Workplace Safety & Prevention Services®

Practical Application of ISO 13849-1

Robert Vomiero, P. Eng., FS Eng, CMSE®, CHSC
Specialized Practice Lead (Machine & Robotics Safety)

Workplace Safety and Prevention Services

Disclaimer

Workplace Safety & Prevention Services®

Objective

- To get a better understanding about ‘Functional Safety’, highlight some important elements of ISO 13849-1, and to provide a simple application example using ISO 13849-1 concepts.

Agenda

- What is *'Functional Safety'*?
- Functional Safety Standards
- ISO 13849-1 overview.
- ISO 13849-1 – Some fundamentals
- ISO 13849 -1 - Key Application Principles
  - Performance Levels
    - Mean Time to Dangerous Failures
    - Diagnostic Coverage
    - Common Cause Failures
  - Category Structures
- The importance of Risk Assessments
- PL vs SIL
- A practical example

What is Functional Safety?

- Part of the overall safety of a machine or machine control system that depends on the correct functioning of the *'safety-related control system'* and other risk reduction measures.

[Source: International Electrotechnical Commission, [IEC] 62061 2021, p. 16]

Functional Safety Standards

IEC 61508:2010 Functional safety of electrical / electronic / programmable electronic safety-related systems

- Part 1: General requirements
- Part 2: Requirements for electrical / electronic / programmable electronic safety-related systems
- Part 3: Software requirements
- Part 4: Definitions and abbreviations
- Part 5: Examples of methods for the determination of safety integrity levels
- Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
- Part 7: Overview of techniques and measures

ISO 13849-1:2015 Safety of Machinery – Safety-Related Parts of Control Systems

- Part 1: General Requirements for Design
- Part 2: Validation

IEC 62016:2021 Safety of Machinery – Functional Safety of Safety-Related Control Systems

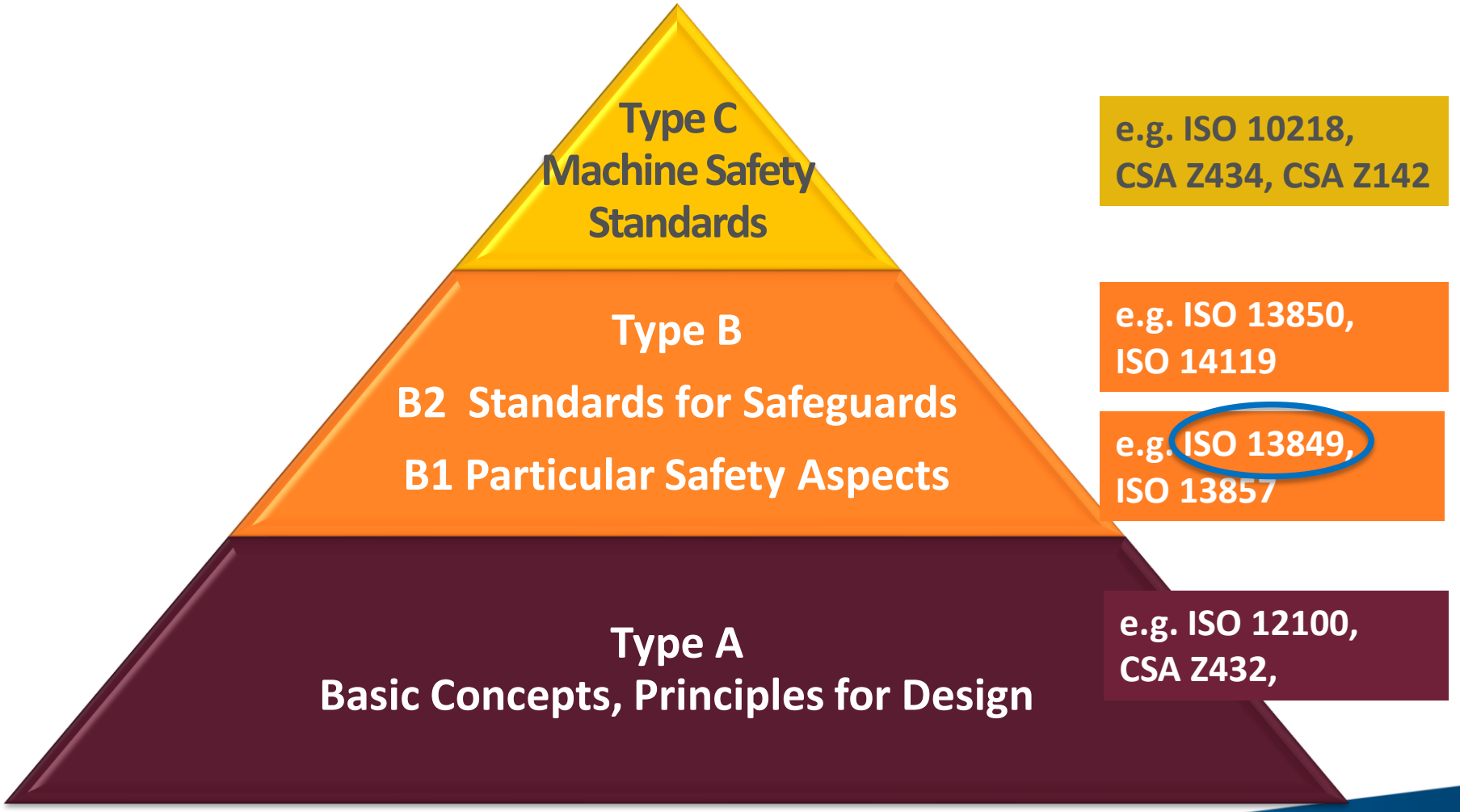
Workplace Safety & Prevention Services®

ISO 13849-1: Safety of Machinery – Safety-Related Parts of Control Systems – General Principles for Design

Overview

- Current version of ISO 13849 is ‘2015’ version
- Third edition – replaced ISO 13849-1:2006
- Standard Type - *‘Type-B1’ – Safety Aspects*
- Used by Technical Committees when developing *type-B2* or *type-C* standards.
- An updated version of ISO 13849-1 is currently under development *(see ISO/DIS 13849-1.2)*

Machine Safety Standard Types



Workplace Safety & Prevention Services®

ISO 13849-1 – Some Fundamentals

- What is a *'Safety Function'*
  - From ISO 12100: *Function of a machine whose failure can result in an immediate increase of the risk(s)*

- Sample safety functions *[from Table 8, ISO 13849]*
  - Safety-related Stop issued by a safeguard (e.g. safety interlock, or light curtain)
  - Muting function
  - Hold to run function
  - Prevention of unexpected start-up

ISO 13849-1 – Some Fundamentals cont'd…

- Parts of machinery control systems that provide safety functions are called the *'safety-related part of control systems' (SRP/CS).*
- *SRP/CS* of a machine can consist of hardware and software elements.
- The purpose of *ISO 13849-1* is to provide a framework and process for assessing the *'performance'* of *SRP/CS*.
- In addition to providing *safety functions*, *SRP/CS* can also provide operational functions *(e.g. a two-hand-control provides both a safety function and a means for process initiation)*

ISO 13849-1 – Key Principles

Performance Levels

- *ISO 13849-1* uses *'Performance Levels (PL)'* to indicate the ability of a machine's *SRP/CS* to perform a *safety function* under foreseeable conditions.

