Guideline Machinery Regulation

The implementation of the Machinery Regulation

Status: September 2026

The implementation of the Machinery Regulation

Contents

Important notice

This guideline provides a concise and practical overview of the main issues arising from the transition to Regulation (EU) 2023/1230. Although every effort has been made to keep the document focused, the scope and complexity of the subject require a certain level of detail. The guideline is intended to help manufacturers identify relevant requirements, responsibilities and practical actions.
The information in this guideline has been prepared with due care and based on the information available at the time of publication. It provides general guidance only and must not be regarded as legally binding, exhaustive or as a substitute for a product-specific conformity assessment, risk assessment or professional advice. Readers and manufacturers remain responsible for verifying the applicable legal, normative and technical requirements and for applying their own professional judgement to the specific product and use case.
The checklists, examples and action points included in the annexes are intended as initial points of reference to support orientation, discussion and further analysis. They are not exhaustive and should not be treated as complete compliance checklists. Depending on the product, its intended use, its interfaces and the applicable legal and technical framework, additional requirements, risks and actions may need to be considered.
This document reflects the current state of knowledge and is not fixed or final. It may be revised as legislation, harmonised standards, official guidance, interpretations or technical knowledge develop. Users should therefore ensure that they consult the latest applicable sources before taking decisions or placing machinery on the market.

This guideline reflects the information available as of September 2026 and may be updated to take account of new information and developments.

Introduction

The Machinery Regulation (EU) 2023/1230 will replace the Machinery Directive 2006/42/EC and will apply from 20 January 2027. The change from a directive to a directly applicable regulation is intended to ensure more uniform machinery safety requirements across the European Union and to adapt the legal framework to technological developments. In particular, the Regulation recognises that digitalisation, software-controlled functions and network connectivity can create new risks where manipulation, unauthorised access or software changes affect the safe operation of machinery. This guideline focuses primarily on these safety-related cybersecurity aspects and their practical implications for manufacturers.

1. The Machinery Directive and the Machinery Regulation

The core of both the Machinery Directive 2006/42/EC and the Machinery Regulation (EU) 2023/1230 remain unchanged:

The manufacturer is responsible for ensuring that the machinery is designed and constructed in such a way that, when used as intended and in the event of reasonably foreseeable misuse[1], it can be used safely and does not pose any unacceptable risks to persons.

This fundamental principle is implemented by both sets of regulations through the same core elements:

- Carrying out a risk assessment.
- Application of the three-step approach:
  1. inherently safe design
  2. technical protective measures
  3. user information/residual risks
- Compliance with the essential health and safety requirements.
- Demonstration of conformity prior to placing the machinery on the market.
  Provision of safe machinery, including the necessary operating instructions and labelling

The Machinery Directive 2006/42/EC and the Machinery Regulation (EU) 2023/1230 pursue the same fundamental safety objective: machinery must be safe when used as intended and in the event of reasonably foreseeable misuse. The manufacturer must therefore carry out a risk assessment and reduce risks to an acceptable level by appropriate design, technical and organizational measures.

2. The new Machinery Regulation

The Machinery Regulation responds to the increasing digitalisation, software control and networking of machinery and aims to ensure a more uniform application of machinery safety requirements across the EU.
The fundamental safety objective of the Machinery Regulation is no different from that of the pervious Machinery Directive: the manufacturer must ensure that an item of machinery does not pose any unacceptable risks to persons when in use ("*safety in use*").

What is new, however, is that machinery has undergone fundamental changes in recent years with increasingly digitalized, networked and software-controlled elements. Safety functions are now frequently implemented via software; machinery communicates via networks, receiving updates or exchange data with other systems. This gives rise to new hazards that can no longer be fully managed by traditional safety measures alone.

[1] "Reasonably foreseeable misuse" does not refer to every theoretically conceivable or deliberately malicious use. Consideration must be given to misuse that is plausibly foreseeable on the basis of typical human behaviour, e.g. bypassing a safety device because it makes work more difficult, remaining within the movement range of a door in relation with its intended use, using a drive system with an unsuitable or incorrectly adjusted door, altering accessible parameters relating to force, speed or end positions. Decisive factors include, amongst others, the intended user group, the foreseeable usage situation, experience with comparable products, known accidents and near-misses, and the question of whether the design practically encourages misuse (Art 3, No 24, (EU) 2023/1230).

For the first time, the Machinery Regulation makes it clear that digital technologies, software, connectivity and security-related events must be considered in the risk assessment where they may affect the safety of the machine.

The Machinery Regulation takes this development into account and extends the existing requirements to include aspects of functional software integrity, the safety of digital control systems and cybersecurity, insofar as these affect the safety of the machinery. The aim is to prevent tampering, unauthorized access or software faults that could impair safety-related functions and thus jeopardise safety in use.

The Machinery Regulation does not fundamentally change the safety objective. However, it extends the concept of safety by recognising that security-related manipulation can affect the safe operation of machinery.

Practical consequence:
Manufacturers should review whether software, communication interfaces, remote access functions or update mechanisms can influence safety-related functions.

3. Harmonised Standards

3a – Harmonised standards and Conformity

Harmonised standards translate the broadly formulated essential health and safety requirements of the Machinery Regulation into specific technical solutions and provide manufacturers with a recognised basis for designing safe machinery.
If a manufacturer fully applies harmonised standards, they may claim the so-called 'presumption of conformity'[2] for the requirements covered by these standards. This makes it easier to demonstrate that the relevant requirements of the Machinery Regulation have been met. However, responsibility for the conformity of the machinery always remains with the manufacturer.

Harmonised standards help manufacturers demonstrate conformity with the Machinery Regulation. If the relevant requirements are covered, their application may provide a presumption of conformity. Where no suitable harmonised standard is available, conformity must be demonstrated by other appropriate means and, where required, with the involvement of a notified body.

