SIEMENS

Help on the Application of ISO 13849-1

Safety Evaluation with TIA Selection Tool

https://www.siemens.com/safety-evaluation

Siemens Industry Online Support

Table of content

1 Performance Level (PL) and Category (Cat.)

1.1 Performance Level (PL)

Five Performance Levels (PL a to PL e) are defined with specific ranges of probability of a dan-gerous failure per hour (PFH_D):

Table 1-1 Performance Level (PL)

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

The performance level of a safety function is the result of the sum of probabilities of dangerous failure per hour (PFH_D) and the lowest performance level of all safety-related parts of control system (SRP/CS).

The following method applies if the performance level for an individual SRP/CS has to be de-termined based on user data (e.g. actuations):

The maximum achievable performance level is determined by the simplified procedure for evaluating from Table 6 and the average probability of a dangerous failure per hour (PFH_D) from Table K.1 of ISO 13849-1.

Table 1-2

Category	**B**	**1**	**2**	**2**	**3**	**3**	**4**
DC_{avg}	**none**	**none**	**low**	**medium**	**low**	**medium**	**high**
$MTTF_D$ of each channel							
low	a	n.a.	a	b	b	c	n.a.
medium	b	n.a.	b	c	c	d	n.a.
high	n.a.	c	c	d	d	d	e

Safety evaluation in TIA Selection Tool only uses the average probability of a dangerous failure per hour (PFH_D) and the corresponding performance level (PL) according to Table K.1 of ISO 13849-1.

1.2 Category (Cat.) - designated architecture

Table 10 of ISO 13849-1 includes the basic requirements to categories. The user shall ensure that all requirements for a category are fulfilled. Full requirements can be found in clause 6 of ISO 13849-1

As a rule, a Performance Level can only be calculated if the requirements to the $MTTF_D$ of each channel, DC_{avg} and CCF correspond to the selected category.

Table 1-3 Summary of requirements for categories

Cat.	Summary of requirements	System behavior	Principle used to achieve safety	$MTTF_D$ of each channel	DC_{avg}	CCF
B	SRP/CS and/or their protective equipment, as well as their components, shall be designed, constructed, selected, assembled and combined in accordance with relevant standards so that they can withstand the expected influence. Basic safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function.	Mainly characterized by selection of components	Low to medium	None	Not relevant
1	Requirements of B shall apply. Well-tried components and well-tried safety principles shall be used.	The occurrence of a fault can lead to the loss of the safety function but the probability of occurrence is lower than for category B.	Mainly characterized by selection of components	High	None	Not relevant
2	Requirements of B and the use of well-tried safety principles shall apply. Safety function shall be checked at suitable intervals by the machine control system.	The occurrence of a fault can lead to the loss of the safety function between the checks. The loss of safety function is detected by the check.	Mainly characterized by structure	Low to high	Low to medium	See Annex F

Cat.	Summary of requirements	System behavior	Principle used to achieve safety	$MTTF_D$ of each channel	DC_{avg}	CCF
3	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that – a single fault in any of these parts does not lead to the loss of the safety function, and – whenever 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 the loss of the safety function.	Mainly characterized by structure	Low to high	Low to medium	See Annex F
4	Requirements of B and the use of well-tried safety principles shall apply. Safety-related parts shall be designed, so that – a single fault in any of these parts does not lead to a loss of the safety function, and – the single fault is detected at or before the next demand upon the safety function, but that if this detection is not possible, an 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 characterized by structure	High	High including accumulation of faults	See Annex F

2 Diagnosis

2.1 Diagnostic coverage (DC)

The value of the Diagnostic Coverage (DC) is indicated by the following four levels:

Table 2-1 Diagnostic coverage (DC)

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

The table E.1 in Annex E of ISO 13849-1 serves as a guideline for the determination of the Diagnostic Coverage examples for input and output units.

Table 2-2 Examples from ISO 13849-1 for input units

Measure	**Diagnostic Coverage (DC)**
Input device	
Cyclic test stimulus by dynamic change of the input signals	90 %
Plausibility check, e.g. use of normally open and normally closed mechanically linked contacts	99 %
Cross monitoring of inputs without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of input signals with dynamic test if short circuits are not detectable (for multiple I/O)	90 %
Cross monitoring of input signals and intermediate results within the logic (L), and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level e !
Monitoring some characteristics of the sensor (response time, range of analogue signals, e.g. electrical resistance, capacitance)	60 %

Table 2-3 Examples from ISO 13849-1 for output units

Measure	Diagnostic coverage (DC)
Output device	
Monitoring of outputs by one channel without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of outputs without dynamic test	0 % to 99 %, depending on how often a signal change is done by the application
Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)	90 %
Cross monitoring of output signals and intermediate results within the logic (L) and temporal and logical software monitor of the program flow and detection of static faults and short circuits (for multiple I/O)	99 %
Redundant shut-off path with monitoring of the actuators by logic and test equipment	99 %
Indirect monitoring (e.g. monitoring by pressure switch, electrical position monitoring of actuators)	90 % to 99 %, depending on the application
Fault detection by the process	0 % to 99 %, depending on the application; this measure alone is not sufficient for the required performance level e !
Direct monitoring (e.g. electrical position monitoring of control valves, monitoring of electromechanical devices by mechanically linked contact elements)	99 %

