Safety of Machinery – Does ISO 13849-1:2023 work for you?

Presented to the Santa Clara Valley Joint Chapter

June 14, 2023

What is “Functional Safety”?

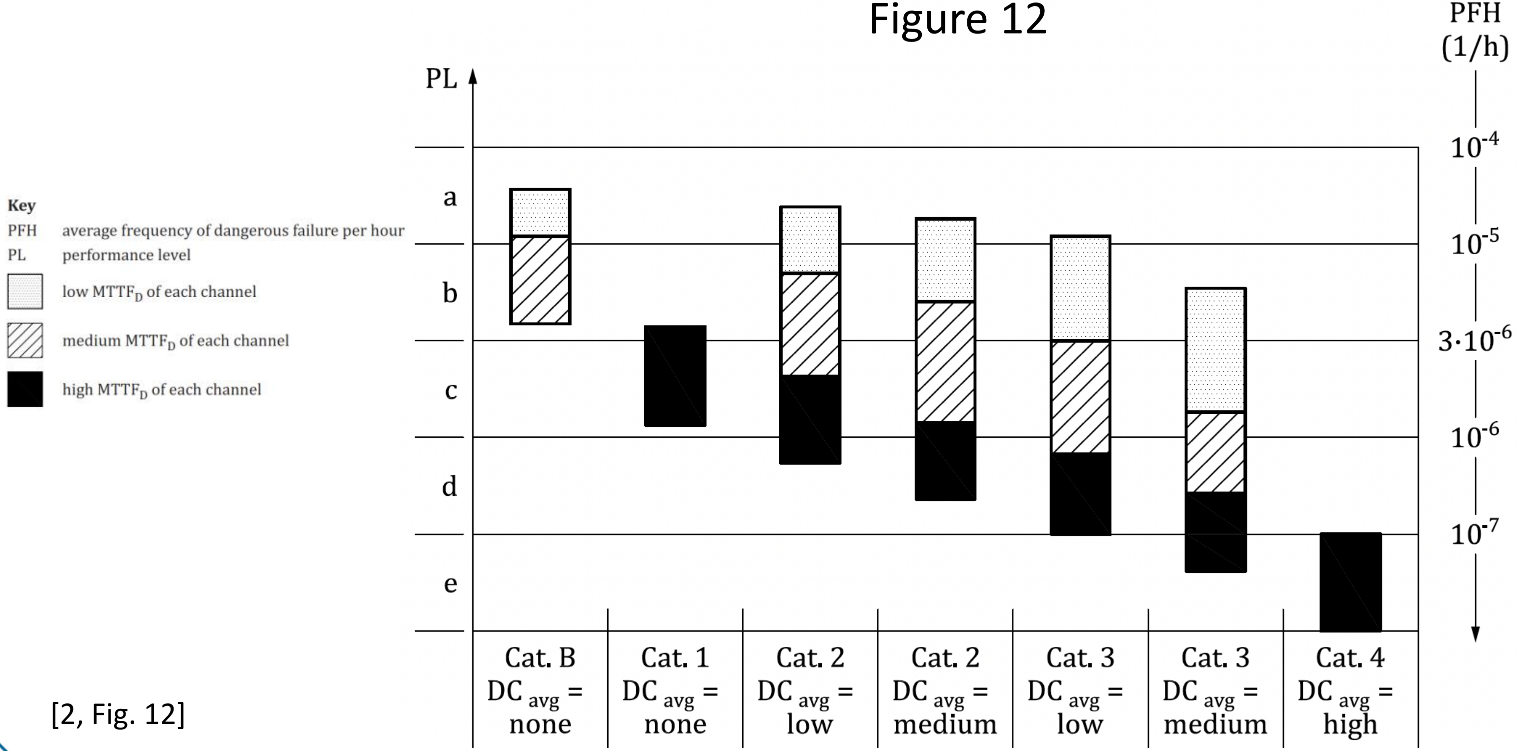
Part of the overall safety relating to the EUC* and **the EUC control system** that **depends on the safety-related systems** and external risk reduction facilities **operating correctly in response to their inputs**.

*EUC: Equipment under control

[1]

Relationship between categories, DC_{avg}, $MTTF_D$ and PL

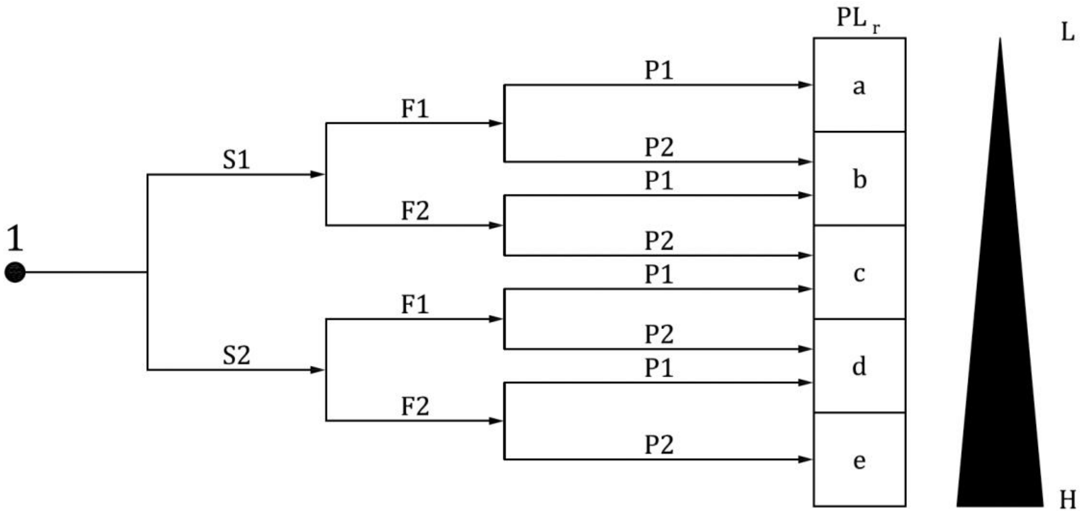
Figure 12



[2, Fig. 12]

Annex A – Guidance for the determination of PL_r*

Figure A.1



*This is NOT a risk assessment method

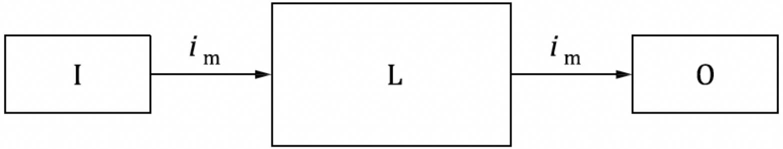
[2]