3b – Harmonised standards – ready for the MR? The Gap-analyses

Harmonisation of standards under the Machinery Regulation does not take place automatically. The standards must be reviewed to ensure that they cover all the requirements of the new Regulation. In particular, the new requirements relating to digital technologies, software, networked functions and cybersecurity may necessitate amendments or additions to existing standards.

[2] Art 20 Para 1 of Regulation (EU) 2023/1230

The aim is to provide harmonised standards under the Machinery Regulation as well, which will continue to allow manufacturers to benefit from the presumption of conformity for the requirements covered by those standards.

The transition of harmonised standards from the Machinery Directive to the Machinery Regulation is not limited to the inclusion of cybersecurity requirements. Rather, each standard must be systematically assessed to determine the extent to which it already covers the amended and new essential health and safety requirements of the Machinery Regulation.

To this end, CEN/CENELEC has provided the Technical Committees with a standardised gap analysis procedure. On this basis, the standardisation bodies assess, for each individual requirement of the Machinery Regulation, whether it is relevant to the standard in question, whether it is already adequately addressed, or whether additions are required. The results of this analysis form the basis for the targeted revision of the standards and their subsequent harmonisation under the Machinery Regulation.

The relevant standards for the door industry – EN 17352, EN 16005 (for power operated pedestrian doorsets), EN 12453 and EN 12978 (for industrial/commercial/garage doors) – were reviewed on the basis of a checklist provided by CEN. In doing so, the amendments were ‘synchronised’, as they constitute additions to the individual standards that apply across all product types.

3c - Harmonised standards and the OJEU from the end of January 2027

The Commission and CEN have announced their intention to make the standards currently listed in the Official Journal of the European Union (OJEU) under the Machinery Directive available for citation under the Machinery Regulation as part of the transition. The timing and final form of the first publication have not yet been confirmed. It is currently expected that such citations may include restrictions identifying provisions of Annex III to Regulation (EU) 2023/1230 for which the respective standard does not confer a presumption of conformity. This guideline therefore provides guidance on how manufacturers may address the resulting gaps.

For illustrative purposes only, a future OJEU listing could take the following form. The structure, wording, dates and restrictions shown below are hypothetical and may differ from the Commission’s final publication.

ESO	Reference and title of the harmonised standard (and reference document)	First publication OJ	Reference of superseded standard	Date of cessation of presumption of conformity of superseded standard Note 1
CEN	EN 16005:2023+A1:2024 Power operated pedestrian doorsets - Safety in use - Requirements and test methods	27.01.2026	DD.MM.YYYY	-
Warning: With regard to paragraph X and Annex Y, this publication does confer a presumption of conformity to the essential health and safety requirements 1.x.x, 1.y.y, 1.z.z. of Annex III to Regulation (EU) 2023/1230.				

The Commission and CEN have also indicated that the list of gaps identified by CEN between the Machinery Directive and the Machinery Regulation should not be regarded as exhaustive. In addition to the main topics of ‘cybersecurity’ and ‘corruption’, further

gaps or restrictions may therefore be identified when an individual standard is listed in the OJEU.

4. Outcome of the Gap-analyses

The standards are currently being revised in areas including protection against corruption (e.g. connection to communication networks) and the security and reliability of control systems (e.g. logging).

For this document, it is important to distinguish between safety, security and corruption. Safety refers to the protection of persons against hazards caused by the machinery. Security refers to protection against unauthorised access, manipulation or attacks. Corruption is relevant where such changes affect safety-related functions, software, data, parameters or configurations and may therefore impair the safe operation of the machinery.
The most significant amendment was made to the 'Corruption' requirement. For EN 17352, EN 16005 (for power operated pedestrian doorsets), EN 12453 and EN 12978 (for industrial/commercial/garage doors) the 'Corruption' requirement is being amended.

Practical consequence:
For manufacturers, this means that the assessment of software integrity and protection against unauthorised modifications becomes an integral part of the conformity process. Where several components are combined, this is particularly relevant for the manufacturer of the final machinery.

5. Declaration of Conformity (DoC)

Before a machinery product or related product is placed on the market under Regulation (EU) 2023/1230, the manufacturer shall complete the applicable conformity assessment procedure and prepare and sign the EU Declaration of Conformity (DoC).

The DoC shall identify the product and the manufacturer and state that the declaration is issued under the sole responsibility of the manufacturer. It shall also identify the applicable Union legislation and, where appropriate, the relevant harmonised standards or other technical specifications and the notified body involved in the conformity assessment (see also Annex D.2 of this guideline).

The declaration shall follow the structure and contain the information specified in Annex V, Part A of the Machinery Regulation. By signing the DoC, the manufacturer assumes responsibility for the conformity of the product.

Where an existing EC type-examination certificate issued under Directive 2006/42/EC is relied upon as supporting evidence, the manufacturer shall perform and document a product-specific gap and risk assessment against the new and amended requirements of Regulation (EU) 2023/1230 before issuing the DoC. This assessment shall establish whether the product complies with all applicable essential health and safety requirements, including those concerning safety-related software, protection against unintended or intentional corruption, communication interfaces, remote access, software updates and the traceability of safety-relevant changes.

Identified gaps shall be closed and the supporting evidence shall be included in the technical documentation. The validity of an existing type-examination certificate (see Annex E) alone is not sufficient evidence that the additional requirements of the Machinery Regulation have been fulfilled.

Where harmonised standards covering the relevant requirements are available and fully applied, they may provide a presumption of conformity for the requirements they cover. Where such standards are unavailable, incomplete or not fully applied, compliance shall be demonstrated through the documented risk assessment, appropriate technical specifications, verification and validation evidence and, where required by the applicable conformity assessment procedure, the involvement of a notified body.
Particular attention shall be given to assessing whether unintended or intentional changes to safety-related software, parameters, configurations or data could affect machinery safety and to documenting the corresponding protective measures.