3 Reliability

3.1 Mean time to dangerous failure of each channel ($MTTF_D$) and component quality (B_{10D})

For each SRP/CS (subsystem) according to Table 4 of ISO 13849-1, the maximum value of $MTTF_D$ for each channel is 100 years. For Category 4 SRP/CS (subsystems) the maximum value of $MTTF_D$ for each channel is increased to 2 500 years. The $MTTF_D$ value of each channel is indicated by the following three levels:

Table 3-1 Mean time to dangerous failure of each channel (MTTFD)

$MTTF_D$	
Detonation 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

The B_{10D} value is determined based on B_{10} (Number of cycles until 10 % of the components fail) and the ratio of dangerous failures (%):

B10D = B10 / ratio of dangerous failures.

Remark: If only the B10D value is known, it can be entered directly into the B10 input screen form, and the ratio of dangerous failures can be set to 100%.

The $MTTF_D$ for wear-prone components is determined based on B_{10D} and the number of actua-tions per year.

The calculation is based on the following assumptions:

1 day = 24 hours; 1 week = 7 days; 1 month = 30 days; 1 year = 365 days.

The following Table C.1 of ISO 13849-1 indicates possible value ranges for B_{10D} and $MTTF_D$ and further relevant standards.

Important note: The information provided by the component manufacturer shall always have pri-ority over the values indicated in the following Table C.1 of ISO 13849-1.

Table 3-2 International Standards dealing with $MTTF_D$ or B_{10D} for components

	Basic and well-tried safety principles according to ISO 13849-2:2003	**Other relevant standards**	**Typical values: $MTTF_D$ (years) B_{10D} (cycles)**
Mechanical components	Tables A.1 and A.2	–	$MTTF_D$ = 150
Hydraulic components with n_{op} ≥ 1 000 000 cycles per year	Tables C.1 and C.2	ISO 4413	$MTTF_D$ = 150
Hydraulic components with 1 000 000 cycles per year > n_{op} ≥ 500 000 cycles per year	Tables C.1 and C.2	ISO 4413	$MTTF_D$ = 300
Hydraulic components with 500 000 cycles per year > n_{op} ≥ 250 000 cycles per year	Tables C.1 and C.2	ISO 4413	$MTTF_D$ = 600
Hydraulic components with 250 000 cycles per year > n_{op}	Tables C.1 and C.2	ISO 4413	$MTTF_D$ = 1 200
Pneumatic components	Tables B.1 and B.2	ISO 4414	B_{10D} = 20 000 000
Relays and contactor relays with small load	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B_{10D} = 20 000 000
Relays and contactor relays with nominal load	Tables D.1 and D.2	EN 50205 IEC 61810 IEC 60947	B_{10D} = 400 000
Proximity switches with small load	Tables D.1 and D.2	IEC 60947 SIO 14119	B_{10D} = 20 000 000
Proximity switches with nominal load	Tables D.1 and D.2	IEC 60947 ISO 14119	B_{10D} = 400 000
Contactors with small load	Tables D.1 and D.2	IEC 60947	B_{10D} = 20 000 000
Contactors with nominal load	Tables D.1 and D.2	IEC 60947	B_{10D} = 1 300 000 (see Note1)
Position switches [a]	Tables D.1 and D.2	IEC 60947 ISO 14119	B_{10D} = 20 000 000
Position switches (with separate actuator, guard-locking) [a]	Tables D.1 and D.2	IEC 60947 ISO 14119	B_{10D} = 2 000 000
Emergency stop devices [a]	Tables D.1 and D.2	IEC 60947 ISO 13850	B_{10D} = 100 000
Push buttons (e.g. enabling switches) [a]	Tables D.1 and D.2	IEC 60947	B_{10D} = 100 000

NOTE 1 B10D is estimated as two times B10 (50 % dangerous failure) if no other information (e.g. product standard) is available.

NOTE 2 “Nominal load” or “small load” should take into account safety principles described in ISO 13849-2, like over-dimensioning of the rated current value. “Small load” means, for example, 20 %.

NOTE 3 Emergency stop devices according to IEC 60947–5-5 and ISO 13850 and enabling switches according to IEC 60947–5-8 can be estimated as a Category 1 or Category 3/4 subsystem depending on the number of electrical output contacts and on the fault detection in the subsequent SRP/CS. Each contact element (including the mechanical actuation) can be considered as one channel with a respective B10D value. For enabling switches according to IEC 60947–5-8 this implies the opening function by pushing through or by releasing. In some cases it may be possible, that the machine builder can apply a fault exclusion according to ISO 13849-2, Table D.8, considering the specific application and environmental conditions of the device.

[a] If fault exclusion for direct opening action is possible.

4 Resistence

4.1 Estimation of susceptibility to common cause failures (CCF)

As from Category 2, measures for the prevention of CCF must be considered.

Based on Table F.1 of ISO 13849-1, the different measures can be assigned points for appraisal (also refer to “Determining the CCF”).

For the CCF prevention measures to be fulfilled, the total score must be >= 65 points.

If a total of < 65 has been determined, the measures for the prevention of CCF are not fulfilled. Therefore, the category requirements are not fulfilled either and no performance level can be determined or no statement is possible.