Three aspects – Architecture, MTTF$_D$, DC

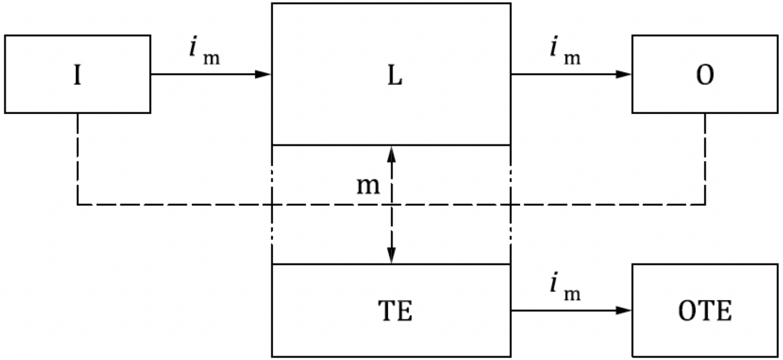
Architecture

Single channel architectures:

- Category B – “Basic”
- Category 1 – Cat. B + “Well-tried components”
- Category 2 – Cat. B + Diagnostic Coverage > 60%



Category B and 1 logical structure



Category 2 logical structure

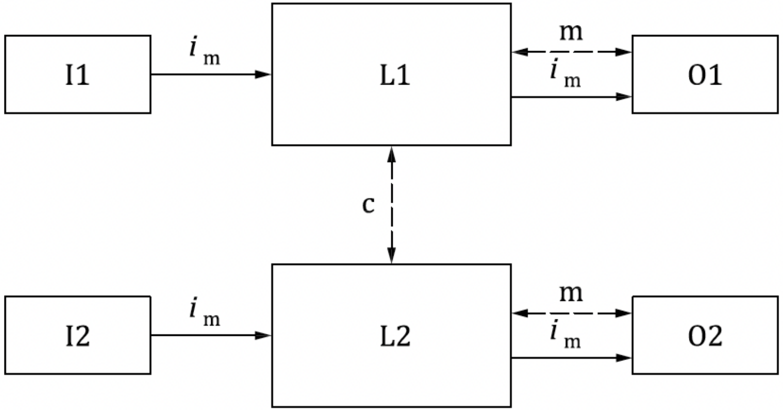
[2]

Three aspects – Architecture, MTTF$_D$, DC

Architecture

Redundant channel architectures:

- Category 3 – Cat. B + Redundant channels + Diagnostics > 60%



Category 3 logical structure

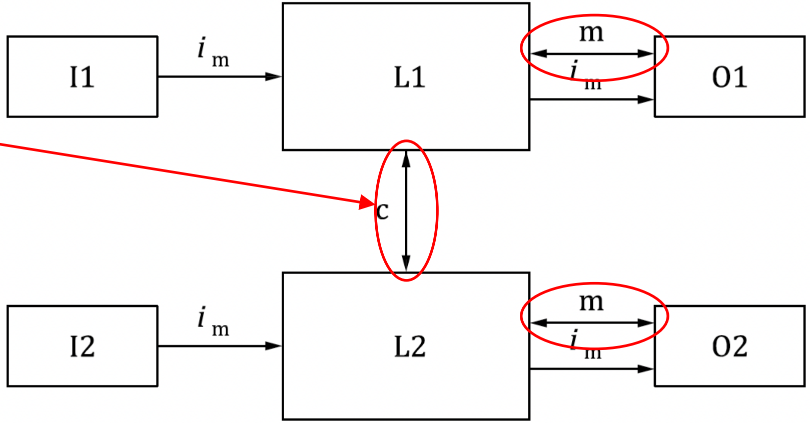
[2]

Three aspects – Architecture, MTTF_D, DC

Architecture

Redundant channel architectures:

- Category 4 – Cat. B + Redundant channels + Diagnostics > 99%



Category 4 logical structure

[2]

Component failure rate

Mean Time to Dangerous Failure (MTTF$_D$)

- Based on the dangerous failure rate of the component (λ_D)
- Given in terms of *years*
- Used to determine the predicted failure rate of each channel in an SRP/CS
- Can be calculated if the lifetime in terms of number of cycles is known (B_{10})

$$MTTF_D = \frac{B_{10D}}{0.1 \times n_{op}}$$

$$n_{op} = \frac{d_{op} \times h_{op} \times 3600\ s/h}{t_{cycle}}$$

Diagnostic Coverage

DC_{avg}

- DC is in relation to the dangerous failures of components in the SRP/CS
- Calculated as (ISO 13849-1:2023 Eq. 1):

$$DC = \frac{\Sigma\lambda_{DD}}{\Sigma\lambda_{Dtotal}}$$

[2 Eq. 1]

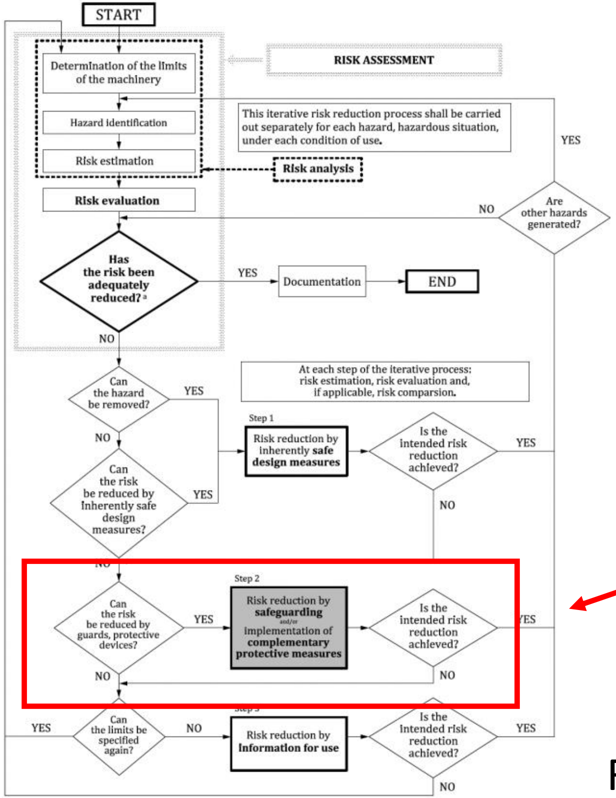
Where
λ_{DD} is the dangerous detectable portion of all failures
$\lambda_{\mathrm{Dtotal}}$ is all of the dangerous failures

Improvements over the 2015 3rd ed.

Improvements in the 4th ed.