The signed DoC shall be kept up to date and retained as part of the technical documentation. It shall accompany the relevant product or be made available in the manner permitted by the Regulation. The conformity assessment, technical documentation and DoC shall be completed before the product is placed on the market or put into service.

For partly completed machinery, an EU Declaration of Incorporation in accordance with Annex V, Part B to Regulation (EU) 2023/1230 shall be issued instead of an EU Declaration of Conformity. Further guidance on partly completed machinery is provided in Annex C and Annex D.2 of this guideline.

6. EN 50742 – the solution to corruption

In this context, cybersecurity is not introduced as an independent objective of machinery law. It becomes relevant only where a security-related event may affect the safe operation of the machinery. EN 50742 therefore addresses the interface between machinery safety and protection against unauthorised or unintended changes to safety-related functions, software, data or configurations (see also Annex A of this guideline).

6a - The standard fills a genuine gap

The new Machinery Regulation (EU) 2023/1230 explicitly requires, for the first time, that machinery must be protected against unintentional and deliberate alterations (Annex III, including Section 1.1.9). Traditional functional safety (e.g. EN ISO 13849 or IEC 62061) addresses failures but pays little attention to targeted manipulation or software tampering.

This is precisely where EN 50742 comes in. It sets out requirements for protection against:

- unintended changes to parameters,
- faulty software updates,
- manipulated configurations,

EN 50742 provides a practical framework for addressing safety-relevant corruption. It does not aim to make machinery fully cybersecure, but focuses on unauthorised or unintended changes to functions, software, data and configurations where these may affect machine safety. Once EN 50742 is listed as a harmonised standard under the Machinery Regulation, its application may provide a presumption of conformity for the requirements covered by the

- unauthorised access,
- deliberate attacks, insofar as these may affect machinery safety.

6b - It is not a cybersecurity standard
EN 50742 explicitly states that it does not cover the entirety of the cybersecurity of machinery. It focuses exclusively on changes that could pose a security risk. This is a key difference compared to standards such as:

- IEC 62443
- ISO/IEC 27001

EN 50742 therefore does not answer the question: "Is my machinery completely IT-secure?", but rather: "Could tampering cause safety functions to fail?" – which is apparently the more important question in our industry.

7. EN 50742 – the lonely standard for the '*cyber-world*'?

The Machinery Regulation makes it clear for the first time that safety and security are no longer separate spheres. The standards landscape is therefore evolving from a 'side-by-side' approach towards a holistic concept. EN 50742 is the central standard addressed in this chapter. The other standards are included only to clarify their complementary roles and to show where EN 50742 fits within the overall machinery safety and security framework. The roles of the key standards can be described as follows:

Standard	Key question	Focus
EN ISO 12100	What are the risks?	Risk analysis
EN ISO 13849-1	Does the safety feature work reliably?	Functional safety
IEC 62061	Which SIL requirements apply?	Functional safety
IEC 62443	How can I prevent cyber-attacks?	Cyber security
EN 50742	How can I prevent security-critical tampering?	Safety ↔ Security Interface

7a - EN ISO 12100 remains the 'cornerstone of all considerations'
Even under the Machinery Regulation, everything begins with the risk assessment. In the past, the questions were:

- Can a sensor fail?
- Can a valve jam?

Today, the following questions have been added:

- Could someone alter the safety parameters?
- Could a safety function be rendered ineffective by a faulty update?
- Could a diagnostic function be manipulated?

This means that corruption becomes a hazard that must be considered in the risk assessment.

7b - EN ISO 13849 and IEC 62061 continue to address the classic safety question
EN ISO 13849-1 and IEC 62061 primarily address the design and reliability of safety-related control functions, including systematic and random failures within their respective scopes. They do not, however, provide a complete framework for assessing deliberate manipulation, unauthorised changes or the wider security of connected machinery. EN 50742 complements these standards where such security-related events may affect machinery safety.

- Wire break
- Welded contacts
- CPU failure
- Short circuit
- Hardware ageing

However, they do little to answer questions such as:

- What happens if the PL-e parameter is changed?
- What happens following a tampered firmware update?
- What happens if diagnostic functions are deactivated?

This is precisely where their scope ends.

7c - IEC 62443 takes an IT-based approach
The IEC 62443 series takes a comprehensive industrial automation and control system security approach. It addresses matters such as identification and authentication, use control, system integrity, restricted data flow, secure remote access and vulnerability management. EN 50742 has a narrower machinery-safety focus: it uses appropriate security measures where unauthorised or unintended changes could impair safety-related functions.

- Who is authorised to log in?
- How are passwords managed?
- Is the network segmented?
- Are certificates used?
- Is remote access secured?
- How are vulnerabilities addressed?

The aim is to ensure the security of the entire automation system. Whether this compromises a safety function is, initially, of secondary importance.

7d - EN 50742 brings the best of both worlds together

EN 50742 provides the machinery-safety-specific link between the risk assessment, functional safety considerations and suitable security measures. It focuses on identifying safety-related assets and determining where protection against unauthorised or unintended changes is necessary to maintain machinery safety.
That is precisely where its real strength lies. It asks: “What data must never be altered without authorisation?”

For example:

- Safety parameters
- Configuration data
- Firmware
- Safety programmes
- Safety certificates
- Calibration data
- Safety-relevant recipe parameters

It requires appropriate protective measures for this data. It is therefore not concerned with just any file on the machinery, but exclusively with data that affects machinery safety.

8. Conclusion - A paradigm shift

Until now, the prevailing mindset has been:

Safety = protection against failures.

The Machinery Regulation does not fundamentally change the safety objective. However, it recognises that safety-related functions may be affected not only by failures, but also by unauthorised changes, manipulated parameters, software corruption or external interference.
Consequently, the traditional view of safety is expanded:

Safety = protection against failures and protection against unauthorised changes.

