CAPIEL

european coordinating committee of manufacturers
of electrical switchgear and controlgear

WHITE PAPER

# Overview and comparison between EN ISO 13849-1 and EN IEC 62061

Edition 1

July, 2024

# CAPIEL
# WHITE PAPER

The target audience for this comparison are manufacturers and users of CAPIEL products, and it is assumed that the reader is already familiar with the concept of functional safety as it relates to both the Machinery Directive (2006/42/EC) and the new Machinery Regulation (EU) 2023/1230.

NOTE

The new Machinery Regulation (EU) 2023/1230 will apply from 20 January 2027 and will replace the current Machinery Directive (2006/42/EC).

# Table of contents

# 1. Introduction

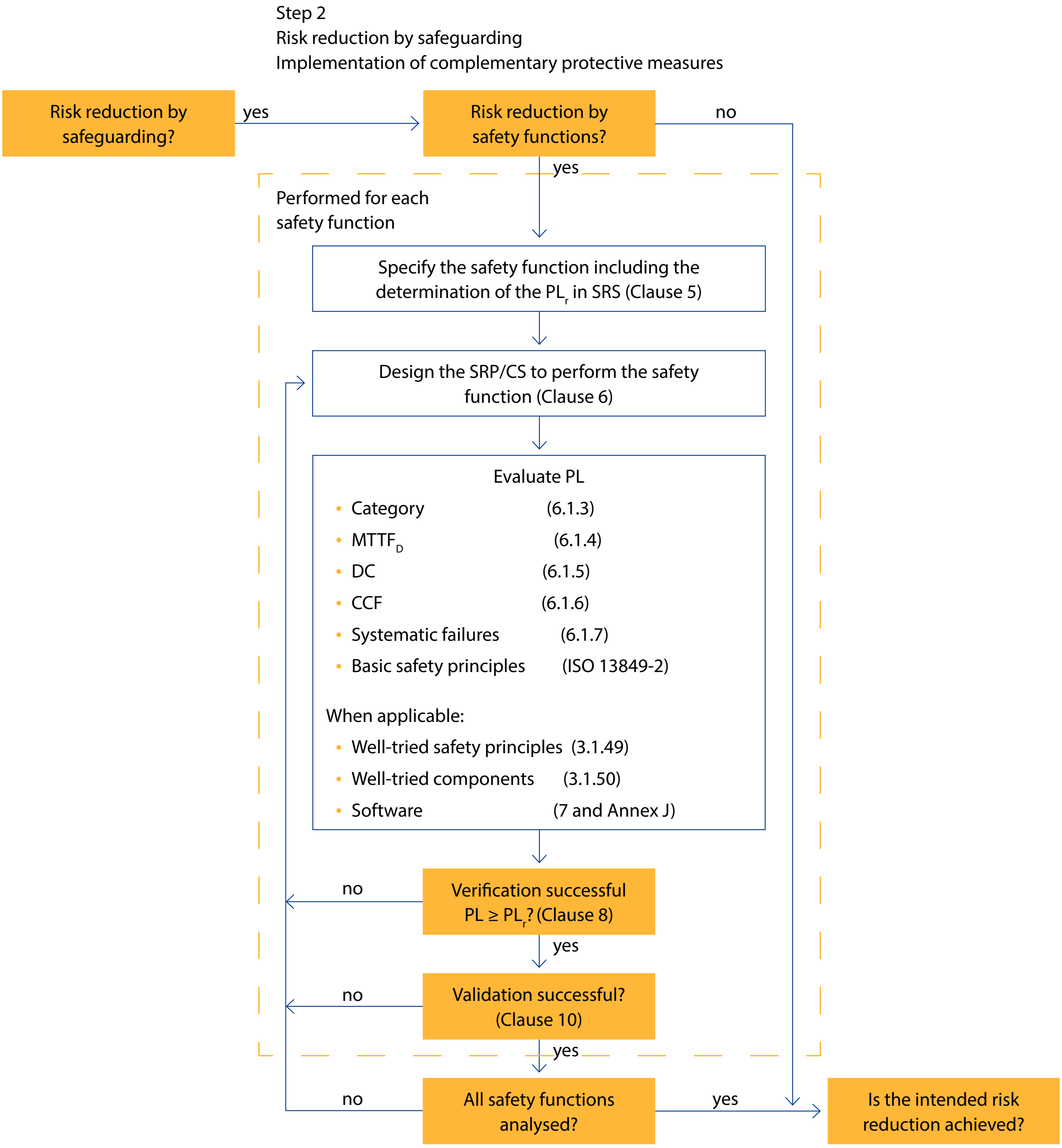
The new editions of EN ISO 13849-1:2023 and EN IEC 62061:2021 have similar scopes and content, and they both aim to achieve the same risk reduction.  However, they use different methodologies for the design of safety related control systems.