- Better flow – document now follows the design and development process better
- new Clause 4 on the relationship to risk assessment
- Improved Clause 5 on specification of the safety functions and combination of several subsystems
- Revised Clause 9 on Ergonomic aspects of design (replaces 4.8 in 3rd ed.)
- ISO 13849-2:2012 normative text moved into ISO 13849-1 Clause 10 and updated.
- New method for determining the “P” parameter in Annex A.
- a new G.5 on management of functional safety;
- a new Annex M with additional information for safety requirements specification;
- a new Annex N on Avoidance of systematic failures in software design
- a new Annex O with safety-related values of components or parts of the control systems.

Risk assessment and reduction process



START

Determination of the limits of the machinery

RISK ASSESSMENT

Hazard identification

This iterative risk reduction process shall be carried out separately for each hazard, hazardous situation, under each condition of use.

Risk estimation

Risk analysis

Risk evaluation

YES

NO

Are other hazards generated?

Has the risk been adequately reduced? [a]

YES

Documentation

END

NO

At each step of the iterative process: risk estimation, risk evaluation and, if applicable, risk comparison.

Can the hazard be removed?

YES

Step 1

NO

Risk reduction by inherently safe design measures

Is the intended risk reduction achieved?

YES

Can the risk be reduced by inherently safe design measures?

YES

NO

NO

Step 2

Can the risk be reduced by guards, protective devices?

YES

Risk reduction by safeguarding and/or implementation of complementary protective measures

Is the intended risk reduction achieved?

YES

NO

NO

Step 3

YES

Can the limits be specified again?

NO

Risk reduction by information for use

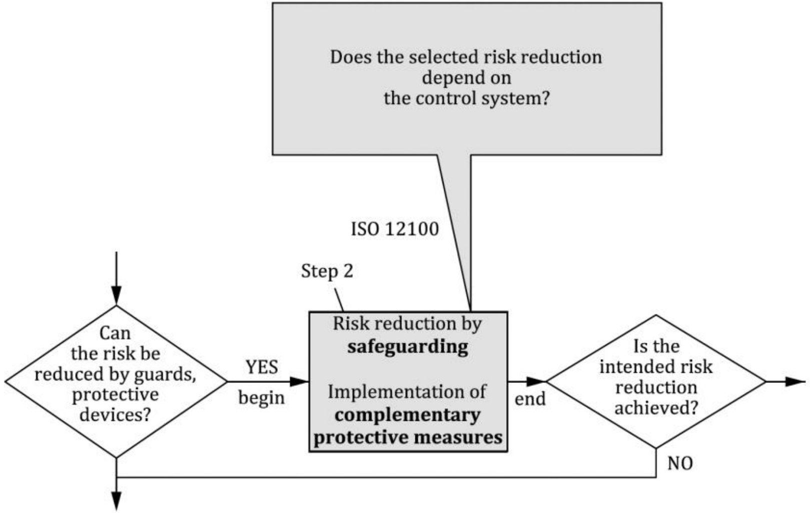
Is the intended risk reduction achieved?

YES

NO

[2]

Figure 2



Does the selected risk reduction depend on the control system?

ISO 12100

Step 2

Can the risk be reduced by guards, protective devices?

YES

begin

Risk reduction by **safeguarding**

Implementation of **complementary protective measures**

end

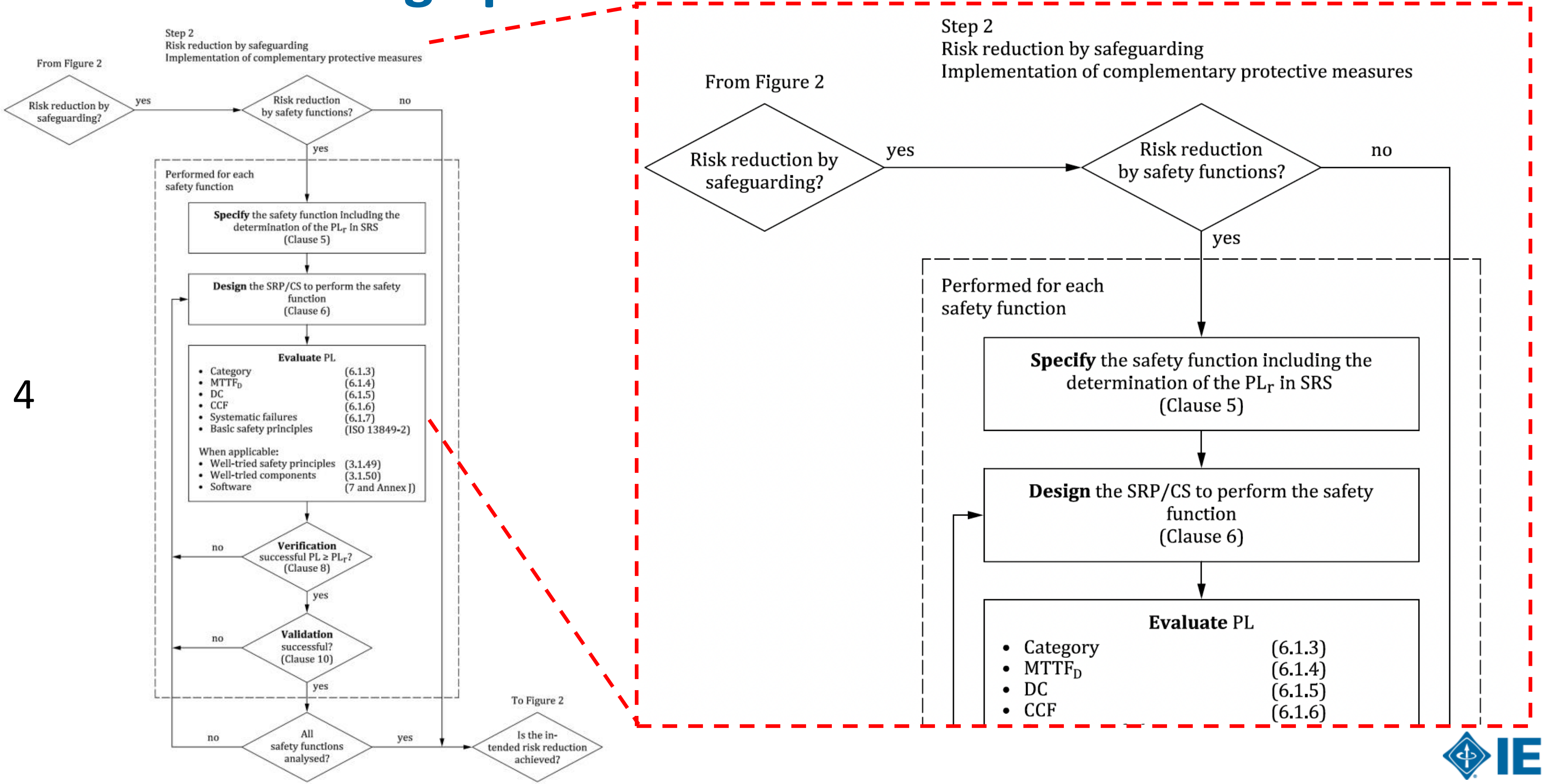
Is the intended risk reduction achieved?