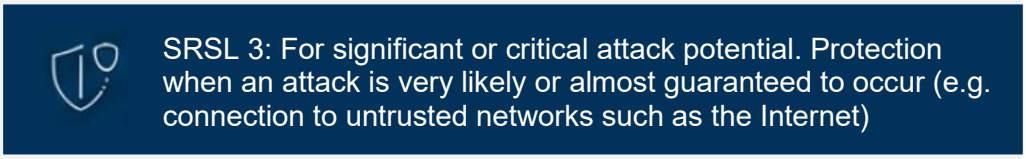
This represents a significant shift in perspective. Manufacturers must therefore not only consider whether safety-related functions are reliable and fault tolerant, but also whether they are adequately protected against intentional or unintentional manipulation.
The Machinery Regulation expands the traditional concept of functional safety to include the integrity of safety-related data, software and configurations.

Annex A
EN 50742 – a guideline

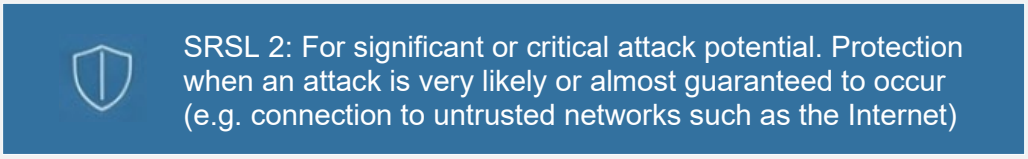
A.1
Safety-Related Security Levels (SRSL)

EN 50742 uses Safety-Related Security Levels (SRSL) to define the degree of protection required against corruption of safety-relevant data. The required SRSL depends on the identified attack potential and the possible severity of harm.

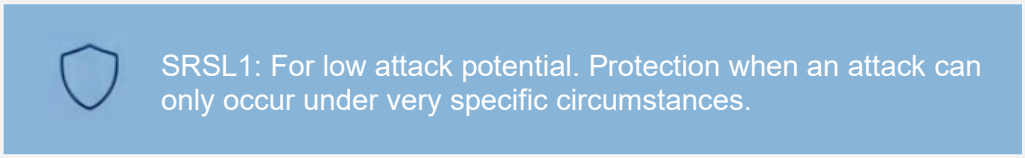
SRSL 3:
High attack potential



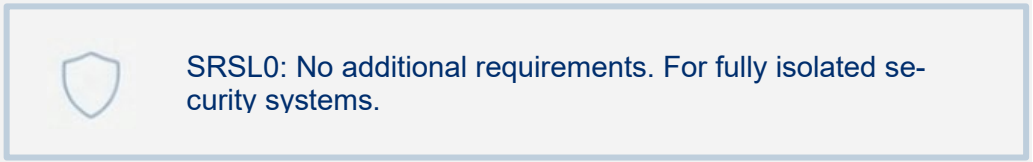
SRSL 2:
Moderate attack potential



SRSL 1:
Low attack potential

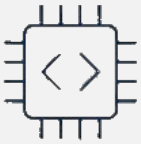


SRSL 0:
No attack potential



A.2
Definition of asset categories

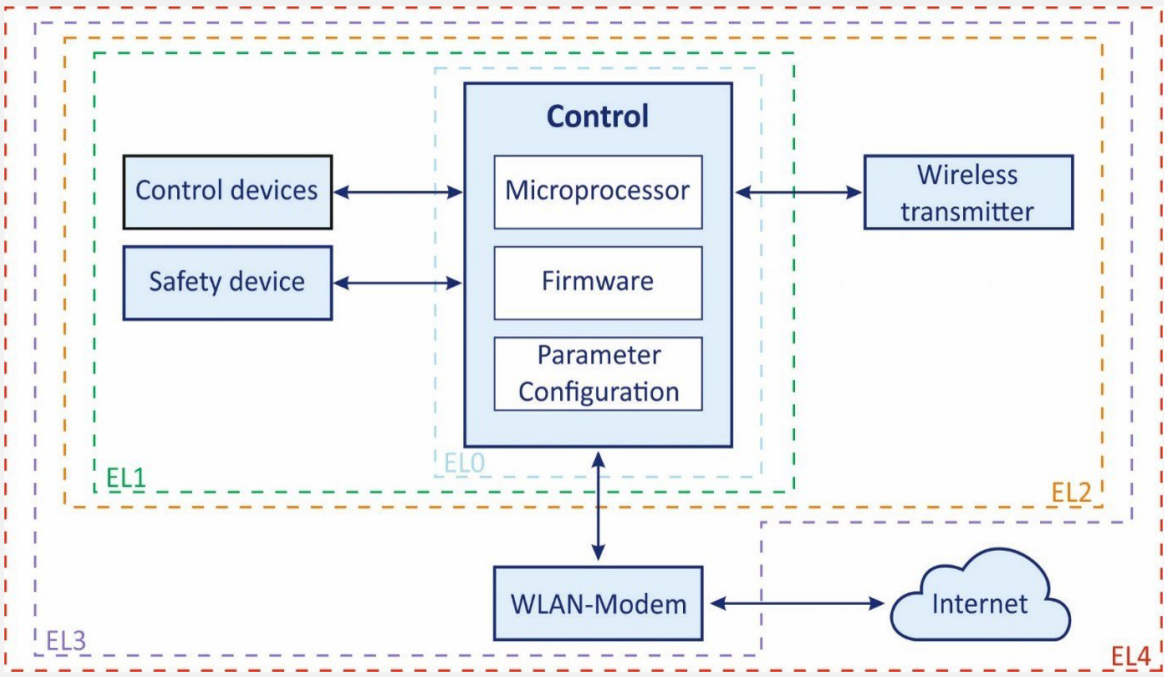
As a first step, all safety-relevant assets must be identified. EN 50742 distinguishes between functions, software, configuration data, input data and hardware.

