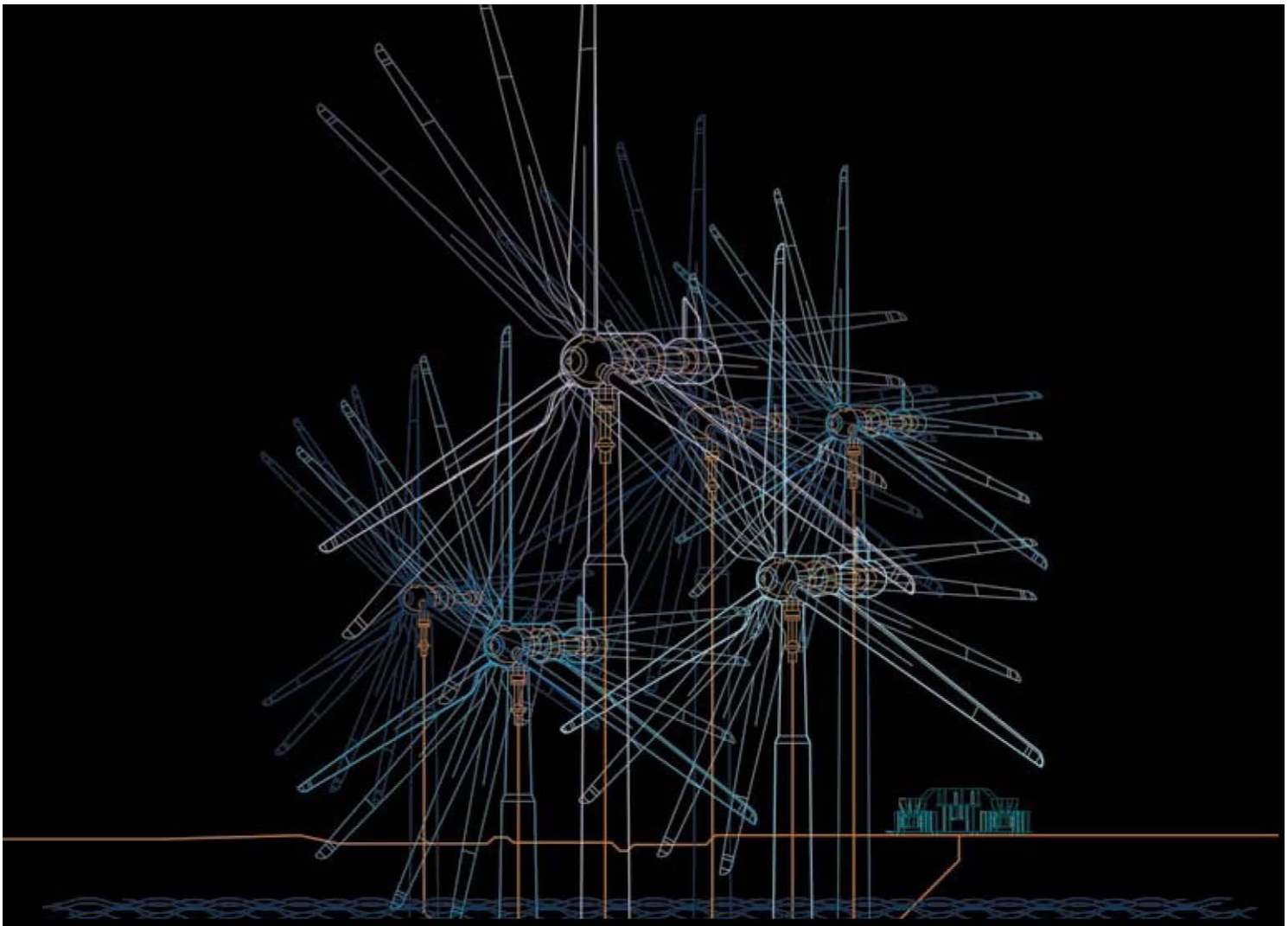


ABB Automation Products

Functional safety and reliability data

2CMT2016-005511 rev 2019-01-xx – Functional safety and reliability data:– Issued by SECRL Krister Linnarud (e-mail: krister.linnarud@se.abb.com)
This document replaces 2CMT002548 2018

Power and productivity for a better world™

Table of Contents

1 Purpose of this document

This document contains functional safety and reliability data that can be used for functional safety and availability calculations.