The existence of these two functional safety standards can cause confusion amongst users – especially when certain machinery standards (C-type standards) offer the possibility to use either of the standards. With the main focus on manufacturers and users of CAPIEL products, the purpose of this document is therefore to explain the similarities and differences between EN ISO 13849-1 and EN IEC 62061 to explore if a future merger of the two standards now is possible.

# 2. What is new?

## 2.1 Overview, EN ISO 13849-1:2023, Ed 4

EN ISO 13849-1 underwent a complete technical revision, and the new edition guides the designer through a logical iterative process for the design of a safety-related control system, as outlined in the figure below.


Step 2
Risk reduction by safeguarding
Implementation of complementary protective measures
Risk reduction by safeguarding?
yes
Risk reduction by safety functions?
no
yes
Performed for each safety function
Specify the safety function including the determination of the $PL_r$ in SRS (Clause 5)
Design the SRP/CS to perform the safety function (Clause 6)
Evaluate PL
Category (6.1.3)
$MTTF_D$ (6.1.4)
DC (6.1.5)
CCF (6.1.6)
Systematic failures (6.1.7)
Basic safety principles (ISO 13849-2)
When applicable:
Well-tried safety principles (3.1.49)
Well-tried components (3.1.50)
Software (7 and Annex J)
no
Verification successful $PL \geq PL_r$? (Clause 8)
yes
no
Validation successful? (Clause 10)
yes
no
All safety functions analysed?
yes
Is the intended risk reduction achieved?

Iterative process for design of safety-related parts of control systems (SRP/CS)
(Source: EN ISO 138491-1, Figure 1)

The revision provided improvements and clarification on the following clauses:

- Specification of safety functions

Clause 5 has been completely revised. It now provides detailed guidance on how to specify the requirements of an SRP/CS and focuses on the development of a safety requirement specification (SRS) as the basis for all SRP/CS design activities.

Clause 6.3 gives requirements on safety related parameterization.

Clause 7 now clearly focuses on the development of both embedded and application software to ensure that it is readable, understandable, testable and maintainable. The new edition also has the following additional improvements.

- Annex G.5 – Management of functional safety
- Annex J, which gives more detailed recommendations for lifecycle activities.
- Annex L – EMC immunity
- Annex M – safety requirements specification (SRS)
- Annex N, gives an overview of measures related to systematic aspects which applies to software design.
- Annex O – safety-related values