- Five (5) *Performance Levels (PLa-PLe)* can be assigned to the *SRP/CS*.
  - PLa - lowest performance level
  - PLe - highest performance level

- Performance Levels are defined in terms of *average 'Probability of Dangerous Failure per Hour' (PFH_D)*

- *Dangerous Failure –* A failure which has the potential to place the *SRP/CS* in a hazardous or fail-to-function state

(Source: International Organization for Standardization, [ISO] 13849-1 2015, p.3)

ISO 13849-1 – Understanding Performance Levels cont'd…

- Each of the (5) Performance Levels have defined ranges of *PFH_D (1/h, fractional hours)*

Table 2 — Performance levels (PL)

PL	Average probability of dangerous failure per hour (PFH_D) 1/h
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Table 2, p 11]

ISO 13849-1 – Understanding Performance Levels cont'd…

- The *Probability of Dangerous Failure per Hour (PFH_D)* depends on several factors including:
  - ***Mean time to Dangerous Failure ($MTTF_D$)*** – Expectation of the mean time to dangerous failure.
  - ***Diagnostic Coverage (DC)***
    - Measure of the effectiveness of diagnostics
    - Ratio between: failure rate of *'Detected Dangerous Failures'* and failure rate of *'Total Dangerous Failures'*
  - ***Common Cause Failure (CCF) –*** Failures of different items, resulting from a single event, where these failures are not consequences of each other.

Elements of Performance Level (PL): Mean Time to Dangerous Failure ($MTTF_D$)

- *$MTTF_D$* is the mean time it takes for a component to fail dangerously
- *$MTTF_D$* values are provided in *years*

Table 4 — Mean time to dangerous failure of each channel ($MTTF_D$)

$MTTF_D$	
Denotation of each channel	**Range of each channel**
Low	3 years ≤ $MTTF_D$ < 10 years
Medium	10 years ≤ $MTTF_D$ < 30 years
High	30 years ≤ $MTTF_D$ ≤ 100 years

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Table 4, p. 17]

- *Table 4* shows 3 ranges of *$MTTF_D$ – Low, Med, High*
- The Max. *$MTTF_D$* value of a safety function for each channel is 100 years

Mean Time to Dangerous Failure ($MTTF_D$)…cont'd

- Process for estimation of *$MTTF_D$* of a component must be in the following order:
  - Use manufacturer's data
  - Use methods in *Annex C* and *Annex D* of ISO 13849-1
  - Choose 10 years

[Source: International Organization for Standardization, [ISO] 13849-1 2015, p. 17]

MTTFD for single components (Annex C)

- Several methods outlined for determining *MTTFD*
- Often MTTFD values for safety function components are provided by the manufacturer.
- For *electromechanical* components (valves, relays, switches, contactors etc.), manufacturers provide B_{10D} values.
  - B_{10D} - *Mean number of cycles until 10% of components fail*
- In situations where *MTTFD* or B_{10D},values are not provided, if the specific criteria outlined in Annex C are met, then *Table C.1* can be used.
  - *(Table C1 e.g.: hydraulic component with nop ≥ 1,000,000 cycles/yr; MTTFD = 150yrs)*

Calculating MTTFD using B_{10D} values

- Important formulas:

$$\mathrm{MTTF_D} = \frac{B_{10D}}{0{,}1 \times n_{op}} \qquad n_{op} = \frac{d_{op} \times h_{op} \times 3600\ \mathrm{s/h}}{t_{cycle}}$$

$$T_{10D} = \frac{B_{10D}}{n_{op}} \qquad \lambda_D \approx \frac{0{,}1}{T_{10D}} = \frac{0{,}1 \times n_{op}}{B_{10D}}$$

$$\mathrm{MTTF_D} = \frac{T_{10D}}{0{,}1} = \frac{B_{10D}}{0{,}1 \times n_{op}}$$

- *(Note: if only B_{10} value is provided, then: $B_{10D} = 2B_{10}$)*

[Source: International Organization for Standardization, [ISO] 13849-1 2015, p. 52]

***B_{10D}** = # of cycles until 10% of components fail dangerously*

***T_{10D}** = mean time until 10% of components fail dangerously*

***n_{op}** = # actuations per year*

***d_{op}** = avg. operating time (days/yr)*

***h_{op}** = avg. operating time (hrs/day)*

***tcycle** = time/cycle (sec)*

***λD** = Dangerous Failure Rate*

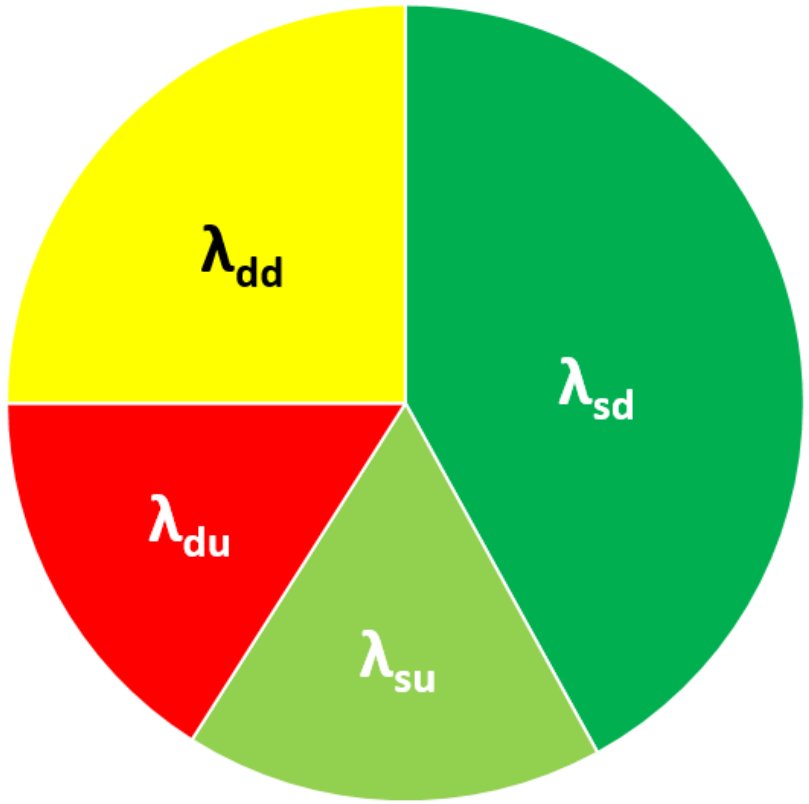
Elements of Performance Level: Diagnostic Coverage (DC)

