Help on the Application of IEC 62061

Safety Evaluation with TIA Selection Tool

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

Siemens Industry Online Support

Table of content

1 Safety Integrity and architecture

1.1 Safety Integrity Level (SIL)

Three Safety Integrity Level (SIL1, SIL 2 and SIL 3) are defined with specific areas of Probability of dangerous Failure per Hour (PFHD):

Table 1-1 1.1 Safety Integrity Level (SIL)

Safety Integrity Level (SIL)	Probability of dangerous Failure per Hour 1/h (PFH_D)
3	≥ 10^{-8} bis < 10^{-7}
2	≥ 10^{-7} bis < 10^{-6}
1	≥ 10^{-6} bis < 10^{-5}

The Safety Integrity Level of a safety function is a result of the sum of probabilities of a danger-ous failure per hour (PFHD) and the least significant SIL CL of all subsystems.

1.2 Architectural constraints on subsystems (SIL CL)

The maximal SIL of a subsystem that can be claimed is indicated with SIL CL (SIL claim limit), i.e. the so-called SIL suitability. The SIL CL depends on:

- the architecture,
- the Safe Failure Fraction (SFF) and,
- indirectly, the diagnosis.

A 1-channel architecture corresponds to a Hardware Failure Tolerance (HFT) of 0, and a 2-channel architecture corresponds to a Hardware Failure Tolerance (HFT) of 1.

Example, HFT = 0

- 1 component (1-channel mechanical and electrical, one position switch)

Examples, HFT = 1

- 2 components (2-channel mechanical and electrical, two position switches)
- 1 component (1-channel mechanical and 2-channel electrical, emergency stop device).

The Safe Failure Fraction (SFF) depends on the Diagnostic Coverage (DC).

Table 1-2 Architectural constraints on subsystems (SIL CL)

Safe Failure Fraction (SFF)	Hardware Fault Tolerance (HFT)		
	0	1	2
< 60%	Not allowed (see remark)	SIL 1	SIL 2
60% bis < 90%	SIL 1	SIL 2	SIL 3
90% bis < 99%	SIL 2	SIL 3	SIL 3
≥ 99%	SIL 3	SIL 3	SIL 3

Remark: SIL 1 can be achieved with proven components (e.g. position switch, emergen-cy stop control device, and contactor) in accordance with ISO 13849-1.

SIL CL can be structurally constrained to SIL 2 if fault exclusions have been applied which can lead to a dangerous failure of the subsystem.

Example: A position switch with a separate actuator (1 component) evaluated on an electrical 2-channel basis.

Exception: SIL 3 can be principally achieved with an emergency stop control device, evaluated on an electrical 2-channel basis.

2 Diagnosis

2.1 Diagnostic Coverage (DC)

To estimate the Diagnostic Coverage, Table E.1 of ISO 13849-1 can be used alternatively for reference purposes.

Examples from Table E.1 of ISO 13849-1 for input and output units:

Table 2-1 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 2-2 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 Dangerous failure rate (λ_D) and component quality (B_{10})

The dangerous failure rate (λ_D) for wear-prone components is determined using the B_{10} value (the expected time at which 10% of the population will fail), the ratio of dangerous failures (%) and the number of actuations per hour.

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 shows possible value ranges for B_{10D} ($B_{10D} = B_{10}$ / ratio of dangerous failures) and $MTTF_D$ and a list of further relevant standards.

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

Table 3-1 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.

3.2 Proof test interval or lifetime (T1)

The validity of the safety characteristics is principally assumed for the period T1.

The T1 value is the lower value of the interval for the proof test or the lifetime: The test per-formed in order to prove the “as-new-state” of a subsystem is referred to as “proof test”, and the permissible period of use is referred to as the “lifetime”.

In most cases, the T1 value can be assumed with the lifetime of the component used.

4 Resistance

4.1 Estimation of susceptibility to Common Cause Failures (CCF)

For a 2-channel architecture or higher, CCF measures must be considered.

Table F.1 of IEC 62061 can be used for the evaluation of the different measures based on points (see also “Determining the CCF”).

The determined total score then serves as a basis for the assessment of the Common Cause Failure factor (CCF factor or β) in accordance with the information specified in Table F.2 of IEC 62061.

This CCF factor can be 10%, 5%, 2% or 1%.

Remark: It is recommended to assume a 10% CCF factor first. A reduction of the CCF factor leads to an improvement of the PFHD; this must be proven in accordance with Table F.1 of IEC 62061.