Function	Software	Configuration Data	Input Data	Hardware
				
Functions, especially security functions as risk mitigation measures	Safety-related application software and embedded software	Data and safety configuration data	Process data on safety-related connections	Components

A.3
Drawing the Trust Boundaries

Trust boundaries define where authorised control ends and where potentially untrusted access begins. They are used to identify interfaces that may require additional protective measures.

In the example shown below, the different Exposure Levels (EL) illustrate how easily a safety-related asset can be accessed. EL0 represents fully trusted internal elements, whereas EL4 represents interfaces exposed to public networks such as the Internet. The trust boundaries help to identify where additional protection measures may be required.



Key:

EL0 = Internal trusted area
EL1 = Physical access required
EL2 = Local access
EL3 = Adjacent network access
EL4 = Public network exposure

A.4
Assess attack potential (AP)

The attack potential (AP) is determined by combining exposure level, window of opportunity and attacker capability. The result is used to derive the necessary SRSL.

AP = (EL x WoO) + AC

1. Exposure Level (EL)	2. Window of Opportunity (WoO)	3. Attacker Capability (AC)
		
How exposed is the interface?	**How much time does an attacker have?**	**What skills do the attacker need for an attack??**
EL0 = 0	Very limited= 0.6 x	Comprehensive knowledge = 1
EL1 = 2	Moderately limited= 0.8 x	Basic knowledge = 2
EL2 = 5	Limited = 0.9 x	Moderate knowledge = 3
EL3 = 16	Unlimited = 1.0 x	Minimal knowledge = 4
EL4 = 24	Very limited= 0.6 x	Comprehensive knowledge = 1

A.5
Classification of the calculated Attack Potential (AP)

The calculated attack potential is classified into one of five attack resilience categories.

Attack potential assessment	Attack potential	Description	Interpretation
0 – 5	AP0	Very low	Minimal attack potential; highly unlikely that this will happen
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 probability of occurrence
15.1 - 20	AP3	High	Significant attack potential; has a high probability of occurrence
> 20	AP4	Very high	Critical attack potential; an attack is almost guaranteed

A.6
Mapping Attack Capability (AP) to SRSL

The required SRSL is determined by combining attack resilience and injury severity.

List of security measures with an indication of the severity of the injury		Attack Resilience (AP)				
		AP0	AP1	AP2	AP3	AP4
Injury Severity	S1 low / reversible	SRSL0	SRSL1	SRSL1	SRSL2	SRSL3
	S2 high / non-reversible	SRSL0	SRSL1	SRSL2	SRSL3	SRSL3

A.7
What each SRSL level requires

Each SRSL level requires a defined set of technical and organizational security measures.

	SRSL 1	SRSL 2	SRSL 3
Authentication	Entities must be authenti-cated.	Entities must be authenti-cated.	Entities must be uniquely authenticated.
Authorization	Basic access control based on roles.	Access con-trol based on roles and per-missions.	Granular access control based on roles, permissions, and context.
Software and Infor-mation Integrity	Will be checked at startup (e.g. check-sums).	Checked at startup and at regular inter-vals.	Cryptographically verified at launch and at regular inter-vals.
Boot integrity	Checking the boot process (e.g. Meas-ured Boot).	Checking the boot process (e.g. Meas-ured Boot).	The boot process is crypto-graphically verified (e.g. Secure Boot).
Integrity of infor-mation exchange	Checksums for integrity.	Crypto-graphic mechanisms for integrity.	Cryptographic mechanisms for integrity and authenticity.
Validation of input data	Basic valida-tion of the data format.	Data Format and range validation.	Comprehensive validation of data format, range and context.
Physical manipula-tion	none.	Tamper-evi-dent seals or labels.	Tamper-proof enclosures or sensors.
Authenticity of SRESW/SRASW	none.	Verification by crypto-graphic sig-natures dur-ing installa-tion.	Verification by cryptographic signatures during installa-tion.

A.8
Compliance through the IEC 62443 series of standards

This approach enables conformity by mapping the requirements of EN 50742 to specific requirements of the established EN IEC 62443 series of standards.

- EN IEC 62443-3-3:
  System requirements for IT security and security levels
- EN IEC 62443-4-1:
  Lifecycle requirements for safe product development
- EN IEC 62443-4-2:
  Technical safety requirements for components of industrial automation systems

Facilitating compliance with machinery developed under the EN IEC 62443 series of standards.

		Machinery systems must comply with EN IEC 62443-3-3	**Machinery components must comply with EN IEC 62443-4-2**
Basic Requirement	**Security Level (SL)**	**System Requirements (SR)**	**Component Requirements (CR)**
Identification and authentication	SL-C2	SR 1.1	CR 1.1, CR 1.2
Usage control	SL-C2	SR 2.1, SR 2.8, SR 2.9	CR 2.1, CR 2.6, CR 2.8, CR 2.9, CR 2.12, EDR 2.13
System Integrity	SL-C2	SR 3.1, SR 3.4, SR 3.5, SR 3.6	CR 3.1, CR 3.4, CR 3.5, CR 3.6, EDR 3.2, EDR 3.11, EDR 3.14
Data confidentiality	none	none	none
Restricted data flow	SL-C1	SR S.1	SR S.1
Timely response to events	SL-C1	SR 6.1	SR 6.1
Resource availability	SL-C2	SR 7.1, SR 7.2	SR 7.1, SR 7.2

A.9
The immutable record - Logging requirements

EN 50742 requires traceability of changes to safety-related functions[3], software, parameters, configuration data and other assets where such changes could affect the safe operation of the machinery.
Logging therefore becomes an essential element of demonstrating compliance.

What needs to be logged?