For all the aspects below, the reader can decide whether it is applicable for his/her situation or not. The values in this document is typical values for normal applications. Depending of the application (ambient air temperature, loads, switching frequency, altitude, humidity, pollution degree, shock and vibration and mounting position etc), the values could differ. The document will be regularly updated and extended to include other ABB products.

The information in this document is also based on recent CAPIEL advices se 5 other references

This document is valid for ABB AF and NF range of contactors

2 Normal B_{10D} Values (operating in high or continuous demand mode)

Safety characteristics

In the following standards, the so-called B_{10D} values for calculating the safety integrity or safety integrity level (SIL) in functional safety at a high or continuous demand rate are required also for electromechanical switchgear:

• IEC 62061 "Safety of machines – Functional safety of safety related electrical, electronic and programmable electronic control systems",

• ISO 13849-1 "Safety of machines – Safety-related components of controls – Part 1: General principles".

Failure rates of electromechanical components are required for calculating the safety integrity or safety integrity level (SIL) in functional safety:

- in the manufacturing industry at a high demand rate
- in the process industry at a low demand rate

Further requirements are laid down in IEC 61511-1 "Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements".

The European versions of the above standards are:

- EN 62061
- EN ISO 13849-1
- EN 61511-1

Table 2 – Typical B_{10D} values for electromechanical components (operating in high or continuous demand mode)

A failure to open the circuit is considered as a dangerous failure in this table.
Values are based on tests made in laboratories by ABB or CAPIEL manufacturers.
The values given are target values that typical components are expected to achieve based on testing, which can be used if the supplier has not provided a value. It is the responsibility of the manufacturer to provide the actual values.
If detailed information about specific product is needed, please contact ABB.

Electromechanical components	**Contact load, utilization category**	**Typical B_{10} values**	**Typical B_{10D} values**	**RDF**	
(only devices with positive opening contacts allowed)					
EMERGENCY STOP DEVICES (push buttons) - Turn-to-release (and key release) - Pull-to-release	1) 1)	20 000 20 000	100 000 100 000	20% 20%	
Cable-operated switches for EMERGENCY STOP function	1)	20 000	100 000	20%	
Hinge switches	1)	20 000	100 000	20%	
Pushbuttons (momentary)	2)	20 000	100 000	20%	4)
Position Switches - Standard version - with separate actuator - with solenoid interlocking, spring forced lock	2) 1) 1)	4 00 000 400 000 200 000	20 000 000 2 000 000 1 000 000	20% 20% 20%	4) 4) 4)
-Contactor Relays	3) AC-15/-14	10 000 000 200 000	20 000 000 400 000	50% 50%	5) 6)
Contactors / Motor Starters - for motorswitching ≤ 100A	3) AC-3	10 000 000 1 000 000	20 000 000 1 300 000	50% 73%	5) 6)
Contactors / Motor Starters - for motorswitching >100A, ≤205A	3) AC-3	5 000 000 1 000 000	10 000 000 1300 000	50% 73%	5) 6)
Contactors / Motor Starters - for motorswitching >205A, ≤370A	3) AC-3	3 000 000 1 000 000	6 000 000 1300 000	50% 73%	5) 6)
Contactors / Motor Starters - for motorswitching >370A, ≤460A	3) AC-3	2 000 000 500 000	4 000 000 680 000	50% 73%	5) 6)
Contactors / Motor Starters - for motorswitching >460A, ≤750A	3) AC-3	1 000 000 500 000	2 000 000 680 000	50% 73%	5) 6)
Contactors / Motor Starters - for motorswitching >750A	3) AC-3	400 000 50 000	800 000 68 000	50% 73%	5) 6)

		1) mainly limited by mechanical wear 2) mainly limited by contact wear 3) maximum value of B_{10} if the current is lower than 1% of rated value (Ie) 4) Ratio of dangerous failure: 50% at usage of the NO contact (one positively driven contact shall be used additionally at least in a redundant architecture ; the single use of a NO contact is not allowed) 5) The diagnostic coverage of the subsystem incorporating a contactor with mirror contacts can be 99% if an appropriate fault reaction function(s) is provided 6) The values given are based on 50% of Ie (based on the common practice for output devices used in safety related systems)

The B_{10D} value used in ISO 13849-1:2016 can be determined as follows:
B_{10D}= B_{10}/*ratio of dangerous failure*
Ratio of dangerous failures is minimum 20%

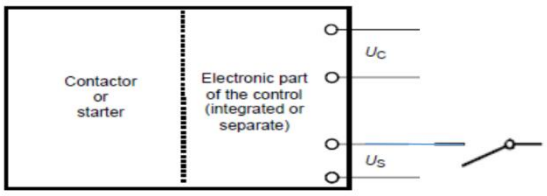
3 Safety elements

Safety evaluation of electromechanical devices containing electronics:

1. If the electronics has no impact on the safety integrity, the device is considered to be a mechanical device only. (B_{10D})

   Example: Contactor with electronic controlled coil

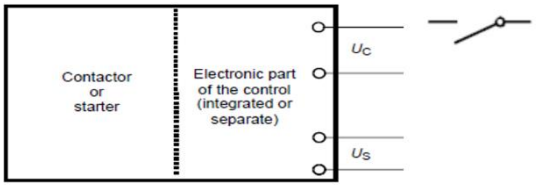
   The position of rest for a contactor is the safe state, and the magnet cannot be kept closed without supply voltage.



2. If the electronics does have an impact on the safety integrity, both the mechanical part and the electronic part have to be considered. ($MTTF_D$+B_{10D} or λ_D)

   Example: Contactor with electronic controlled coil

   The magnet is operated through the electronic.



U_c= control voltage
U_s= supply voltage

4 Standard Failure Rates operating in low demand mode

On the basis of the failure rates, it is possible to calculate the average probability of failure on demand (PFDavg) of a PLT protective device.
A so-called low demand rate is assumed, meaning the rate of demand on the safety-related system amounts to no more than once a year and is not greater than double the frequency of the repeat test.
A repeat test once a year is recommended for electromechanical components in order to reveal passive faults.

For special applications it is possible, in agreement with the inspecting institution (e.g. a technical inspectorate, government agency or the like) to extend the test intervals by using suitable solutions (e.g. a multi-channel version etc.).

Table contains general data based on functional safety and reliability calculations done by ABB for product groups. If detailed information about specific product is needed, please contact ABB.

Table 2 - Normal failure rates for ABB Automation Products' electromechanical and electrical components (operating in low demand mode)

ABB Automation Products' product group	Normal failure rate (FIT)	Ratio of dangerous failures	Safety function

Emergency stop control devices	100	20%	Circuit disconnected when actuated
Pushbuttons	100	20%	Circuit disconnected when actuated
Softstarter	200	20%	Disconnecting the motor at overload
Contactors	100	40%	Main circuit disconnected after the coil is de-energised in a given time
Motor starters	100	40%	Main circuit disconnected after the coil is de-energised in a given time

5 Normative references

EN ISO 13849-1:2016 , Safety of machinery — Safety-related parts of control systems — Part 1: General principles for design

EN ISO 13849-2:2012 Safety of machinery - Safety-related parts of control systems - Part 2: Validation

IEC 61508:2010 (all parts), Functional safety of electrical/electronic/programmable electronic safety-related systems

IEC 62061:2005/AMD2:2015 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

IEC 60947-4-1:2018 Edition 4 : Annex K: Low-voltage switchgear and controlgear – Part 4-1 Contactors and Motor-starters – Electromechanical contactors and motor-starters
IEC 61511-1:2016 Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming requirements

EU Harmonized standards:

MD **Directive 2006/42/EC - *OJ C 173 of 13/05/2016***

B-type standards CEN

EN ISO 13849-1:2015 Safety of machinery - Safety-related parts of control systems - Part 2: Validation (ISO 13849-2:2012)

EN ISO 13850:2015 Safety of machinery - Emergency stop function - Principles for design (ISO 13850:2015)

B-type standards CENELEC

EN 62061:2005/A2:2015 IEC 62061:2005/A2:2015	15/01/2016

Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

C-type standards

EN 60947-5-5:1997/A2:2017 IEC 60947-5-5:1997/A2:2016	09/06/2017

Low-voltage switchgear and controlgear - Part 5-5: Control circuit devices and switching elements - Electrical emergency stop device with mechanical latching function

6 Other references.

CAPIEL: Low voltage switchgear and controlgear - functional safety aspects

Functional safety is an important part of machine safety. The European Machinery Directive together with the harmonized standards EN 62061 and EN ISO 13849-1 gives the requirements.
This brochure provides information concerning the application of these standards and the European Machinery Directive, relevant to the implementation of low voltage switchgear and control gear in functional safety applications. Together with important facts it gives examples of low and high demand mode.
http://www.capiel.eu/data/6686-Capiel-low-Voltage-EN-version.pdf
http://www.capiel.eu/data/6686-Capiel-low-Voltage-DE-version.pdf

CAPIEL: Functional Safety

"Functional Safety is a subject that is important in many areas such as machine safety and process safety. CAPIEL products are used in this type of applications, This presentation explains the basics of Functional Safety."

http://www.capiel.eu/data/5-2-FunctionalSafety-Basic-2014-05-13.pdf

CAPIEL WHITE PAPER Edition 2 2016-12-10

Low voltage switchgear and control gear - safety aspects

Annex A Hardware fault tolerance

The HFT values for our products can be calculated based on the below described guidance according to the international standards.