- *λ – Rate of failure derived from rate of safe failures and the rate of failure to danger.*

- Types of Failures
  - ‘Safe’ failures (detected, undetected)
  - ‘Dangerous’ Failure (detected, undetected)

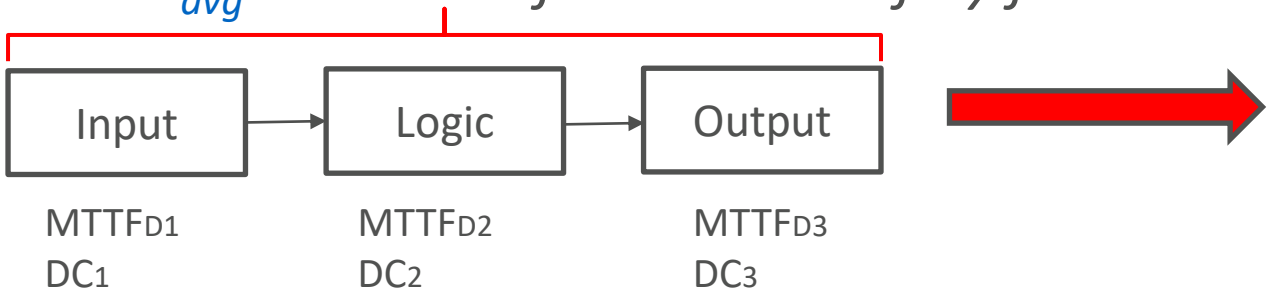
- DC = $\sum \lambda_{dd} / \sum \lambda_{dtotal}$

- DC values are provided as a percentage (%)



Elements of Performance Level: DC…Cont'd

- How do you determine DC?
  - Provided by safeguarding device and component manufacturer, or…
  - You can estimate it for individual components - See *ISO 13849, Annex E, Table E.1*
  - *Note: DC_{avg} calculated for entire a safety function*



$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}}$$

(Note: Cat B and Cat 1, DC = 0)

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Annex E, p. 60]

Table 5 — Diagnostic coverage (DC)

DC	
Denotation	**Range**
None	DC < 60 %
Low	60 % ≤ DC < 90 %
Medium	90 % ≤ DC < 99 %
High	99 % ≤ DC

DC < 60% only has a slight effect on reliability

DC < 99% difficult to achieve

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Table 5, p. 17]

Workplace Safety & Prevention Services®

Elements of Performance Level (PL): Common Cause Failure (CCF)

- *CCFs* are failures of different items, resulting from a single event, where the failures are not a consequence of each other.
  - *Example – Electromagnetic disturbances in electrical and electronic systems can result in failures of multiple elements in the system.*
- This is a qualitative process that should be considered for the whole system
- A *CCF* score ≥ 65 must be achieved *(see Annex F)*

Table F.1 — Scoring process and quantification of measures against CCF

No.	Measure against CCF	Score
1	**Separation/ Segregation**	
	Physical separation between signal paths, for example: — separation in wiring/piping; — detection of short circuits and open circuits in cables by dynamic test; — separate shielding for the signal path of each channel; — sufficient clearances and creepage distances on printed-circuit boards.	15
2	**Diversity**	
	Different technologies/design or physical principles are used, for example: — first channel electronic or programmable electronic and second channel electrome-chanical hardwired, — different initiation of safety function for each channel (e.g. position, pressure, tem-perature), and/or digital and analog measurement of variables (e.g. distance, pressure or temperature) and/or	20
6.2	Other influences Consideration of the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards).	10
	Total	**[max. achievable 100]**

Total score	Measures for avoiding CCF[a]
65 or better	Meets the requirements
Less than 65	Process failed ⇒ choose additional measures

[a] Where technological measures are not relevant, points attached to this column can be considered in the comprehensive calculation.

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Annex F, Table F.1, p. 61, 62]

Categories Structures

- ISO 13849-1 also utilizes different *Category Structures* to assist in the assessment of achieved *Performance Levels (PL)*

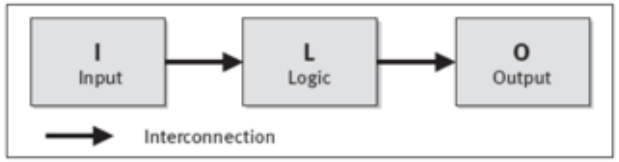
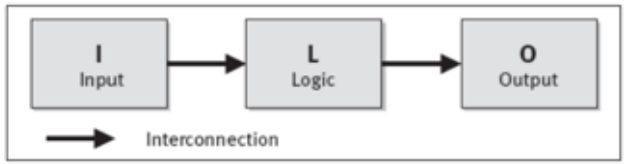
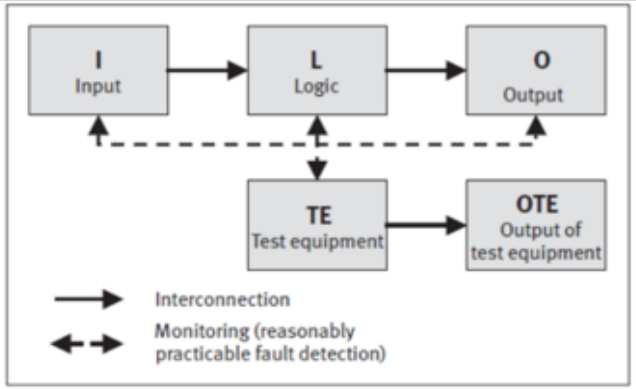
- *Category Structures* refer to the architecture of the *safety functions* that make-up the *SRP/CS*.

- There are five (5) levels of Category Structure defined in ISO 13849-1
  - *Category B, 1, 2, 3, 4*
  - Cat B is the lowest / Cat 4 is the highest