NO

Figure 1

Clause 4 – Design process

Fig. 4



Step 2
Risk reduction by safeguarding
Implementation of complementary protective measures

From Figure 2

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)

Verification successful $PL \geq PL_r$? (Clause 8)

no

yes

Validation successful? (Clause 10)

no

yes

All safety functions analysed?

no

yes

To Figure 2

Is the in-tended risk reduction achieved?

Step 2
Risk reduction by safeguarding
Implementation of complementary protective measures

From Figure 2

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)

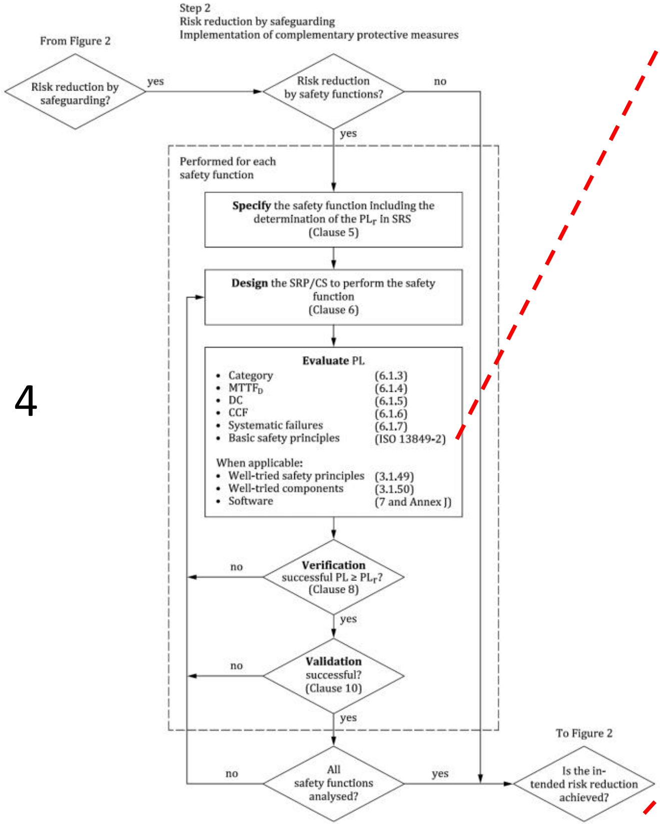
Evaluate PL

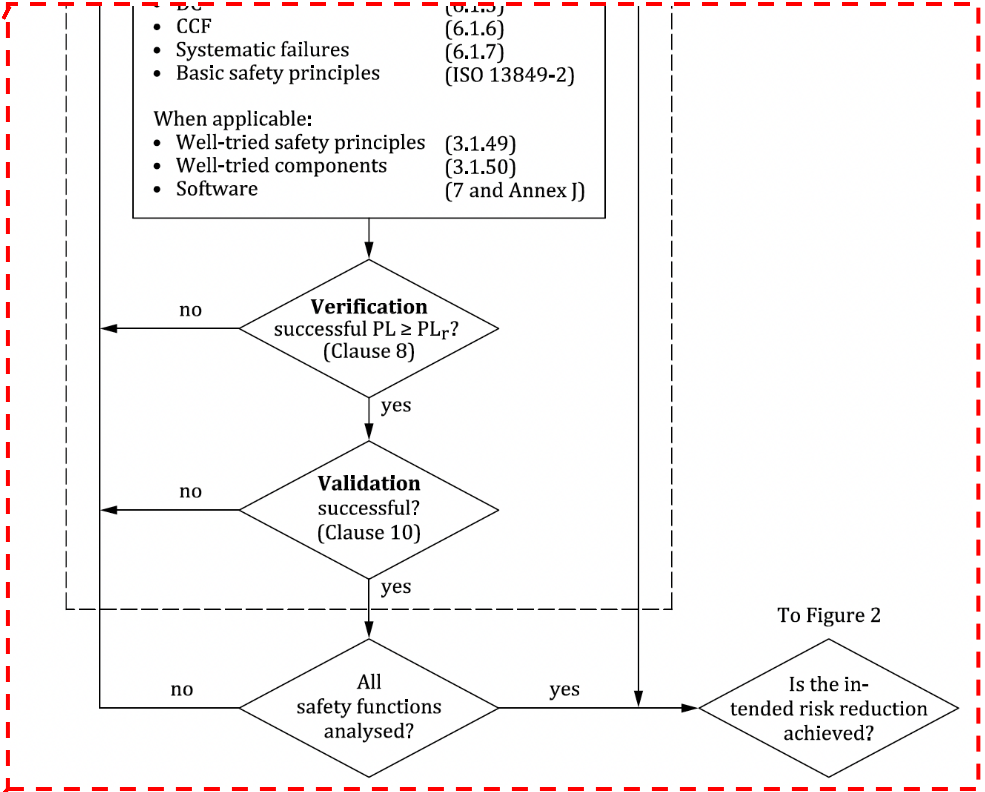
- Category (6.1.3)
- $MTTF_D$ (6.1.4)
- DC (6.1.5)
- CCF (6.1.6)

[2]

