can lead to dangerous  
58 situations.

59 By exploitation of vulnerabilities via communication with the machine, the machine could be operated outside  
60 safe parameters or degrade safety functions.

61 Vulnerabilities cannot create new hazards.

62 The probability that someone will use a vulnerability for a malicious attempt cannot be predicted.

63 The risk can only be assessed in terms of its impact on functional safety.

64 Vulnerabilities are divided into several types.

65 This document provides two approaches:

66 — Approach A (Clause 5 and 7) has been developed to facilitate compliance for machinery developed without  
67 references to EN IEC 62443 series of standards.

68 — Approach B (Clauses 6 and 8) has been provided to facilitate compliance for machinery developed in the  
69 context of the EN IEC 62443-3-3:2019, EN IEC 62443-4-1:2018, EN IEC 62443-4-2:2019.

70 NOTE 1 The EN IEC 62443 series provides information and a methodology to approach cybersecurity.

71 This document is intended for use by machinery designers, control system manufacturers and integrators, and  
72 others involved in the specification, design and validation of an SCS.

73 NOTE 2 See EN IEC 62443-4-1:2018; the manufacturer can be a product supplier or system integrator.

74 This document does not address the role of the user.

<https://standards.iteh.ai/catalog/standards/sist/07a63742-502d-4d13-bdb9-17a86e07b9f8/osist-pren-50742-2026>

## 1 Scope

This document provides requirements and recommendations for protection against corruption for machinery, related products and partly completed machinery referred to in this document as 'machinery'.

This document provides requirements and recommendations to prevent accidental and intentional (including malicious) corruption of machines resulting in hazardous situations.

This document applies to:

- hardware components, including interfaces to remote devices and control systems, that can transmit signals or data;

- software and data;

if they could influence the safety of the machinery.

NOTE 1 Topics can overlap with the domain of cybersecurity but are not necessarily identical in their coverage.

NOTE 2 This document does not describe functional safety requirements of control systems in machinery.

This document specifies requirements to related risks in all lifecycle steps.

Machinery interfaces to external systems and services are in the scope of this document. External systems and services are out of the scope of this document.

This document does not apply to machinery installed before the date of its publication.

This document specifies requirements related to protection against corruption related risks in all lifecycle steps such as:

- development;

- manufacturing;

- commissioning;

- operation;

- maintenance;

- decommissioning.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

EN ISO 12100:2010, *Safety of machinery - General principles for design - Risk assessment and risk reduction (ISO 12100:2010)*

EN IEC 62443-3-3:2019,<sup>1</sup> *Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels*

EN IEC 62443-4-1:2018, *Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements*

<sup>1</sup> As impacted by EN IEC 62443-3-3:2019/AC:2019.