Category Structures Cont'd…

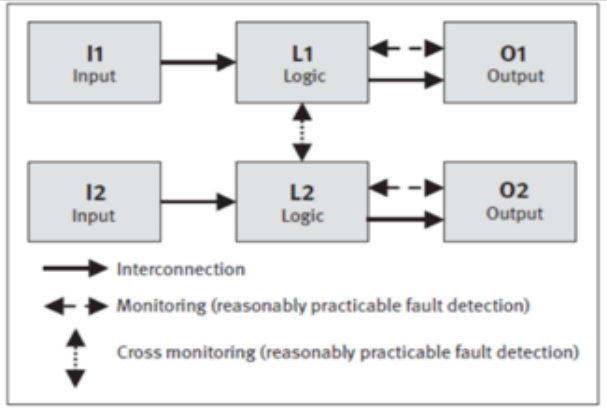
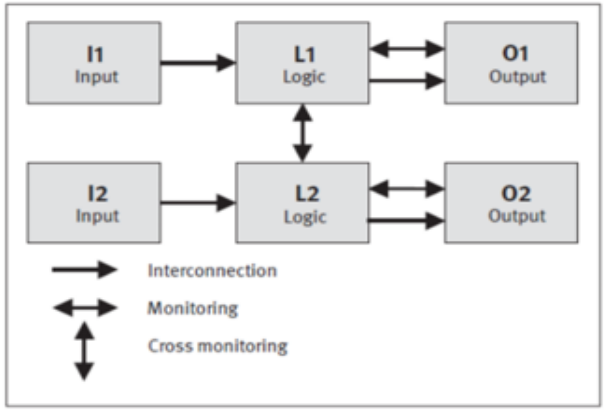
- The contribution to reliability (e.g. MTTFD, structure) can vary with the technology used.
- For example, it is possible (within certain limits) for a *single channel safety function* that uses high reliability components to provide the same or higher *PL* as a *fault-tolerant safety function* of lower reliability components.
- Therefore, *ISO 13849-1* incorporates an approach that considers both *PLs* and *Category Structures* to achieve required reliability levels.
  - Improving *PL* improves the ability of the individual components and the overall safety function to resist faults or failures.
  - Improving *Category Structure* improves the ability of the safety function to detect and avoid the hazardous effects of a fault.

Category Structure Requirements

Cat	Summary of requirements	System Behavior	Safety achieved by	Block Diagram / $MTTF_D$ (each chnl) / DC_{avg}
B	SRP/CS components to be designed, constructed, selected… in accordance with relevant standards. *Basic safety principles* shall be used	Fault can lead to loss of safety function	Mainly selection of components	 - $MTTF_D$: Low–High - DC_{avg} : None - Max PL: PLb
1	Requirements of Cat B apply. *Well-tried components* and *well-tried safety principles* shall be used	Probability of fault leading to loss of safety function is lower than Cat B	Mainly selection of components	 - $MTTF_D$: High - DC_{avg} : None - Max PL: PLc
2	Requirements of Cat B, and the use of *well-tried safety principles* Safety function shall be checked by control system at suitable intervals.	Occurrence of a fault can lead to loss of the safety function between the checks. Loss of safety function is detected by the check.	Mainly by structure of safety function	 - $MTTF_D$: Low – High - DC_{avg} : Low–Med - Max PL: PLd

(Source: International Organization for Standardization, [ISO] 13849-1 2015, p 32-38)

Category Structure Requirements Cont'd…

Cat	Summary of requirements	System Behavior	Safety achieved by	Block Diagram / $MTTF_D$ (each chn.) / DC_{avg}
3	Requirements of Cat B, and the use of *well-tried safety principles* A single fault in any safety-related parts does not lead to loss of safety function Wherever reasonably practicable, the single fault is detected	When a single fault occurs, the safety function is always performed. Some, but not all, faults will be detected. Accumulation of undetected faults can lead to loss of the safety function.	Mainly by structure of safety function	 - $MTTF_D$: Low – High - DC_{avg} : Low–Med - Max PL: PLe
4	Requirements of Cat B, and the use of *well-tried safety principles* A single fault in any safety-related parts does not lead to loss of safety function The single fault is detected at or before the next demand upon the safety function if possible, or accumulation of undetected faults shall not lead to the loss of the safety function.	When a single fault occurs the safety function is always performed. Detection of accumulated faults reduces the probability of the loss of the safety function (high DC). The faults will be detected in time to prevent the loss of the safety function.	Mainly by structure of safety function	 - $MTTF_D$: High - DC_{avg} : High (incl. fault accumulation) - Max PL: PLe

(Source: International Organization for Standardization, [ISO] 13849-1 2015, p 32-38)

Workplace Safety & Prevention Services®

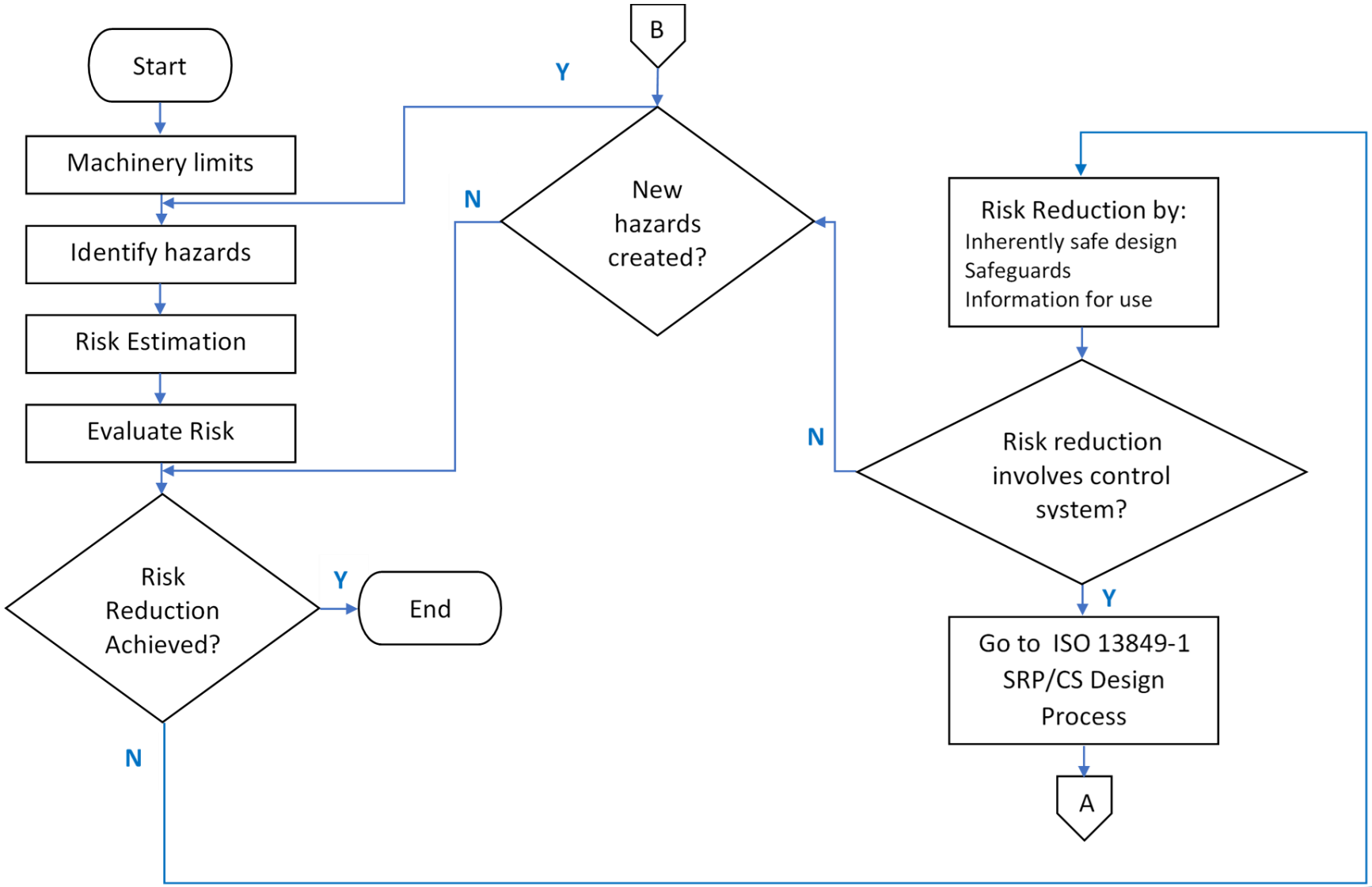
The Importance of the Risk Assessment

- The *Risk Assessment* process is utilized to identify hazards associated with a machine or system, and to establish a *'risk reduction'* strategy.