Clause 4 – Design process

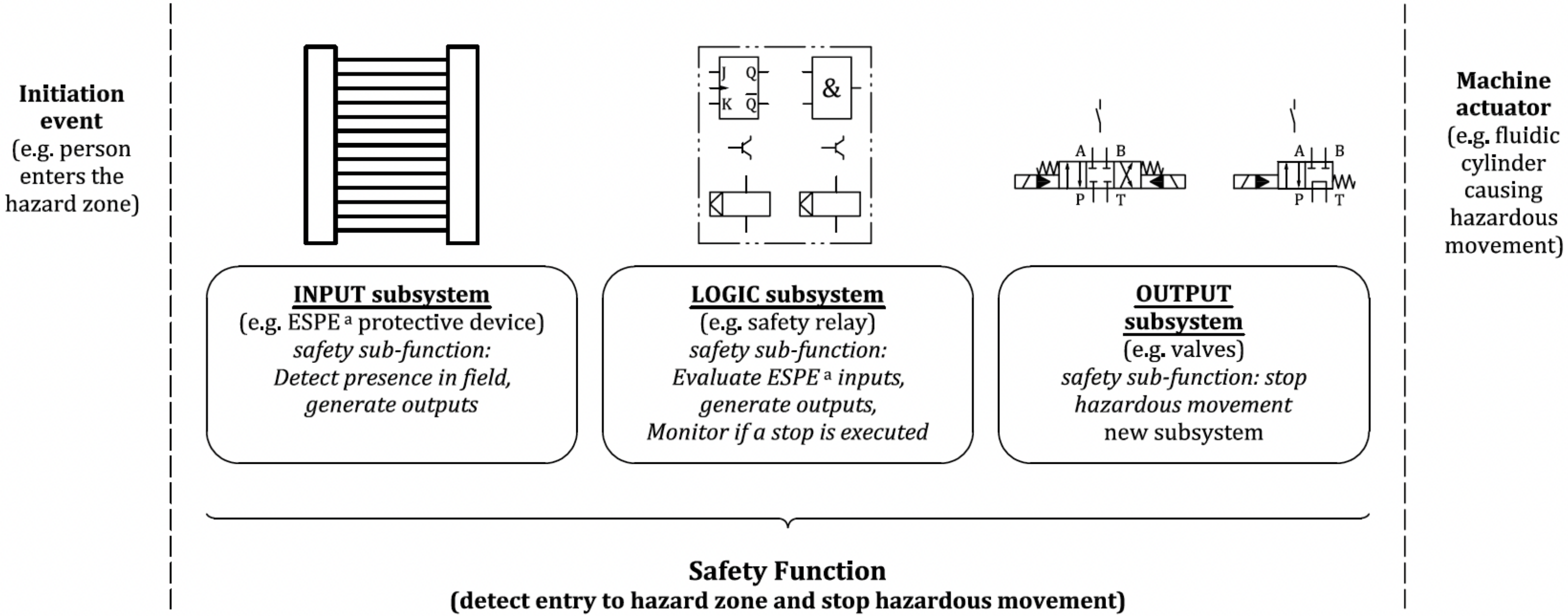
Fig. 4


Step 2
Risk reduction by safeguarding
Implementation of complementary protective measures
From Figure 2
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 ≥ PL_r? (Clause 8)
yes
no
Validation successful? (Clause 10)
yes
no
All safety functions analysed?
yes
To Figure 2
Is the in-tended risk reduction achieved?


- 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 ≥ PL_r? (Clause 8)
yes
no
Validation successful? (Clause 10)
yes
no
All safety functions analysed?
yes
To Figure 2
Is the in-tended risk reduction achieved?

[2]

Clause 5 – Specification of Safety Functions



Initiation event
(e.g. person enters the hazard zone)

INPUT subsystem
(e.g. ESPE [a] protective device)
safety sub-function:
Detect presence in field, generate outputs

LOGIC subsystem
(e.g. safety relay)
safety sub-function:
Evaluate ESPE [a] inputs, generate outputs,
Monitor if a stop is executed

OUTPUT subsystem
(e.g. valves)
safety sub-function: stop hazardous movement
new subsystem

Machine actuator
(e.g. fluidic cylinder causing hazardous movement)

Safety Function
(detect entry to hazard zone and stop hazardous movement)

[2]

Figure 5

Clause 9 – Ergonomic aspects of design

3rd Ed.

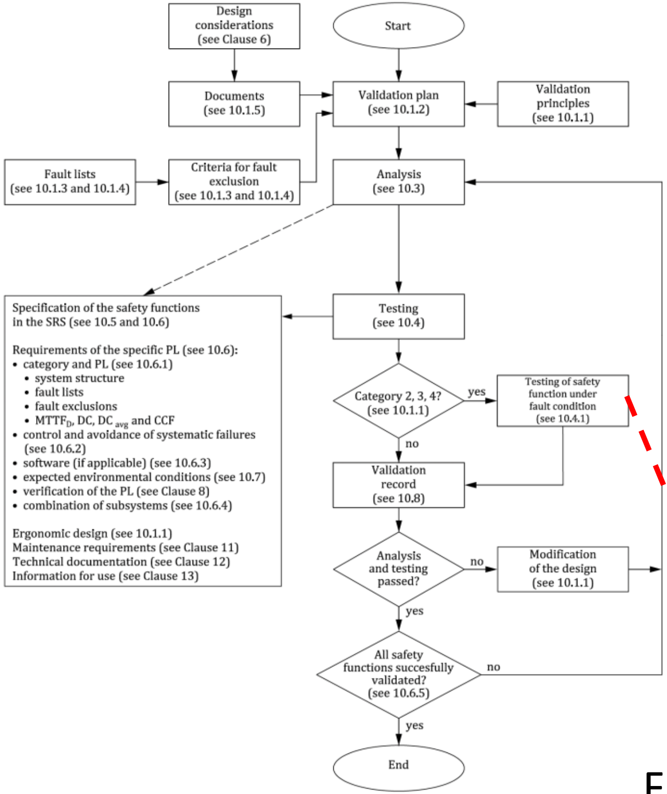
- The interface between operators and the SRP/CS shall be designed and realized such that no person is endangered during all intended use and reasonable foreseeable misuse of the machine [see also ISO 12100, EN 614-1, ISO 9355-1, ISO 9355-2, ISO 9355-3, EN 1005-3, IEC 60204-1:2005, Clause 10, IEC 60447 and IEC 61310].
- Ergonomic principles shall be used so that the machine and the control system, including the safety related parts, are easy to use, and so that the operator is not tempted to act in a hazardous manner.
- The safety requirements for observing ergonomic principles given in ISO 12100:2010, 6.2.8, apply.

4th Ed.

- The interface between operators and the SRP/CS shall be designed and realized to minimize exposures to hazards during the intended use and the reasonably foreseeable misuse of the machine due to neglecting ergonomic principles.
- The ergonomic principles given in ISO 12100:2010, 6.2.8, apply.
- NOTE Ergonomic principles are intended to improve the ease of use of the control systems to avoid motivation for defeating or unintended misuse of the machine. See ISO/TR 22100-3 and ISO 9241-210 for guidance on ergonomics.