- Changes to Security parameters/configurations
- Updates/Changes to SRESW
- (Embedded Software)
- Updates to SRASW
- (Application Software)
- Deleting the log file itself

Storage requirements

- Protocols must be protected against manipulation.
- The log records of each intervention shall be stored at least 5 years

[3] This does not refer to every technical change, but only to changes that could give rise to a hazard or render a safety measure ineffective, for example the deactivation or reconfiguration of protective devices, changes to safety configurations or access rights, or updates to safety-related application software (SRASW) or embedded software (SRESW).

Terminology notes for Annexes B to H

The annexes use the terms **drive manufacturer**, **door manufacturer**, **installer**, **manufacturer of partly completed machinery**, **manufacturer of the final machinery** and **user** in a functional sense. The decisive factor is the role a party assumes in the specific supply and integration chain.

A **drive manufacturer** supplies the drive unit. Depending on the placing on the market, the drive may be supplied either as a final item of machinery or as **partly completed machinery**, in which case the drive manufacturer assumes the role of the **manufacturer of partly completed machinery**.
A **door manufacturer** supplies the door and may also become the **manufacturer of the final machinery** if the door, drive and relevant safety devices are supplied as one assessed system.

An **installer** combines the door, drive and safety devices on site or retrofits an existing manually operated door. Where the installer creates the final assembled and operational door system, the installer may assume the role of the **manufacturer of the final machinery**. The manufacturer of the final machinery is responsible for the final door system, including its risk assessment, conformity assessment and documentation.
The **user** operates the installed door system and should not make safety-relevant changes outside the manufacturer's instructions or without qualified personnel.
One company may assume more than one role.

A **notified body** is a conformity assessment body formally notified under applicable Union legislation to perform specified conformity assessment tasks. An **independent testing body** may carry out voluntary testing or issue standards-based test reports but does not thereby act as a notified body. References to certificates, assessments and testing in Annex E must be understood in accordance with this distinction.

Annex B
Door drive as machinery (B2C / retail sales)

When placing drives on the market (for sale) as

- garage door drives in DIY stores
- online sales to private individuals
- kits to be installed by qualified personnel

the drive manufacturer must assume that the purchaser has no specialist knowledge and yet still receives a safe product.

This has the following implications:

- CE marking as machinery
- EU Declaration of Conformity
- Complete operating instructions
- Risk assessment for the entire scope of use
- Evidence of safe use by the user
- Safety functions must already be an integral part of the product or be clearly specified

Annex C
Door drive as partly completed machinery (B2B)

In this scenario, the drive manufacturer supplies a component intended for integration into a final item of machinery.

For the placing on the market (sale) of drive units as

- supplies to door manufacturers
- supplies to installers
- supplies to specialist firms for integration into a door

the drive manufacturer provides only one component of the subsequent final assembled and operational door system (final machinery).
This has the following consequences:

- Declaration of Incorporation instead of a Declaration of Conformity
- Installation instructions for the installer or manufacturer of the final machinery
- No CE marking under machinery legislation for the drive unit as partly completed machinery
- Risk assessment is limited to the drive unit and the intended interfaces
- Integration conditions must be clearly defined

Annex D:
Supplementary guidance on declarations

D.1 Complete machinery

The Machinery Regulation does not prescribe a specific layout for the EU Declaration of Conformity, but the declaration shall contain the information specified in Annex V, Part A to Regulation (EU) 2023/1230. Where harmonised standards do not cover all applicable requirements, the manufacturer may also refer, where appropriate, to other technical specifications, industry standards or recognised technical rules used for the conformity assessment. Listing such specifications in the declaration does not in itself demonstrate compliance; the corresponding evidence shall be included in the technical documentation.

EU DECLARATION OF CONFORMITY - **EXAMPLE**-

Manufacturer:
GateDrive Europe Ltd.
Endless Av 15
12345 Somewheretown
Europe

Product Identification:
DoorDrive Pro 800
Electromechanical drive for power operated doors
Type GDP-800
Serial number: see rating plate

Applicable Union Legislation:
- Regulation (EU) 2023/1230 on machinery products
- Directive 2014/30/EU (EMC)
- Directive 2014/35/EU (Low Voltage)

Applied harmonised standards:
EN 12453:2017
EN ISO 12100:2010
EN 60335-2-103:2015

Other technical specifications applied:
EN 50742:20XX
Cybersecurity requirements and protective measures

Person authorised to compile the Technical Documentation:
Max Headroom
The Art of Noise Blvd 15
12345 Somewheretown
Europe

Place, Date, Signature
Dr. John Long-Silver
Director Product Compliance

D.2 Partly Completed Machinery (Declaration of Incorporation)

For partly completed machinery, the manufacturer shall issue an EU Declaration of Incorporation containing the information specified in Annex V, Part B to Regulation (EU) 2023/1230. The declaration does not establish conformity of the final machinery and does not permit the partly completed machinery to be put into service independently. The manufacturer of the final machinery remains responsible for integration, the final risk and conformity assessment and the EU Declaration of Conformity. The corresponding supply and integration scenario is described in Annex C of this guideline.

DECLARATION OF INCORPORATION -**EXAMPLE** -

Manufacturer: …

Product: ...

Type / Serial Number: ...

Declaration:
The partly completed machinery described above is intended to be incorporated into a complete machine. The product must not be put into service until the final machine has been declared in conformity with Regulation (EU) 2023/1230.

Applied Standards: ...

Additional Technical Specifications: ...

Person authorised to compile the Technical Documentation: ...

Place, Date
Name and Signature

Annex E:
EC Type Examination (and Third-Party Testing)

E.1 The basics

For most doors and door drives, conformity assessment remains the responsibility of the manufacturer placing the machinery on the market. An EU type examination by a notified body is required only for the product categories and conformity assessment procedures specified in Regulation (EU) 2023/1230.