- *ISO 13849-1 indicates that SRP/CS of a machine shall be designed and constructed in accordance with the principles of ISO 12100.*
  - *(see: ISO 12100:2010 Safety of Machinery – General Principles for Design – Risk Assessment and Risk Reduction)*

- When the machine control system contributes to the risk reduction of machine hazards, the risk assessment process provides the *Required Performance Level (PLr)* for each *safety function* that makes up the *SRP/CS*

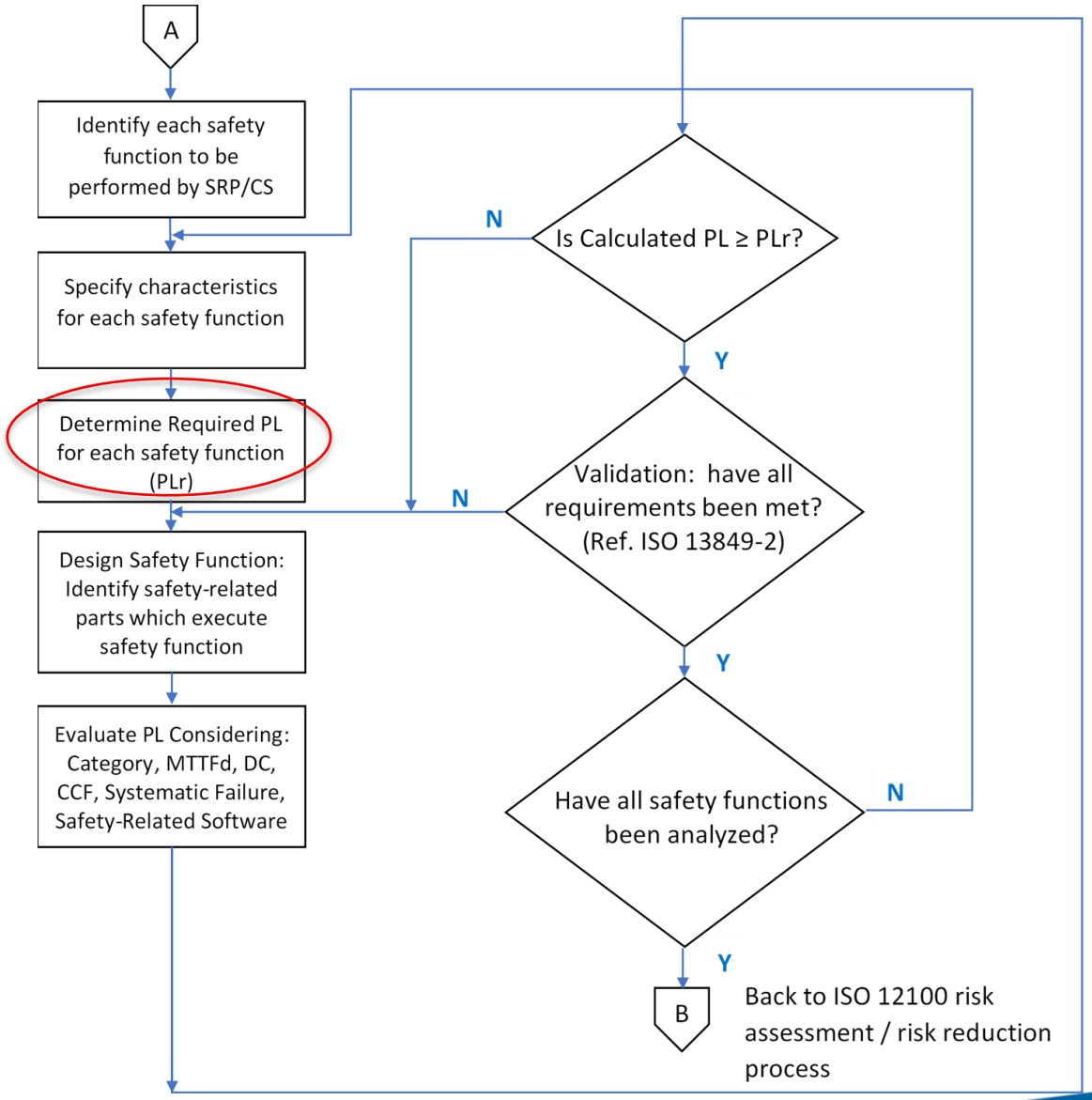
ISO 12100 Risk Assessment / Risk Reduction Process



[Source: International Organization for Standardization, [ISO] 13849-1 2015, Fig. 1, p 10)

Workplace Safety & Prevention Services®

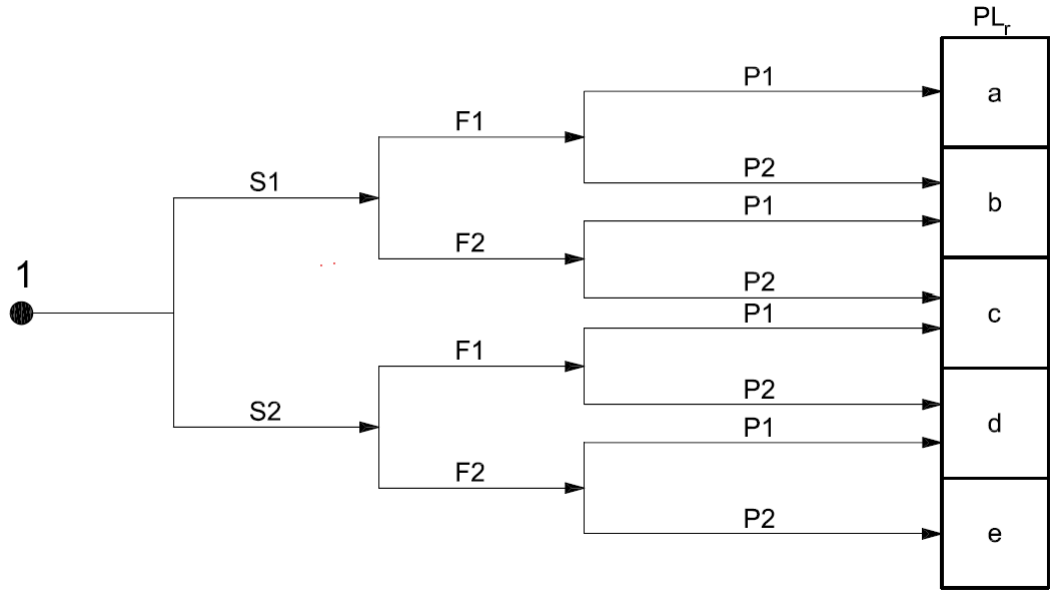
ISO 13849-1 Design Process for SRP/CS



[Source: International Organization for Standardization, [ISO] 13849-1 2015, Fig. 3, p 13]