[2], [3]

Clause 10 - Validation



Design considerations (see Clause 6)

Start

Documents (see 10.1.5)

Validation plan (see 10.1.2)

Validation principles (see 10.1.1)

Fault lists (see 10.1.3 and 10.1.4)

Criteria for fault exclusion (see 10.1.3 and 10.1.4)

Analysis (see 10.3)

Specification of the safety functions in the SRS (see 10.5 and 10.6)

Requirements of the specific PL (see 10.6):

- category and PL (see 10.6.1)
  - system structure
  - fault lists
  - fault exclusions
  - $MTTF_D$, DC, DC_{avg} and CCF
- control and avoidance of systematic failures (see 10.6.2)
- software (if applicable) (see 10.6.3)
- expected environmental conditions (see 10.7)
- verification of the PL (see Clause 8)
- combination of subsystems (see 10.6.4)

Ergonomic design (see 10.1.1)
Maintenance requirements (see Clause 11)
Technical documentation (see Clause 12)
Information for use (see Clause 13)

Testing (see 10.4)

Category 2, 3, 4? (see 10.1.1)

yes

Testing of safety function under fault condition (see 10.4.1)

no

Validation record (see 10.8)

Analysis and testing passed?

no

Modification of the design (see 10.1.1)

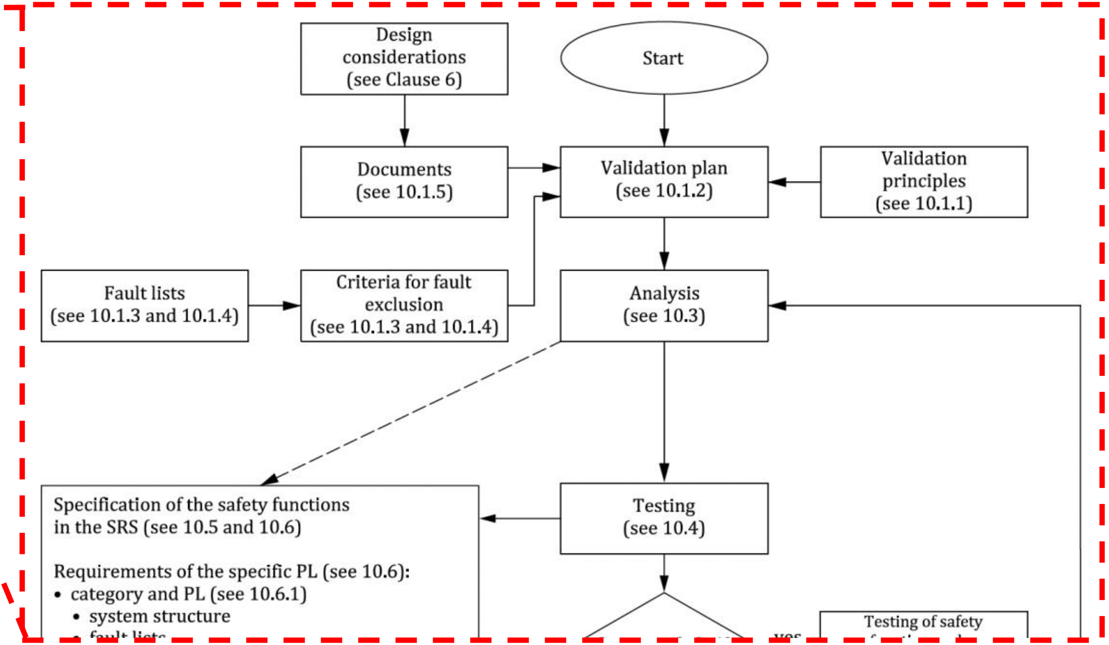
yes

All safety functions succesfully validated? (see 10.6.5)

no

yes

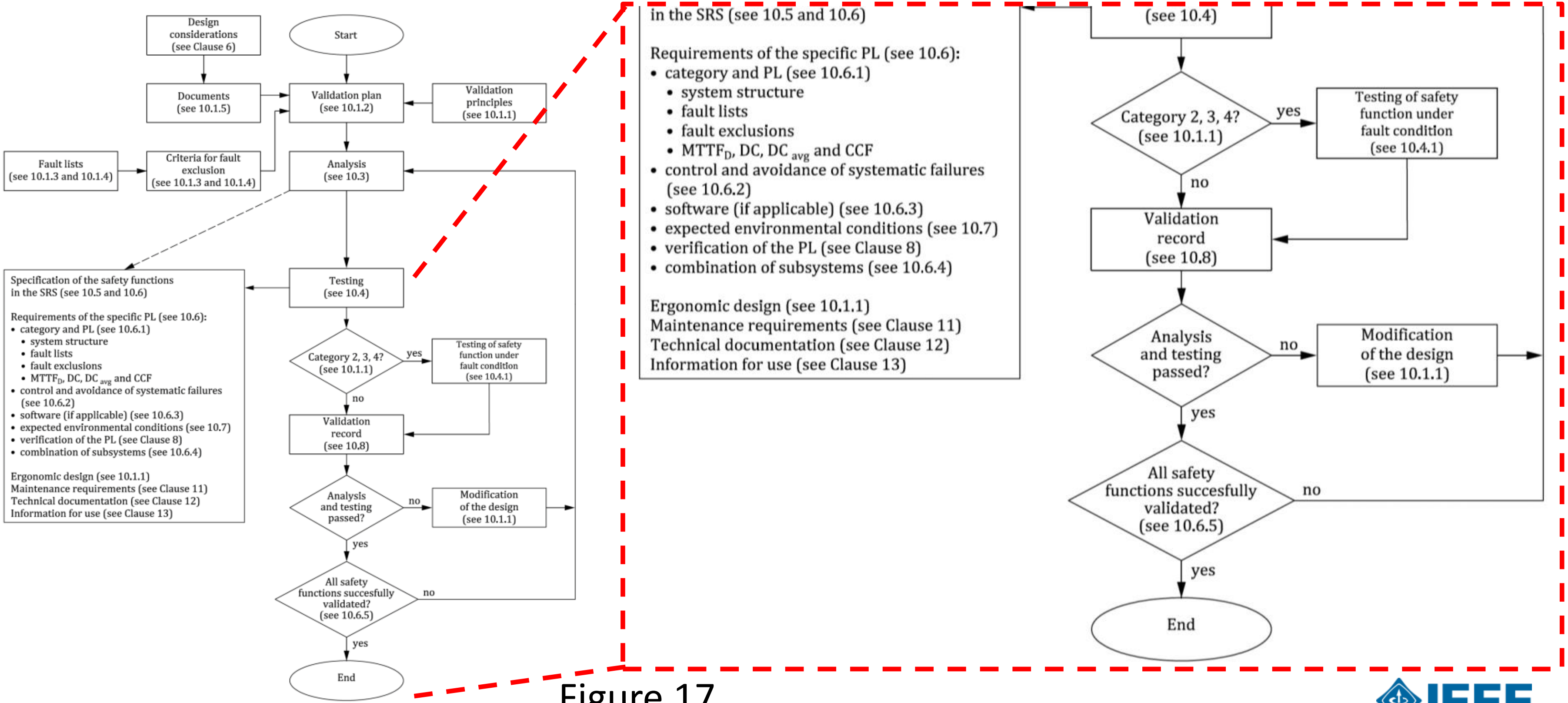
End


Design considerations (see Clause 6)
Start
Documents (see 10.1.5)
Validation plan (see 10.1.2)
Validation principles (see 10.1.1)
Fault lists (see 10.1.3 and 10.1.4)
Criteria for fault exclusion (see 10.1.3 and 10.1.4)
Analysis (see 10.3)
Specification of the safety functions in the SRS (see 10.5 and 10.6)
Requirements of the specific PL (see 10.6):
• category and PL (see 10.6.1)
• system structure
Testing (see 10.4)
Testing of safety