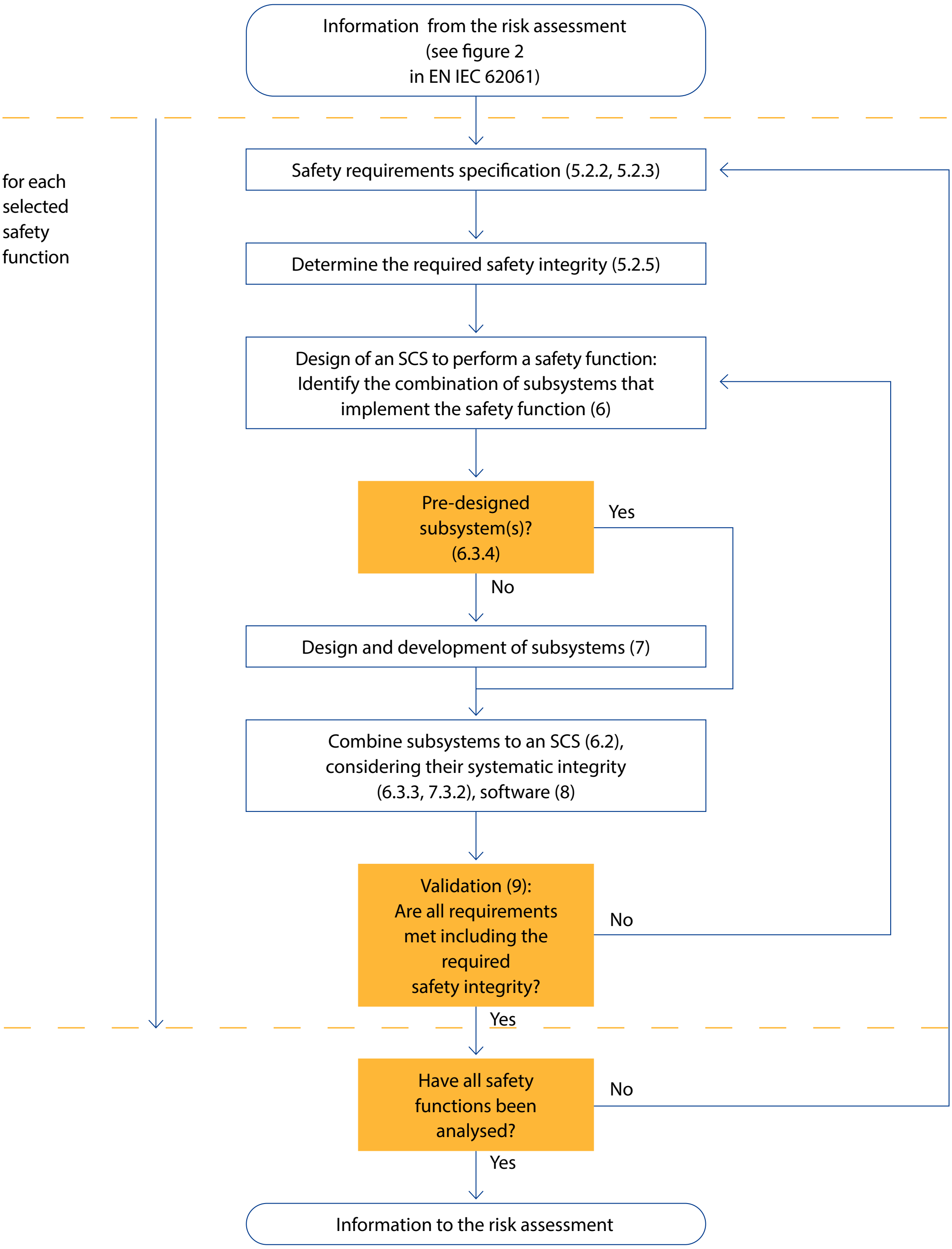
- Validation

Clause 10 now incorporates the normative requirements from EN ISO 13849-2:2012 in their entirety.

It should be noted that the new EU Machinery Regulation (2023/1230) introduces cyber security requirements via the new clause 1.1.9 (Protection against corruption) and added content to 1.2.1 (Safety and reliability of control system). EN ISO 13849-1: 2023 does not provide specific measures for cyber security.

## 2.2 Overview, EN IEC 62061:2021, Ed 2

Similarly, EN IEC 62061 underwent a significant technical revision, and now has a revised structure that reflects the ISO 12100 process more accurately when designing a safety function.


Information from the risk assessment
(see figure 2
in EN IEC 62061)
for each
selected
safety
function
Safety requirements specification (5.2.2, 5.2.3)
Determine the required safety integrity (5.2.5)
Design of an SCS to perform a safety function:
Identify the combination of subsystems that
implement the safety function (6)
Pre-designed
subsystem(s)?
(6.3.4)
Yes
No
Design and development of subsystems (7)
Combine subsystems to an SCS (6.2),
considering their systematic integrity
(6.3.3, 7.3.2), software (8)
Validation (9):
Are all requirements
met including the
required
safety integrity?
No
Yes
Have all safety
functions been
analysed?
No
Yes
Information to the risk assessment

The revision provided the following improvements and clarifications:

- Standard extended to non-electrical technologies
- Definitions updated to be aligned with IEC 61508-4, Ed 2
- Functional safety plan introduced, and configuration management updated (Clause 4). To stress the importance of Functional Safety Management, this aspect has been added, fully in line with IEC 61508. At the same time, the differences between configuration management and change management have been clarified.
- Requirements on parameterization expanded (Subclause 6.7)
  This important use case has been significantly extended, starting with a description, followed by determining the effect of failures, deriving requirements, and closing with verification.
- Requirements on periodic testing added (Subclause 6.9)
  This subclause explains the different purposes of periodic testing and sets out requirements for them.
- Various improvements and clarification on architectures and reliability calculations (Clause 6 and Clause 7)
  Based on field feedback on the previous editions, example architectures have been defined more clearly along with more background and details on associated reliability calculations. Focus has been put on the architectural relationship of safety function diagnostics and fault reaction.
- "SILCL" replaced with "maximum SIL" of a subsystem,
- Use cases for software described including requirements added (Clause 8). Three levels of application software are defined (using LVL or FVL). When running on a safe platform (comprising both hardware and software), the standard sets out requirements for both LVL (level 1) and FVL (level 2). FVL is limited to SIL 2, while LVL can be used up to SIL 3. The requirements are fully consistent with those defined in IEC 61508, but adapted to the machinery domain. V models, tailored to this use case, are provided. The benefit for users is that they do not have to apply another standard (e.g. IEC 61508), so EN IEC 62061 is a one stop approach. For completeness, level 3 is defined as application software developed according to IEC 61508 (up to SIL 3).
- Guidance about independence for software verification and validation activities (Annex J) have been added. These are based on IEC 61508, tailored to the machinery domain and address common misunderstandings. Note, that this annex is informative.

# 3. What is common?

## 3.1 Scope of the standards

The previous edition of EN IEC 62061 covered only electric, electronic and programmable systems, whereas the new edition also covers other technologies, e.g., hydraulic, pneumatic and mechanical systems (as does EN ISO 13849-1). NOTE: These standards are explicitly covering high demand mode. In addition, the relevant aspects of low demand mode from IEC 61508-1 are addressed by the systematic safety measures.

Scope from EN ISO 13849-1.

“1 Scope

This document specifies a methodology and provides related recommendations and requirements for the design and integration of safety-related parts of control systems (SRP/CS), including the design of software. This document specifies a methodology and provides related guidance for the design and integration of safety-related parts of control systems (SRP/CS) that perform safety functions, including the design of software. This document applies to SRP/CS for high demand and continuous mode including their subsystems, regardless of the type of technology and energy (e.g. electrical, hydraulic, pneumatic, and mechanical). This document does not apply to low demand mode.”

Scope from EN IEC 62061

“1 Scope

This International Standard specifies requirements and makes recommendations for the design, integration and validation of safety-related control systems (SCS) for machines. It is applicable to control systems used, either singly or in combination, to carry out safety functions on machines that are not portable by hand while working, including a group of machines working together in a coordinated manner.”

## 3.2 Terms and definitions

The two standards use similar but not always identical wording, e.g. the definition of a subsystem was previously only present in EN IEC 62061 but is now present in both standards.

Some examples:

| EN IEC 62061:2021 | EN ISO 13849-1:2023 |
|---|---|
| 3.2.15<br>risk<br>combination of the probability of occurrence of harm and the severity of that harm | 3.1.19<br>risk<br>combination of the probability of occurrence of harm (3.1.16) and the severity of that harm |
| 3.2.3<br>safety-related control system<br>SCS<br>part of the control system of a machine which implements a safety function by one or more subsystems | 3.1.1<br>safety–related part of a control system<br>SRP/CS<br>part of a control system that performs a safety function, starting from a safety-related input(s) to generating a safety-related output(s) |
| 3.2.4<br>subsystem<br>entity of the top-level architectural design of a safety-related system where a dangerous failure of the subsystem results in dangerous failure of a safety function | 3.1.46<br>subsystem<br>entity which results from a first-level decomposition of an SRP/CS and whose dangerous failure results in a dangerous failure of a safety function |
| 3.2.24<br>safety integrity level<br>SIL<br>discrete level (one out of a possible three) for describing the capability to perform a safety function where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest | 3.1.5<br>performance level<br>PL<br>discrete level used to specify the ability of safety-related parts of control systems to perform a safety function under foreseeable conditions |