Workplace Safety & Prevention Services®

Determining Required Performance Level (PLr)



Risk parameters:

S	severity of injury
S1	slight (normally reversible injury)
S2	serious (normally irreversible injury or death)
F	frequency and/or exposure to hazard
F1	seldom-to-less-often and/or exposure time is short
F2	frequent-to-continuous and/or exposure time is long
P	possibility of avoiding hazard or limiting harm
P1	possible under specific conditions
P2	scarcely possible

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Annex A, Fig A.1, p 45]

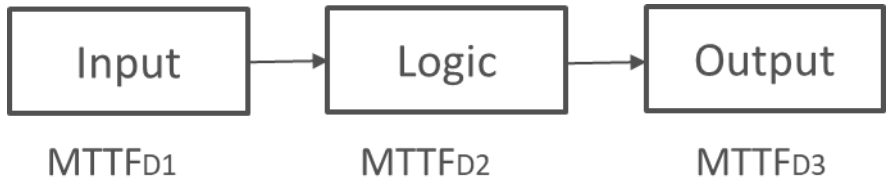
Note:

- The above is a generic estimation tool found in Annex A of ISO 13849-1.

- Other formal risk assessment methodologies exist – e.g. ANSI/RIA TR R15.036-2016.

Calculating $MTTF_D$

- MTTFD for each channel of a safety function



- In a redundant architecture *(Cat 3, Cat 4)* it is assumed that the $MTTF_D$ for each channel are the same
- If the $MTTF_D$ of the channels are the same value – use that value in Fig. 5 *(next slide)* to determine *PL*
- IF the $MTTF_D$ of the channels is different use this formula to estimate a common $MTTF_D$ for use in Fig. 5 to find *PL*

MTTFD for single channel safety function

$$\frac{1}{\mathrm{MTTF_D}} = \sum_{i=1}^{\tilde{N}} \frac{1}{\mathrm{MTTF_{D\,i}}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{\mathrm{MTTF_{D\,j}}}$$

where

$\mathrm{MTTF_D}$ is for the complete channel;

$$\frac{1}{MTTF_D} = \frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \frac{1}{MTTF_{D3}}$$

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Annex D, p. 56]

MTTFD for redundant channel safety function where each channel has different $MTTF_D$

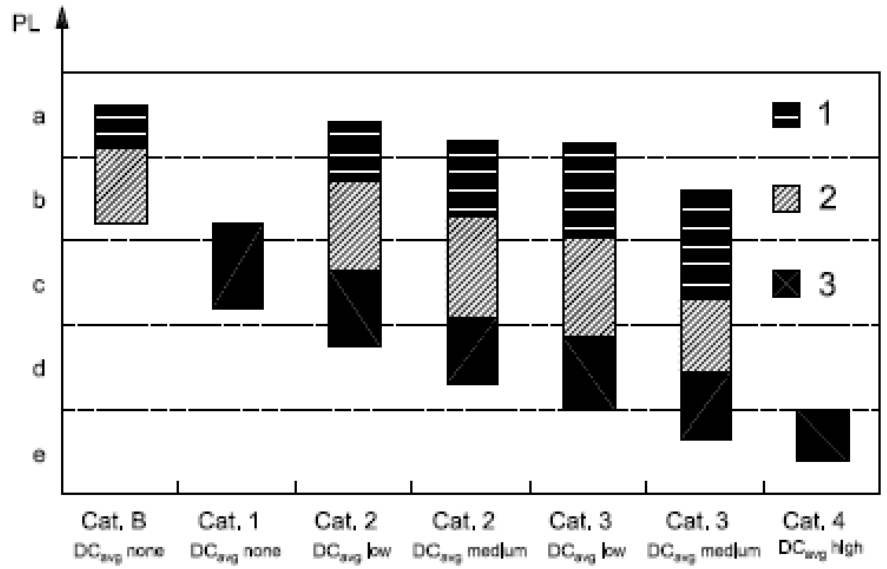
$$\mathrm{MTTF_D} = \frac{2}{3}\left[\mathrm{MTTF_{D\,C1}} + \mathrm{MTTF_{D\,C2}} - \frac{1}{\frac{1}{\mathrm{MTTF_{DC1}}} + \frac{1}{\mathrm{MTTF_{DC2}}}}\right]$$

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Annex D, p. 57]

Workplace Safety & Prevention Services®

Relationship - Categories, DCavg, MTTFD, and PL

- Fig. 5 shows how the combination of Category, DC_{avg}, $MTTF_D$ (each channel), can be used to estimate PL of a safety function *(simplified approach)*.
- PL can be read off the vertical axis of Fig. 5.



Key

PL	performance level
1	$MTTF_D$ of each channel = low
2	$MTTF_D$ of each channel = medium
3	$MTTF_D$ of each channel = high

Figure 5 — Relationship between categories, DC_{avg}, $MTTF_D$ of each channel and PL

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Table 6, p. 19]

Table 6 — Simplified procedure for evaluating PL achieved by SRP/CS

Category	B	1	2	2	3	3	4
DC_{avg}	none	none	low	medium	low	medium	high
$MTTF_D$ of each channel							
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

- Notes: If shaded MTTFD area of applicable vertical bar spans multiple PLs, use Table 6 to find PL.
- For a more precise value of PL based on precise MTTFD see *Annex K, Table K.1 Table*

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Fig 5, p. 19]

Workplace Safety & Prevention Services®

Combination of SRP/CS to determine overall PL

- If the PFH_D is known for each of the SRP/CS, add them together to find the total PFH_D for the safety function.