[2]

Figure 17

Clause 10 - Validation



Design considerations (see Clause 6)

Start

Documents (see 10.1.5)

Validation plan (see 10.1.2)

Validation principles (see 10.1.1)

Fault lists (see 10.1.3 and 10.1.4)

Criteria for fault exclusion (see 10.1.3 and 10.1.4)

Analysis (see 10.3)

Specification of the safety functions in the SRS (see 10.5 and 10.6)

Requirements of the specific PL (see 10.6):
- category and PL (see 10.6.1)
  - system structure
  - fault lists
  - fault exclusions
  - $MTTF_D$, DC, DC_{avg} and CCF
- control and avoidance of systematic failures (see 10.6.2)
- software (if applicable) (see 10.6.3)
- expected environmental conditions (see 10.7)
- verification of the PL (see Clause 8)
- combination of subsystems (see 10.6.4)

Ergonomic design (see 10.1.1)
Maintenance requirements (see Clause 11)
Technical documentation (see Clause 12)
Information for use (see Clause 13)

Testing (see 10.4)

Category 2, 3, 4? (see 10.1.1)

yes

Testing of safety function under fault condition (see 10.4.1)

no

Validation record (see 10.8)

Analysis and testing passed?

no

Modification of the design (see 10.1.1)

yes

All safety functions succesfully validated? (see 10.6.5)

no

yes

End

in the SRS (see 10.5 and 10.6)

Requirements of the specific PL (see 10.6):
- category and PL (see 10.6.1)
  - system structure
  - fault lists
  - fault exclusions
  - $MTTF_D$, DC, DC_{avg} and CCF
- control and avoidance of systematic failures (see 10.6.2)
- software (if applicable) (see 10.6.3)
- expected environmental conditions (see 10.7)
- verification of the PL (see Clause 8)
- combination of subsystems (see 10.6.4)

Ergonomic design (see 10.1.1)
Maintenance requirements (see Clause 11)
Technical documentation (see Clause 12)
Information for use (see Clause 13)

(see 10.4)

Category 2, 3, 4? (see 10.1.1)

yes

Testing of safety function under fault condition (see 10.4.1)

no

Validation record (see 10.8)

Analysis and testing passed?

no

Modification of the design (see 10.1.1)

yes

All safety functions succesfully validated? (see 10.6.5)

no

yes

End

Figure 17

[2]

Annex A – New Method for determining the “P” factor

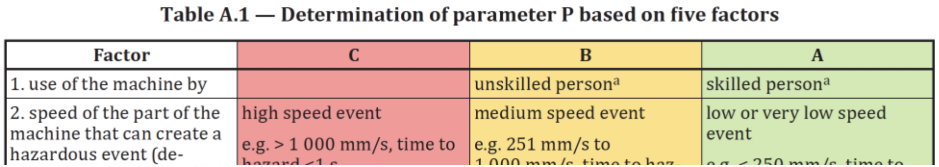


Table A.1 — Determination of parameter P based on five factors

Factor	C	B	A
1. use of the machine by		unskilled person[a]	skilled person[a]
2. speed of the part of the machine that can create a hazardous event (de-	high speed event e.g. > 1 000 mm/s, time to hazard <1 s	medium speed event e.g. 251 mm/s to 1 000 mm/s, time to haz-	low or very low speed event e.g. ≤ 250 mm/s, time to

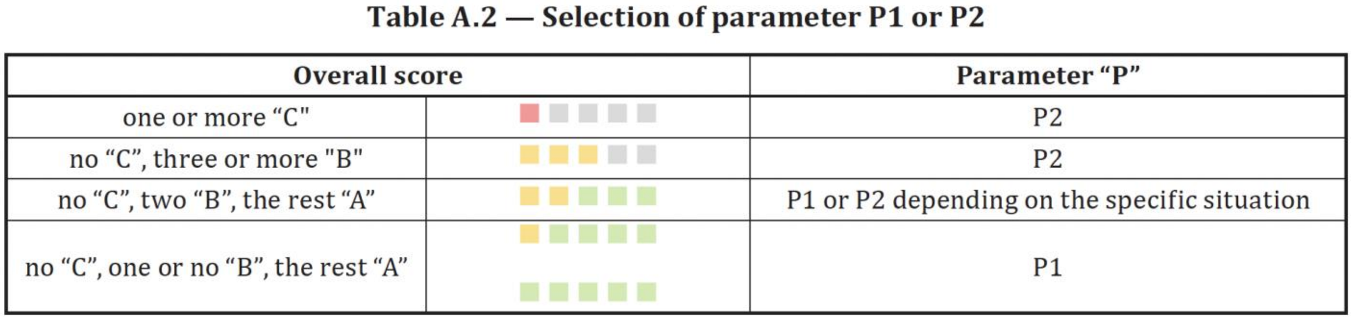
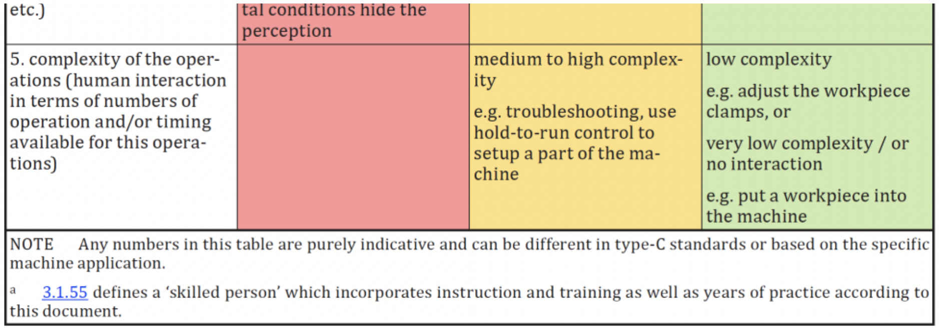


Table A.2 — Selection of parameter P1 or P2

Overall score		Parameter “P”
one or more “C"	🟥⬜⬜⬜⬜	P2
no “C”, three or more "B"	🟨🟨🟨⬜⬜	P2
no “C”, two “B”, the rest “A”	🟨🟨🟩🟩🟩	P1 or P2 depending on the specific situation
no “C”, one or no “B”, the rest “A”	🟨🟩🟩🟩🟩 🟩🟩🟩🟩🟩	P1



etc.)	tal conditions hide the perception		
5. complexity of the operations (human interaction in terms of numbers of operation and/or timing available for this operations)		medium to high complexity e.g. troubleshooting, use hold-to-run control to setup a part of the machine	low complexity e.g. adjust the workpiece clamps, or very low complexity / or no interaction e.g. put a workpiece into the machine

NOTE Any numbers in this table are purely indicative and can be different in type-C standards or based on the specific machine application.