## 3.3 Structure with respect to the design process

For the ease of use of the standards, both have been changed to reflect the design process of the safety function. This is stated in the forewords:

EN IEC 62061

“This edition includes the following significant technical changes with respect to the previous edition:

- structure has been changed and contents have been updated to reflect the design process of the safety function,”

EN ISO 13849-1

“The main changes are as follows:

- the whole document was reorganized to better follow the design and development process for control systems;”

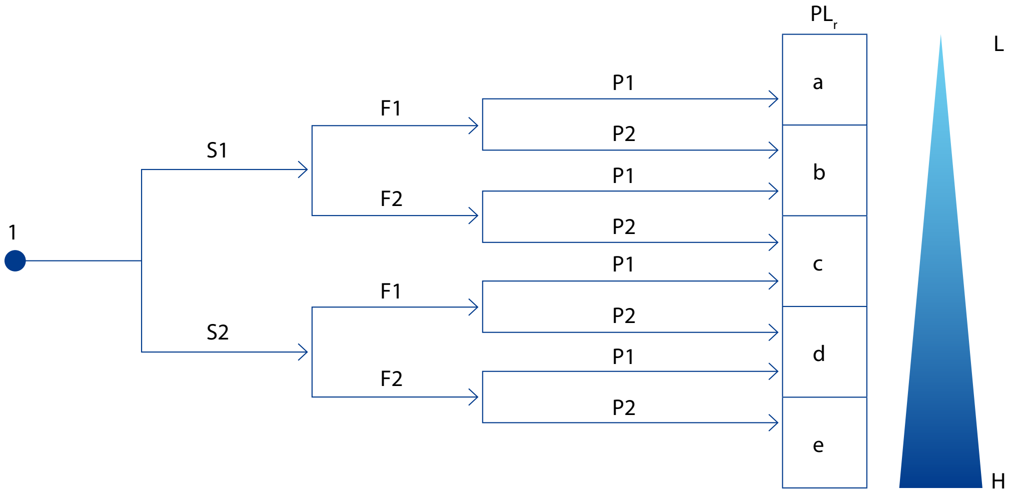
## 3.4 Determination of required safety integrity, SIL, versus Guidance for the determination of required performance level ($PL_r$)

The table A.6 in EN IEC 62061 for the determination of SIL, now also shows the corresponding PL's. In a similar way Table 4 in EN ISO 13849-1 shows the correspondence between PL and SIL.

Table 4 – Correlation between performance level (PL) and safety integrity level (SIL)

| PL | SIL<br>(see IEC 62061:2021 for information) high/continuous operating mode |
|---|---|
| a | no correlation |
| b | 1 |
| c | 1 |
| d | 2 |
| e | 3 |
| NOTE 1 PL a has no correlation on the SIL scale and is mainly used to reduce the risk of slight, normally reversible, injury. | |
| NOTE 2 PL e corresponds to SIL 3 which is defined as the highest level typically used for machinery | |

Both standards use the parameters Severity, Frequency, Possibility of Occurrence and Possibility of Avoidance to determine SIL and $PL_r$ respectively.



Source: Figure A.1 from EN ISO 13849-1

| Consequences | Severity Se | Class Cl = Fr + Pr + Av | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| Death, losing an eye or arm | 4 | SIL 1 | | SIL 2 | | | SIL 2 | | | SIL 3 | | | SIL 3 | |
| | | PL$_r$ b | PL$_r$ c | PL$_r$ d | | | PL$_r$ d | | | PL$_r$ e | | | PL$_r$ e | |
| Permanent injury,losing fingers | 3 | No SIL (or PL) required | | OM | | | SIL 1 | | | SIL 2 | | | SIL 3 | |
| | | | | PL$_r$ a | | | PL$_r$ b | PL$_r$ c | | PL$_r$ d | | | PL$_r$ e | |
| Reversible injury,medical attention | 2 | | | | | | OM | | | SIL 1 | | | SIL 2 | |
| | | | | | | | PL$_r$ a | | | PL$_r$ b | PL$_r$ c | | PL$_r$ d | |
| Reversible injury, first aid | 1 | | | | | | | | | OM | | | SIL 1 | |
| | | | | | | | | | | PL$_r$ a | | | PL$_r$ b | PL$_r$ c |