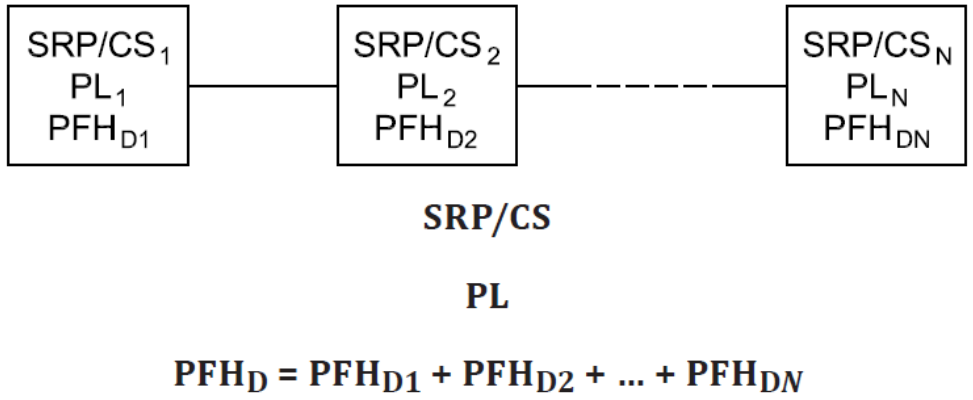


Figure 13 — Combination of SRP/CS to achieve overall PL

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Fig 13, p. 39]

Table 2 — Performance levels (PL)

PL	Average probability of dangerous failure per hour (PFH_D) 1/h
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Table 2, p 11]

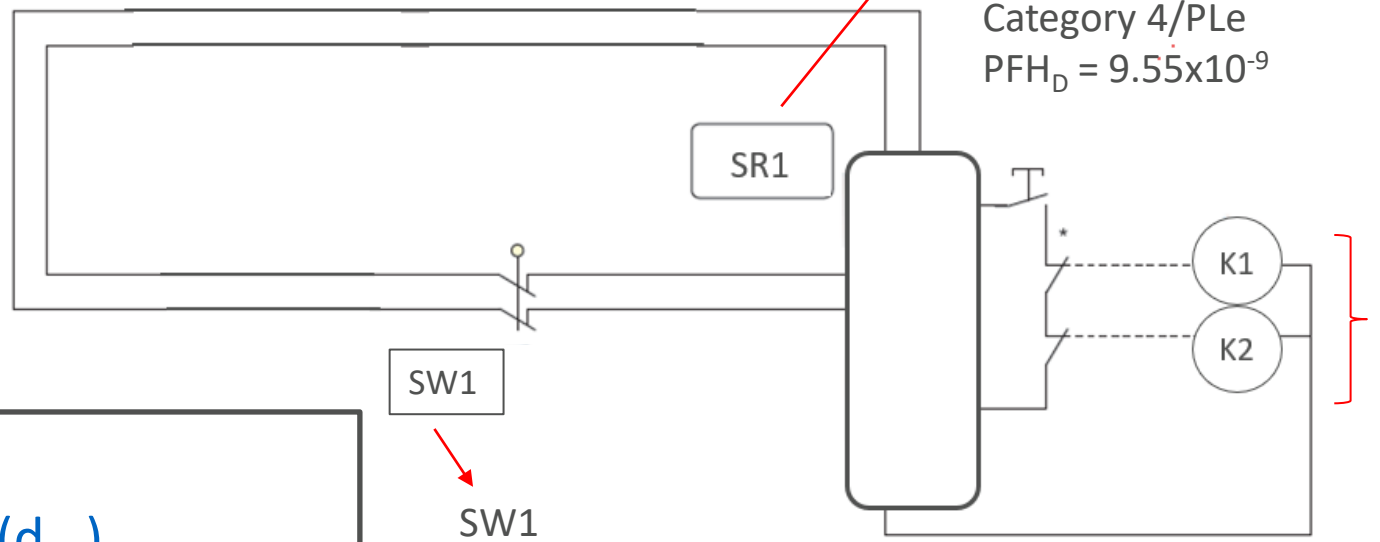
- The overall PL for the safety function is limited by: The component with the *lowest PL* and the PL *Table 2* in corresponding to the total PFH_D.

ISO 13849-1 – Sample Calculation: Determine the PL of the safety function?

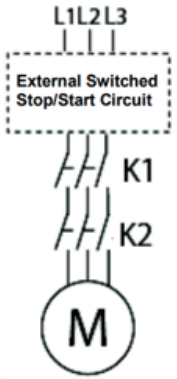
SW1 – Guard Lock Switch

SR1 – Safety Relay

K1/K2 – Motor Contactors



SR1
$MTTF_D$ = 40 years
DC = 99%
Category 4/PLe
$PFH_D = 9.55x10^{-9}$



SW1
Category 1
$B10_D$ = 2,000,000

K1
$B10_{DCon}$ = 20,000,000

K2
$B10_{DCon}$ = 20,000,000

Usage:

- 365 days/year (d_{op})
- 3 shifts (24 hours/day), (h_{op})
- 30 minutes (time between two cycles in seconds), (t_{cycle})
- *Assumption - CCF Score ≥ 65*

Workplace Safety & Prevention Services®

Safety Function block diagram

SW1
Category 1
$B10_D$ = 2,000,000
DC = 0

SR1
$MTTF_D$ = 40 years
DC = 99%
Category 4/PLe
$PFH_D = 9.55x10^{-9}$

K1/K2
$B10_{DCon}$ = 20,000,000
DC = 99%

Contactor DC = 99% (since direct monitoring of electromechanical devices by mechanically linked contact elements) – See Annex Table E.1 for scoring DC

Calculate $MTTF_D$ of SW1

SW1
Category 1
$B10_D$ = 2,000,000

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

$$MTTF_D = \frac{B_{10D}}{0,1 \times n_{op}}$$

[Source: International Organization for Standardization, [ISO] 13849-1 2015, p. 52]

$n_{op} = (d_{op} \times h_{op} \times 3600 \text{ sec/hr}) / (t_{cycle})$

n_{op} = (365 days/year x 24 hrs/day x 3600 sec/h) / (1800 sec)

➢ n_{op} = 17, 520 cycles / year

$MTTF_D = B_{10D} / (0.1 \times n_{op})$

$= 2x10^6 / (0.1 \times 17{,}520) =$ ~1142 years (High)

Usage:

- 365 days/year (d_{op})
- 3 shifts (24 hours/day), (h_{op})
- 30 minutes (time between two cycles in seconds), (t_{cycle})

Table 4 — Mean time to dangerous failure of each channel ($MTTF_D$)

$MTTF_D$	
Denotation of each channel	**Range of each channel**
Low	3 years ≤ $MTTF_D$ < 10 years
Medium	10 years ≤ $MTTF_D$ < 30 years
High	30 years ≤ $MTTF_D$ ≤ 100 years

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Table 4, p. 17]

Calculate $MTTF_D$ of K1

K1
$B10_{DCon}$ = 20,000,000

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

n_{op} = (d_{op} x h_{op} x 3600 sec/hr) / (t_{cycle})

n_{op} = (365 days/year x 24 hrs/day x 3600 sec/h) / (1800 sec)

➤ n_{op} = 17, 520 cycles / year

$$MTTF_D = \frac{B_{10D}}{0,1 \times n_{op}}$$

[Source: International Organization for Standardization, [ISO] 13849-1 2015, p. 52]

$MTTF_D$ = B_{10D} / (0.1 x n_{op})

= $2x10^7$ / (0.1 x 17,520) = ~11,142 years (High)

Usage:

- 365 days/year (d_{op})
- 3 shifts (24 hours/day), (h_{op})
- 30 minutes (time between two cycles in seconds), (t_{cycle})

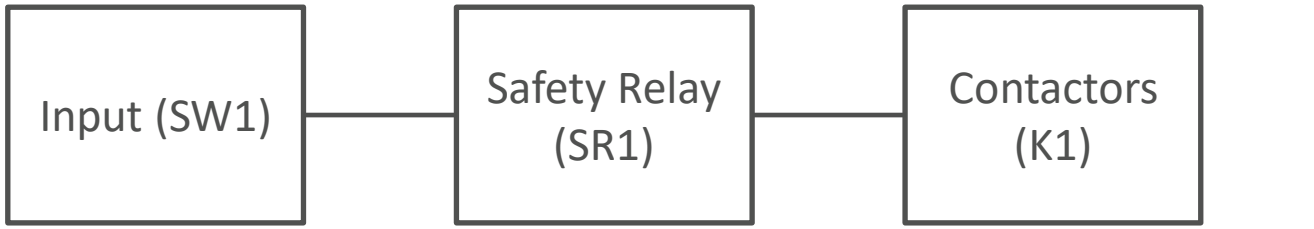
Table 4 — Mean time to dangerous failure of each channel ($MTTF_D$)

Denotation of each channel	$MTTF_D$ Range of each channel
Low	3 years ≤ $MTTF_D$ < 10 years
Medium	10 years ≤ $MTTF_D$ < 30 years
High	30 years ≤ $MTTF_D$ ≤ 100 years

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Table 4, p. 17]

Safety Function block diagram

- Now we know the $MTTF_D$ and DC for each of the components of the safety function
- We can calculate the $MTTF_{DCH}$, DC_{avg}



SW1
Category 1
$B10_D$ = 2,000,000
DC = 0
MTTFD = 1142 years

SR1
$MTTF_D$ = 40 years
DC = 99%
Category 4/PLe
$PFH_D = 9.55x10^{-9}$

K1/K2
$B10_{DCon}$ = 20,000,000
DC = 99%
MTTFD = 11,142 years

$MTTF_{DCH}$ = 38.5 years (medium)

DC_{avg} = 95.7% (medium)

→ PLc

$$\frac{1}{MTTF_D} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{Di}} = \sum_{j=1}^{\tilde{N}} \frac{n_j}{MTTF_{Dj}}$$

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Annex D, p. 56]

$$\frac{1}{MTTF_{DCH}} = \frac{1}{1142\,yrs} + \frac{1}{40\,yrs} + \frac{1}{11,142\,yrs}$$

$MTTF_{DCH} = 38.5\,yrs$ (Medium)

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}} + \ldots + \frac{DC_N}{MTTF_{DN}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}} + \ldots + \frac{1}{MTTF_{DN}}}$$

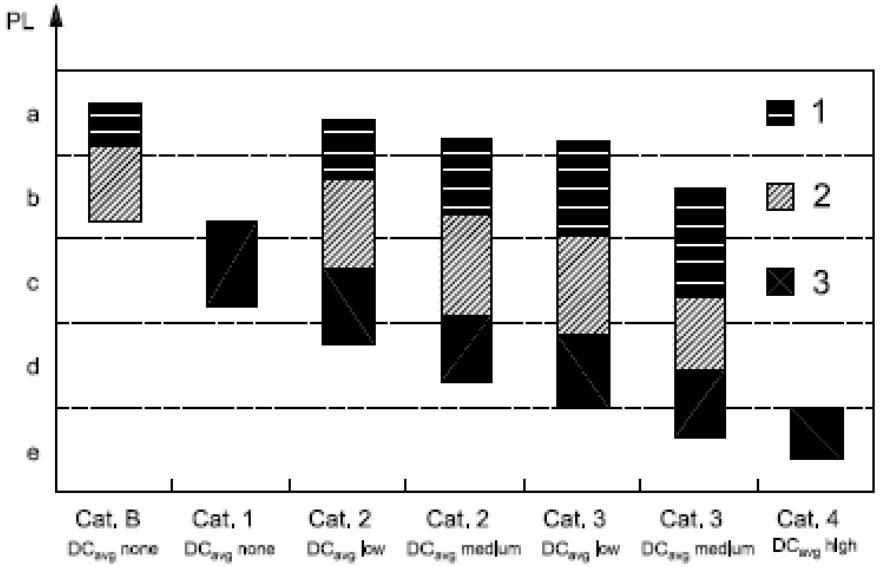
[Source: International Organization for Standardization, [ISO] 13849-1 2015, Annex E, p. 60]

$$DC_{avg} = \frac{\frac{0}{1142} + \frac{99}{40} + \frac{99}{11,142}}{\frac{1}{1142} + \frac{1}{40} + \frac{1}{11,142}}$$

$DC_{avg} = 95.7$ (Medium)

Relationship - Categories, DCavg, MTTFD, and PL

- Fig. 5 shows how the combination of Category, DC_{avg}, $MTTF_D$ (each channel), can be used to estimate PL of a safety function *(simplified approach)*.
- PL can be read off the vertical axis of Fig. 5.



Key

PL	performance level
1	$MTTF_D$ of each channel = low
2	$MTTF_D$ of each channel = medium
3	$MTTF_D$ of each channel = high

Figure 5 — Relationship between categories, DC_{avg}, $MTTF_D$ of each channel and PL

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Table 6, p. 19]

Table 6 — Simplified procedure for evaluating PL achieved by SRP/CS

Category	B	1	2	2	3	3	4
DC_{avg}	none	none	low	medium	low	medium	high
$MTTF_D$ of each channel							
Low	a	Not covered	a	b	b	c	Not covered
Medium	b	Not covered	b	c	c	d	Not covered
High	Not covered	c	c	d	d	d	e

- Notes: If shaded $MTTF_D$ area of applicable vertical bar spans multiple PLs, use Table 6 to find PL.
- For a more precise value of PL based on precise MTTFD see *Annex K, Table K.1 Table*

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Fig 5, p. 19]

Workplace Safety & Prevention Services®

PL vs SIL

Table 3 — Relationship between performance level (PL) and safety integrity level (SIL)

PL	SIL (IEC 61508–1, for information) high/continuous mode of operation
a	No correspondence
b	1
c	1
d	2
e	3

[Source: International Organization for Standardization, [ISO] 13849-1 2015, Table 3, p. 16]

References

- International Electrotechnical Commission (2021). *Safety of machinery – Functional safety of safety-related control systems* (IEC 62061)
- International Organization for Standardization (2015). *Safety of machinery – Safety-related parts of control systems. Part 1 – General principles for design* (ISO 13849-1)

For all your health and safety solutions, contact:

Workplace Safety & Prevention Services

1 877 494 WSPS (9777)

WSPS.CA

CONNECT WITH US

Workplace Safety & Prevention Services®