Where a harmonised standard is correctly applied, the manufacturer may claim a presumption of conformity for the requirements it covers. If no harmonised standard is available, an EU type examination is not automatically required; however, compliance must be demonstrated by other appropriate technical evidence, such as risk assessments, specifications, tests or expert reports.

In practice, the term 'type examination' may refer to three different forms of evidence:

(1) a formal EU or EC type-examination certificate issued by a notified body under machinery legislation;
(2) a voluntary type-examination by an independent testing body, e.g. TÜV; or
(3) a test report or certificate confirming compliance with individual standards, such as EN 12453 or EN 16005.

Only the first form (1) is a legally regulated conformity assessment procedure. Voluntary third-party testing (2) can support the technical documentation and market acceptance, but it does not replace the manufacturer's responsibility or automatically have the legal effect of an EU type-examination certificate.

! A valid EC type-examination certificate issued under Directive 2006/42/EC remains valid until its expiry. For machinery placed on the market from 20 January 2027, however, it may be used as supporting evidence only for the requirements and product characteristics covered by the original assessment. The manufacturer must assess and document compliance with all applicable requirements of Regulation (EU) 2023/1230. Where the applicable conformity assessment procedure requires the involvement of a notified body, or where the scope of a formal certificate needs to be extended, a supplementary assessment or a new EU type examination may be necessary

E.2 Existing type-examination certificates and the transition to the Machinery Regulation

EC type-examination certificates issued under Directive 2006/42/EC remain valid until their expiry. However, their continued validity only applies to the scope of the original assessment and does not automatically demonstrate compliance with requirements newly introduced or substantially amended by Regulation (EU) 2023/1230.

For machinery placed on the market from 20 January 2027, the manufacturer responsible for its placing on the market must assess it against the applicable requirements of the Machinery Regulation. Existing certificates, test reports and assessments may continue to be used as supporting evidence for the aspects they cover.
Where existing product standards have not yet been harmonised under the Machinery Regulation or do not fully cover new requirements, the manufacturer should perform and document a gap assessment. Additional technical specifications, such as EN 50742 for

safety-related protection against corruption, may be used to address identified gaps, even where they do not yet provide a presumption of conformity.

Manufacturers should contact the body that issued the existing certificate or test report at an early stage. For a formal EC type-examination certificate (1), this should be the relevant notified body; for a voluntary assessment (2) or standards-based test report (3), it should be the responsible testing body. The parties should determine whether the existing assessment can be supplemented by a delta assessment or whether a new EU type examination or additional testing is required. An existing certificate should not be regarded as automatically covering cybersecurity, software integrity or other requirements that were not part of the original assessment.

E.3 Checklist

What happens during the standardisation gap?

The absence of harmonised versions of EN 12453, EN 16005 and EN 50742 under the Machinery Regulation does not prevent conformity assessment.
During the transitional phase, the current editions of EN 12453 and EN 16005 may be cited in the Official Journal with restrictions. In that case, the presumption of conformity would apply only to the essential health and safety requirements actually covered by the respective standard and not to new or amended requirements of the Machinery Regulation that are not yet addressed. The ongoing revisions of EN 12453 and EN 16005 are intended to close these gaps and enable broader harmonisation under the Machinery Regulation.
EN 50742 is in a different position because it has been developed as a new standard specifically to address safety-related protection against corruption and is intended to

support the requirements of the Machinery Regulation. Manufacturers must provide other appropriate technical evidence for any applicable requirements not covered by the cited standards and therefore not benefiting from a presumption of conformity.

For the transitional phase, manufacturers should follow this practical approach:

1. Evaluate existing certificates and test reports: Which requirements and product characteristics are actually covered?
2. Carry out a gap analysis against the Machinery Regulation, in particular regarding the new requirements set out in Annex III.
3. Assess any missing aspects: for example, by referring to EN 50742, even though it is not yet a harmonised standard with a presumption of conformity.
4. Document supplementary technical evidence: risk analysis, architecture, protective measures, verification, software and update processes, as well as test reports.
5. Involving a testing body: where possible, as a supplementary or delta assessment, rather than rushing into a full repeat test[4].
6. Align the EU Declaration of Conformity with the Machinery Regulation: the old certificate[5] may only be used as evidence to the extent of the matters actually tested.

[4] Consider involving the body that issued the existing certificate or test report where clarification or supplementary testing would add value. Where the applicable conformity assessment procedure under Regulation (EU) 2023/1230 requires a notified body, that body must be involved in accordance with the Regulation. In other cases, a supplementary or delta assessment by a competent testing body may provide useful supporting evidence without automatically requiring a full repeat test.

[5] An existing EC type-examination certificate or test report may continue to support the technical documentation for the requirements and product characteristics covered by the original assessment, but it does not by itself demonstrate compliance with requirements that were not assessed.

Annex F:
Model checklist – What information must manufacturers provide to their customers as of today?

Important information must be made available at an early stage to the sales, product management and existing customer teams.

Examples as a checklist:

F.1 Documentation
- ☐ Will operating instructions be made available digitally in future?
- ☐ How long will documents be kept available?

F.2 Cybersecurity
Are there any software-based security features?
- ☐ Are software updates provided?
- ☐ What are the implications of unauthorised modifications?

F.3 Roles and Responsibilities
- ☐ Who is the manufacturer of the final assembled and operational door system (final machinery)?
- ☐ Who carries out the final conformity assessment?
- ☐ What information does the door manufacturer require from the drive manufacturer

F.4 Product and integration information
- ☐ What is the intended use and scope of the supplied product?
- ☐ Is the product supplied as complete machinery or as partly completed machinery?
- ☐ Which installation, integration and interface conditions must the customer observe?
- ☐ Which safety devices, compatible components or additional measures are required for the final application?