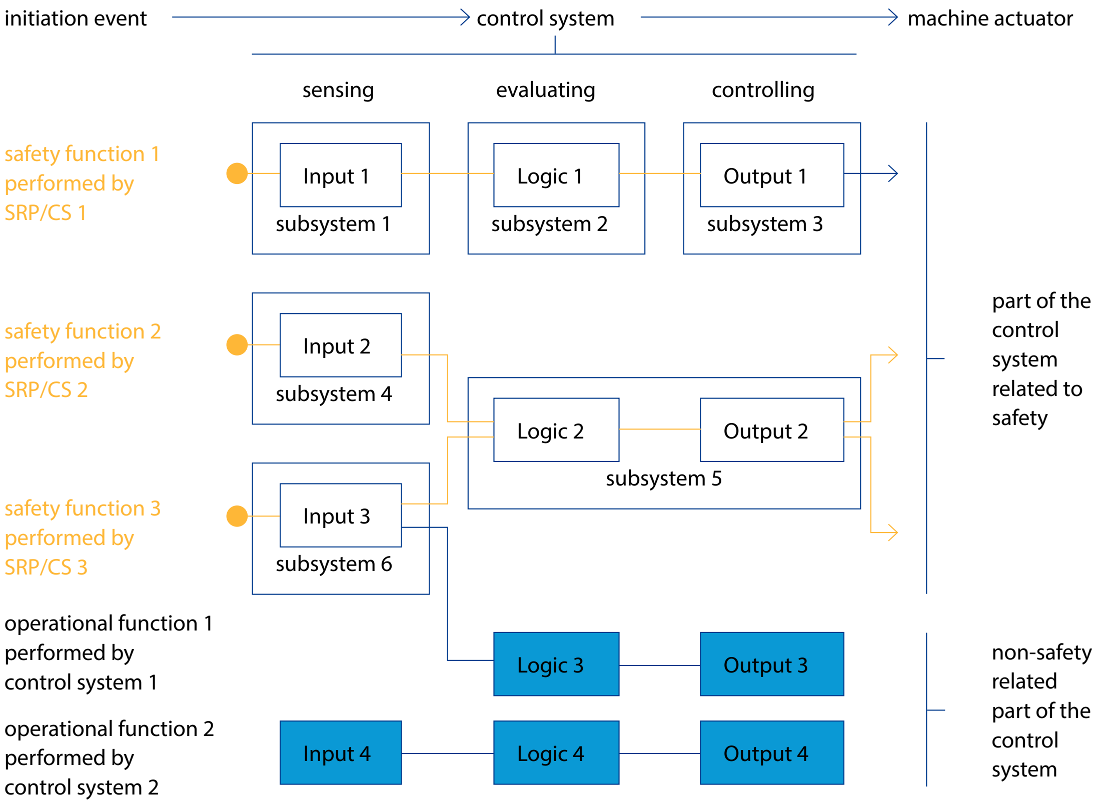
Source: Table A.6 from EN IEC 62061

## 3.5 Decomposition of a safety function

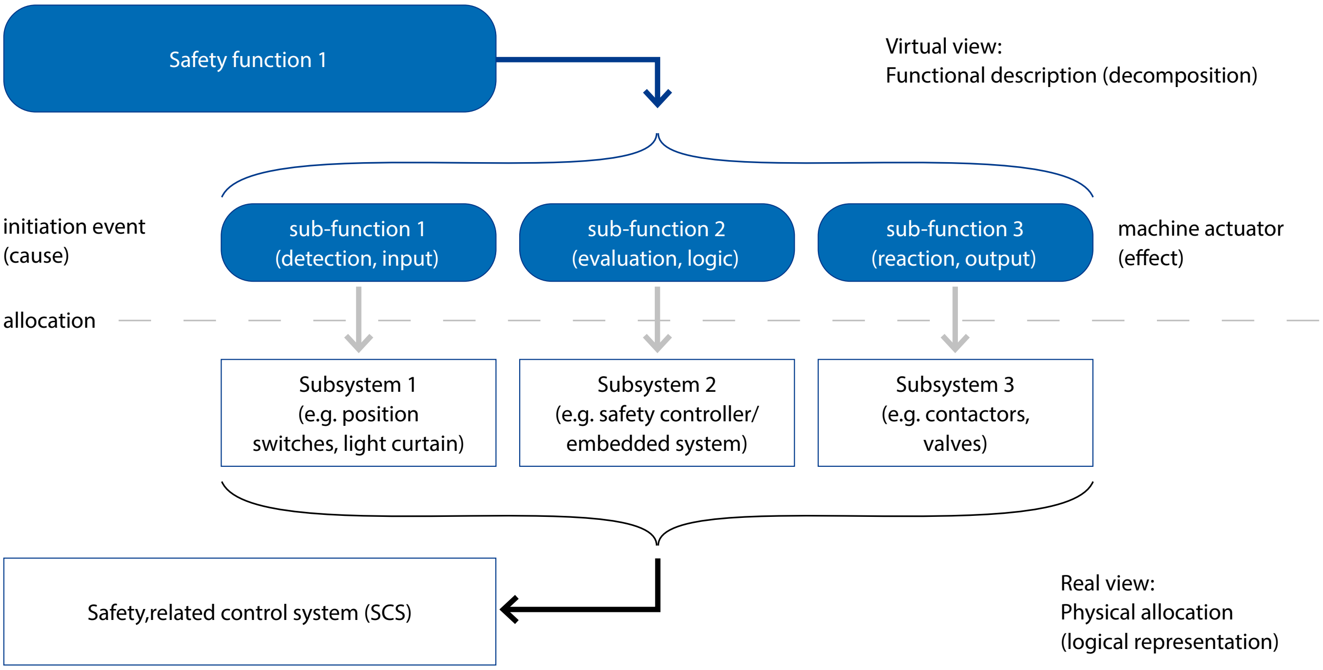
Both standards describe how the safety function/SCS is decomposed in subfunctions/ subsystems.

Figures below show the decomposition of the safety functions and supports a common understanding between the two standards.

From EN ISO 13849-1


initiation event
control system
machine actuator
sensing
evaluating
controlling
safety function 1 performed by SRP/CS 1
Input 1
subsystem 1
Logic 1
subsystem 2
Output 1
subsystem 3
safety function 2 performed by SRP/CS 2
Input 2
subsystem 4
Logic 2
Output 2
subsystem 5
safety function 3 performed by SRP/CS 3
Input 3
subsystem 6
part of the control system related to safety
operational function 1 performed by control system 1
Logic 3
Output 3
operational function 2 performed by control system 2
Input 4
Logic 4
Output 4
non-safety related part of the control system

From EN IEC 62061



## 3.6 Cybersecurity

Cyber security is currently excluded from the scopes of both standards.

NOTE: It is expected that the standards will be updated to include cyber security in order to address the requirements in the new Machinery Regulation.

## 3.7 Specification of safety function/safety system

An important part of the design of safety functions is the SRS – Safety Requirements Specification. The requirements are now described in an equal manner in both editions.

From EN ISO 13849-1

“5.2 Safety requirements specification

5.2.1 General requirements

5.2.1.1 General

The SRS is the basis for all SRP/CS design activities and shall document details of each safety function to be performed.

The SRS provides the necessary information at the transition from the risk assessment and risk reduction process according to ISO 12100:2010 to the SRP/CS design and evaluation process according to this document, especially if these two processes are performed by different persons or organizations (see Table 3)."

From EN IEC 62061

"5.2 Safety requirements specification (SRS)

5.2.1 General

Each safety function shall be specified by:

- functional requirements specification (see 5.2.3);
- safety integrity requirements specification (see 5.2.5)

and these shall be documented in the safety requirements specification (SRS)."

4.8 Predesigned subsystems

EN IEC 62061 allows for the use of predesigned subsystems according to EN ISO 13849-1 or IEC 61508. The restriction is that subsystems using complex components designed according to EN ISO 13849-1 can only be used if they also meet the requirements of IEC 61508 or an applicable functional safety product standard.

From EN ISO 13849-1

EN ISO 13849-1 gives the possibility to design a safety function with "previously validated subsystems".