[a] 3.1.55 defines a ‘skilled person’ which incorporates instruction and training as well as years of practice according to this document.

[2]

Technical Flaws in the 2023 4th ed.

Systematic failures

Clause 6.1.7

- The clause speaks to the ways that systematic failures can occur.
- It requires that measures against EMI be taken, which leads to Annex L and the four routes, including the use of “Route C” which relies upon a risk scoring method that is previously undocumented*.
- More on this in the discussion on Annex L

*Developed at DGUV in Germany, but no peer-reviewed publications or filed trial data is available.

[2]

Determining the PL & PFH$_D$ without data

Clause 6.1.9

- A new approach has been proposed that does not require PFHD (Probability of a Dangerous Failure per Hour) data to determine the Performance Level (PL) of components.
- The approach allows for determining the PL and related PFHD even when failure rate data for components are unknown or not indicated by the manufacturer for safety-related applications, based solely on the architecture, DC, and CCF.
- The use of components without failure-rate data is subject to the conditions that:
  - they are mechanical, hydraulic, pneumatic, electrohydraulic or electropneumatic components, and
  - in Categories 2-4 are limited to well-tried components. It is unclear how a component can be considered well-tried without any reliability information.
- The T10D value for component replacement is limited to 10 years. However, specifying a 20-year mission time for components without knowledge of their useful lifetime creates a conflict, as the useful life should be greater than the mission time for proper replacement planning.
- In the absence of reliability data, the alternative method suggests using failure rate field data from similar component applications collected over a significant period of time, or assuming a worst-case MTTFD (Mean Time to Dangerous Failure) of 10 years.
- The alternative method has been criticized for lacking a technical basis and relying on questionable assumptions.

[2]

Software safety requirements – Clause 7

Use of AI/ML in SRP/CS

- Clause 7.1 opens with the following:

  “Although artificial intelligence (AI) can be used for SRP/CS, this clause does not address additional specific requirements necessary for AI technology and its use as part of SRP/CS.”
- This clause opens the door for the use of AI/ML technology without offering guidance on its use.
- No validation requirements for systems incorporating AI/ML are included in the 4th Ed.
- ISO/IEC DTR 5469, Artificial intelligence — Functional safety and AI systems [4] is in development jointly in ISO/IEC JTC 1/SC 42 – Artificial intelligence and IEC/TC 65/SC 65A – System Aspects.
  https://www.iso.org/standard/81283.html

  1 Scope
  This document describes the properties, related risk factors, available methods and processes relating to:
  - Use of AI inside a safety related function to realize the functionality;
  - Use of non-AI safety related functions to ensure safety for an AI controlled equipment;
  - Use of AI systems to design and develop safety related functions.
- [4] includes validation techniques in Clause 9. However, it is unclear when this document will be published.

[2]

Safety-related embedded software (SRESW) – Cl. 7.3

Applications of embedded software

- The 4th Edition includes requirements outside the scope of the document. From the Scope:

  “This document **does not give specific requirements for the design of products/components** that are part of SRP/CS. Specific requirements for the design of some components of SRP/CS are covered by applicable ISO and IEC standards.”

- The scope includes the design of safety systems, not safety components; however, the clause covering the development of safety-related embedded software (SRESW), i.e., safety software developed using high-variability language and provided as firmware, requires the use of design techniques at the component level.
- The development of SRESW is covered in detail in IEC 61508-3:2010 [2] but is outside the scope of ISO 13849-1. This is the first reason I recommend that you do not use ISO 13849-1:2023.

[2]

Allowance for use of standard PLCs

Clause 7.3.2 and Annex I

- The 4th edition of ISO 13849-1 includes new approaches to functional safety systems unsupported by sound engineering practices.
- One unresolved question arising from this clause is whether two standard PLCs used in Cat. 3 or 4 architecture for systems with PL_r up to e is acceptable.
- This approach yields different results than could be achieved using the standard calculations on the same components. It is likely to produce control systems that will not perform as required.
- It is possible to demonstrate that the two approaches will give PFH_D values that differ approximatively by more than one decade and PL values that differ at least for one level!
- The result is that the standard makes it possible to get two different values for the same circuit.

[2]

Annex L – EM resilience for functional safety systems

Four Routes

- Route A – Use the product standard
  - This method is good engineering practice
  - Supported by product standards
  - Does not use increased test stimulus, ∴ will miss susceptibilities
  - Does not address the effect of electro-magnetic pulses (EMP) on safety systems
- Route B – Use IEC 61000-6-2 [5]
  - Follows a published standard
  - The standard is not comprehensive and has some significant flaws
  - Uses increased stimulus levels
  - Requires the use of IEC 61000-2-9 [6] for high-altitude electromagnetic pulse (HEMP)

[2]

Annex L – EM resilience for functional safety systems

Four Routes

- Route C – Implement EMC measures on a system level
  - Unproven risk assessment method
  - Can be used to justify doing nothing
- Route D – Follow IEC 61000-6-7 [7] or other generic EMC standards for functional safety
  - Requires increased immunity levels compared to basic standards like [5]
  - Allows for the use of other generic EM immunity standards e.g., IEC 61326-3-1 [8]

[2], [5], [7], [8]

IEEE 1848 and the Machinery Sector Specific Version

Techniques and Measures to improve electromagnetic resilience of functional safety systems

What to do?

Consider using IEEE 1848:2020

- IEEE 1848:2020, *IEEE Standard for Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetic Disturbances*
- Supports the existing standards [2], [3], [5], [6], [7], [8]
- Requires testing
- Addresses shortcomings in existing standards by adding EMC for Functional Safety techniques and measures
- Adaptation of the IET "Code of Practice for Electromagnetic Resilience", 2017 [10]
- New machinery sector specific version starts development in fall 2023: https://sagroups.ieee.org/1848-mssv/

Compliance
inSight
Consulting Inc.

Expert Advice, Safety Reviews, In-Depth Training

Doug Nix, C.E.T., SM-IEEE '14

Managing Director & Principal Consultant

+1 519 729 4704

dnix@complianceinsight.ca

www.complianceinsight.ca

Machinery Safety 101 blog

machinerysafety101.com

Online Training

courses.complianceinsight.ca