F.5 Existing products
- ☐ Will existing products still be available unchanged after 2027?
- ☐ Are technical modifications required?
- ☐ Does existing technical documentation need to be adapted to meet the requirements of the Machinery Regulation?

F.6 Software as a safety component
Many modern door drives include software-controlled functions such as obstacle detection, force monitoring, electronic limit switches, wireless controls, cloud connectivity or app control. The decisive question is whether such functions, interfaces or subsequent software changes can affect machinery safety. The following questions may be used as a starting point:
- ☐ Are there any safety-related software functions?
- ☐ Can software updates affect safety functions?
- ☐ Are safeguards in place against unauthorised modifications?

☐ Has the risk assessment been extended to include software and cyber risks?

Annex G
FAQs - Information for customers and business partners

G.1 Does the new Machinery Regulation apply to our products?
Yes. The new Machinery Regulation (EU) 2023/1230 replaces the previous Machinery Directive and comes into force on 20 January 2027. It also applies to door drives and their placing on the European market.

G.2 Will the classification of our drives change?
The classification continues to depend on the specific application.
- When sold to users, a door drive may – depending on its design and intended use – be supplied as a final item of machinery.
- When sold to door manufacturers or installers, the same drive may be supplied as partly completed machinery.

The respective documentation and verification requirements differ accordingly.

G.3 Are the CE requirements changing?
The essential requirements remain unchanged. However, the new Regulation expands certain requirements, in particular regarding:
- the digitisation of documentation,
- software-based safety functions,
- protection against tampering,
- record-keeping and technical documentation.

G.4 Will user manuals only be made available digitally in future?
The new regulation allows for the digital provision of user manuals. The specific implementation may vary depending on the product and customer group. However, customers may still request a paper copy.

G.5 How important are software and updates?
Security-related software will become increasingly important in the future. Manufacturers must be able to demonstrate that security functions continue to meet the necessary security requirements even when software changes are made.

G.6 Is there anything users or installers need to bear in mind?
Yes. In the case of partly completed machinery in particular, the manufacturer of the final machinery remains responsible for the integration, risk assessment and conformity assessment of the finished machinery.

G.7 What do we need to do now?
We need to systematically review our products, technical documentation and conformity assessment processes against the requirements of the new Machinery Regulation, identify any gaps and implement the necessary measures in good time before 20 January 2027.

G.8 What is the significance of cybersecurity and protection against tampering?
The new Machinery Regulation takes greater account than before of risks that may arise from software, networking or unauthorised interference with control systems (often summarised under the term ‘cybersecurity’). Manufacturers must assess whether tampering

or modifications to safety-related functions could compromise the safety of the machinery and, where necessary, provide for appropriate protective measures.
For door drives, this may be relevant, for example, in the case of:

- wireless and remote controls,
- app or cloud connections,
- parameterisation of safety-related functions,
- software updates,
- remote maintenance access.

G.9 Does cybersecurity only apply to connected products?

No. Even non-connected products can be affected if security-related settings, parameters or software functions can be altered without authorisation.
For door drives, for example, the following aspects may be relevant:

- Altering force limits
- Altering end positions
- Deactivating safety devices
- Replacing or tampering with firmware
- Access to service or parameterisation levels

Annex H

A quick self-assessment for manufacturers

This self-assessment provides a quick first indication of roles, responsibilities and possible safety-related cybersecurity relevance. It is not exhaustive and does not replace the product-specific risk assessment and conformity assessment required under Regulation (EU) 2023/1230.

H.1 - Roles and responsibilities check

Do you purchase our drives for integration into your own door systems?

☐ Yes → Please continue to observe your obligations as the manufacturer of the final machinery.

Do you sell our products directly to users?

☐ Yes → Please contact us if you require information on future documentation and labelling requirements.

Do you use safety-related software functions or remote access?

☐ Yes → We recommend early consultation regarding the new requirements of the Machinery Regulation.

H.2 - Cybersecurity Check

Key question: “Can anyone disable or compromise a safety function by altering parameters, software or communication interfaces?”

Do one or more of the following statements apply?

☐ yes	☐ no	The drive is equipped with a wireless control system.
☐ yes	☐ no	The drive can be operated via an app, a network or the internet.
☐ yes	☐ no	Safety-related parameters can be changed electronically.
☐ yes	☐ no	Software or firmware updates are possible.
☐ yes	☐ no	Remote maintenance or remote access is provided for.
☐ yes	☐ no	Safety devices are software-based.
☐ yes	☐ no	Safety-related parameters can be changed without special access authorisation.
☐ yes	☐ no	Service or maintenance access points are available.

If one or more of the above statements apply, the manufacturer shall assess and document whether the relevant function, interface or possible modification can affect machinery safety. Where a safety impact is possible, the affected safety-related assets, interfaces and foreseeable changes shall be identified, appropriate protective measures shall be selected, and the corresponding verification evidence shall be included in the technical documentation. The result should also identify who is responsible for implementing, maintaining and updating each measure within the supply and integration chain.

If all statements are answered with ‘no’, this does not automatically mean that safety-related cybersecurity is irrelevant. The manufacturer should verify that no other electronic, physical or organisational means exist by which safety-related software, parameters, configurations, data or functions could be changed without authorisation.

H.3 - Lifecycle and change management check

☐ Lifecycle and change management check: Are responsibilities defined for approving, installing, verifying and documenting software updates, parameter changes and configuration changes throughout the expected lifetime of the machinery?

☐ Are safety-relevant changes traceable and are users informed about permitted changes, required qualifications and foreseeable consequences?

Text / Editorial team:

Status: September 2026

E.D.S.F.
European Door and Shutter Federation e.V.
Neumarktstr. 2 b
58095 Hagen · Deutschland

Fon +49 2331 2008-0
Fax +49 2331 2008-40
info@edsf.com
www.edsf.com