IEC 61511-1:2016 **11.4.4** When determining the achieved HFT, certain faults may be excluded, provided that the likelihood of them occurring is very low in relation to the safety integrity requirements.
Any such fault exclusions shall be justified and documented.
NOTE Further information about fault exclusion can be found in ISO13849-1:2006 and ISO13849-2:2012

Note: the hardware fault tolerance of table 6 in DIN IEC 61511-1 may be reduced by one if requirements according to IEC 61511, 11.4.4 are fulfilled.

11.4.5 The minimum HFT for a SIS (or its SIS subsystems) implementing a SIF of a specified SIL shall be in accordance with Table 6 and if appropriate 11.4.6 and 11.4.7.

NOTE The HFT requirements in Table 6 represent the minimum system or, where relevant, the SIS subsystem redundancy. Depending on the application, device failure rate and proof-testing interval, additional redundancy can be required to satisfy the failure measure for the SIL of the SIF according to 11.9.

Table 6 – Minimum HFT requirements according to SIL

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (high demand or continuous mode)	1
3 (any mode)	1
4 (any mode)	2

11.4.6 For a SIS or SIS subsystem that does not use FVL or LVL programmable devices and if the minimum HFT as specified in Table 6, would result in additional failures and lead to decreased overall process safety, then the HFT may be reduced. This shall be justified and documented. The justification shall provide evidence that the proposed architecture is suitable for its intended purpose and meets the safety integrity requirements.

NOTE Fault tolerance is the preferred solution to achieve the required confidence that a robust architecture has been achieved. When 11.4.6 applies, the purpose of the justification is to demonstrate that the proposed alternative architecture provides an equivalent or better solution. This may vary depending on the application and/or the technology in use; examples include: back-up arrangements (e.g., analytical redundancy, replacing a failed sensor output by physical calculation results from other sensors outputs); using more reliable items of the same technology (if available); changing for a more reliable technology; decreasing common cause failure impact by using diversified technology; increasing the design margins; constraining the environmental conditions (e.g. for electronic components); decreasing the reliability uncertainty by gathering more field feedback or expert judgment.

EN ISO 13849-1:2016 (E)

7 Fault consideration, fault exclusion

…

7.3 Fault exclusion

It is not always possible to evaluate SRP/CS without assuming that certain faults can be excluded. For detailed information on fault exclusions, see ISO 13849‑2.
Fault exclusion is a compromise between technical safety requirements and the theoretical possibility of occurrence of a fault.
Fault exclusion can be based on
— the technical improbability of occurrence of some faults,
— generally accepted technical experience, independent of the considered application, and
— technical requirements related to the application and the specific hazard.
If faults are excluded, a detailed justification shall be given in the technical documentation.

IEC 61508-2 table 2 for safety related subsystems type A

Table 2 – Maximum allowable safety integrity level for a safety function carried out by a type A safety-related element or subsystem

Safe failure fraction of an element	Hardware fault tolerance		
	0	1	2
< 60 %	SIL 1	SIL 2	SIL 3
60 % – < 90 %	SIL 2	SIL 3	SIL 4
90 % – < 99 %	SIL 3	SIL 4	SIL 4
≥ 99 %	SIL 3	SIL 4	SIL 4

NOTE 1 This table, in association with 7.4.4.2.1 and 7.4.4.2.2, is used for the determination of the maximum SIL that can be claimed for a subsystem: given the fault tolerance of the subsystem and the SFF to the elements used.

i. For general application to any subsystem see 7.4.4.2.1.

ii. For application to subsystems comprising elements that meet the specific requirements of 7.4.4.2.2. To claim that a subsystem meets a specified SIL directly from this table it will be necessary to meet all the requirements in 7.4.4.2.2.

NOTE 2 The table, in association with 7.4.4.2.1 and 7.4.4.2.2,can also be used:

i. For the determination of the hardware fault tolerance requirements for a subsystem given the required SIL of the safety function and the SFFs of the elements to be used.

ii. For the determination of the SFF requirements for elements given the required SIL of the safety function and the hardware fault tolerance of the subsystem.