The requirement for the subsystem is as follows:

"If previously validated subsystems according to EN IEC 62061:2021 or the IEC 61508 series (SIL) for high demand or continuous mode that use Route 1H (see IEC 61508-2:2010, 7.4.4.2) are used, the SIL can be correlated to a PL using 6.1.2 and 6.2.2. PFH values calculated according to the IEC 61508 series or IEC 62061:2021 with the above-mentioned limitations can be considered as PFH values according to this document."

From EN IEC 62061

"The safety performance of a pre-designed subsystem, according to other standards, shall be in line with Table 4."

| IEC 62061<br>(IEC 61508) | IEC 62061 | IEC 61508[a] | ISO 13849[b] | IEC 61496 |
|---|---|---|---|---|
| PFH | SIL | at least... | at least... | at least... |
| < $10^{-5}$ | SIL 1 | SIL 1 | PL b, c | Type 2 |
| < $10^{-6}$ | SIL 2 | SIL 2 | PL d | Type 3 |
| < $10^{-7}$ | SIL 3 | SIL 3 | PL e | Type 4 |

NOTE A relation between IEC 62061 and IEC 61511 (all parts) or ISO 26262 cannot be assumed within this table.

[a] This column includes SIL-based standards that fulfil the architectural constraints of IEC 61508, such as IEC 61800-5-2 and IEC 60947-5-3.

[b] Does not apply to subsystems using complex components, unless they meet the requirements of IEC 61508 or applicable functional safety products standards.Performance Level b does not correspond to SIL1 in case of a category B (ISO 13849-1) structure.

Source: Table 4 from EN IEC 62061

# 4. What is different?

## Parameters

The two standards are using similar parameters such as $MTTF_D$ (Mean Time To Dangerous Failure) and DC (Diagnostic Coverage). However, there are also some parameters expressed differently, but leading to similar conclusion, e.g. HFT and two channel structure.

## Complex electronics

For complex electronics EN IEC 62061 refers directly to IEC 61508 or an applicable functional safety product standard, whereas EN ISO 13849-1 does not provide this requirement.

## EMC

EN IEC 62061 (clause 6) requires application of IEC 61000-1-2, also referring to appropriate immunity levels for functional safety stated in IEC 61326-3-1 or IEC 61000-6-7 as a minimum.

EN ISO 13849-1 has no such requirements and instead describes four recommended routes in the informative Annex L.

# 5. CAPIEL position and visions for the future of Functional Safety standards

CAPIEL acknowledges the great work done to align EN IEC 62061 and EN ISO 13849-1 and supports all future efforts to create a common standard for safety control systems of machinery. This would be a great advantage for all stakeholders to have common requirements and implementation methods. Efforts and misinterpretations can be reduced when having a common standard for safety control systems of machinery. The two standards have very similar scope and content and CAPIEL therefore believes that a merged standard is now feasible.

# 6. Standards referred to in this document.

| | |
|---|---|
| EN 61508 | Functional safety of electrical/electronic/programmable electronic safety-related systems |
| EN 62061 | Safety of machinery – Functional safety of safety-related control systems |
| EN ISO 13849-1 | Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design |
| EN ISO 13849-2 | Safety of machinery - Safety-related parts of control systems - Part 2: Validation |

- CAPIEL is the Coordinating Committee for the Associations of Manufacturers of Switchgear and Controlgear equipment for industrial, commercial and similar use in the European Union, that work in the range of voltages until 1 kV a.c. of 1,5 kV d.c.
- The objective of CAPIEL is to promote and to support the common technical, industrial, economical, environmental and political interests of the European low voltage switchgear and controlgear industry (products, systems and assemblies)
- CAPIEL members are national associations representing small, medium and large-sized companies that in total employ more than 100.000 people directly in Europe. Their scope covers all the equipment, product fittings, systems installed and services required for operations of low voltage and control gear (products, systems and assemblies)
- CAPIEL plays an active role in driving emerging technologies and in supporting the values of ethical, environmental, health and safety, innovation for sustainability, quality and fair competition in accordance with the imperatives of the Treaty of Rome

CAPIEL

european coordinating committee of manufacturers
of electrical switchgear and controlgear