NOTE 3 The requirements in 7.4.4.2.3 and 7.4.4.2.4 are based on the data specified in this table and Table 3.

NOTE 4 See Annex C for details of how to calculate safe failure fraction.

EN-ISO 13849-2:2012

Table D.3 — Well-tried components

Well-tried component	Additional conditions for "well-tried"	Standard or specification
Switch with positive mode actuation (direct opening action), e.g.: — push-button; — position switch; — cam-operated selector switch, e.g. for mode of operation	—	IEC 60947-5-1:2003, Annex K
Emergency stop device	—	ISO 13850 IEC 60947-5-5
Fuse	—	IEC 60269-1
Circuit-breaker	—	IEC 60947-2
Switches, disconnectors	—	IEC 60947-3
Differential circuit-breaker/RCD (residual current device)	—	IEC 60947-2:2006, Annex B

Table D.3 *(continued)*

Well-tried component	Additional conditions for "well-tried"	Standard or specification
Main contactor	Only well-tried if a) other influences are taken into account, e.g. vibration, b) failure is avoided by appropriate methods, e.g. overdimensioning (see Table D.2), c) the current to the load is limited by the thermal protection device, and d) the circuits are protected by a protection device against overload. NOTE Fault exclusion is not possible.	IEC 60947-4-1
Control and protective switching device or equipment (CPS)	—	IEC 60947-6-2
Auxiliary contactor (e.g. contactor relay)	Only well-tried if a) other influences are taken into account, e.g. vibration, b) there is positively energized action, c) failure is avoided by appropriate methods, e.g. overdimensioning (see Table D.2), d) the current in the contacts is limited by a fuse or circuit-breaker to avoid the welding of the contacts, and e) contacts are positively mechanically guided when used for monitoring. NOTE Fault exclusion is not possible.	EN 50205 IEC 60947-5-1 IEC 60947-4-1:2001, Annex F

Annex B

4 Information needed for safety verification process

For each implementation level, different data is required in order for the machine manufacturer to verify the required PL/SIL of the safety functions.
The following table shows the data required.

Information to be provided by product manufacturer	Implementation levels							
	Safety control system		Safety subsystem		Safety element		Generic element	
	TB	WB	TB	WB	TB	WB	TB	WB
SIL and/or PL	■	■						
SILCL and/or PL			■	■				
PFH_D and/or PFD	■	■	■	■				
Operation limit		1)		1)		2)		2)
$MTTF_D$ or MTTF and RDF					■			
B_{10D} or B_{10} and RDF						■		
MTBF							■	
B_{10}								■
T_M	■	■	■	■	■	■	■	■

■ *Mandatory field, data required,*
■ *Optional field, data optional (application-specific),*

TB *Time based, e.g. electronic products*
WB *Wear based, e.g. electro-mechanical products*

PL *Performance Level (EN ISO 13849)*
SIL *Safety Integrity Level (EN 61508)*
SILCL *Safety Integrity Level Claim Limit (EN 62061)*
PFH_D *Probability Failure per Hour (EN 62061)*
T_M *Mission time (EN ISO 13849)*
MTBF *Mean Time Between Failure (EN ISO 13849)*

$MTTF_d$ *Mean Time To Dangerous Failure (EN ISO 13849)*
RDF *Ratio of Dangerous Failures*
B_{10} *10% of the devices failed (EN ISO 13849)*
B_{10d} *10% of the devices failed dangerous (EN ISO 13849)*
PFD *Probability of failure on Demand (EN 61511)*
Operation limit *maximum number of operations that is used in the calculation on the PFH_D*

1) PFH_D value valid up to the operation limits of the different components
Example: electrical life time, number operations per hour, 50% of nominal current
2) Operation limits as declared by the manufacturer

1) Note: subsystem elements corresponding to the CAPIEL Brochure are safety elements (with safety related date) and generic elements (without safety related data)

Annex C Formulas and Definitions

Formulas

λ	**λ *(t) dt*** is the probability that a unit which has not failed by a certain time *t* will fail in the following interval (*t; t +dt*). Failure rates have the dimension 1/time unit, e.g. 1/h.
B_{10D}	Number of cycles until 10 % of the components fail dangerously (for pneumatic and electromechanical components) *EN ISO 13849-1 Annex C* B_{10D} = B_{10} / ratio of dangerous to all failures as a percentage
MTTF	Mean time to failure • The mean value of this exponential distribution is also referred to as: - Mean Time To Failure (MTTF) in the case of irreparable components; 63 % of components fail by the MTTF. - Mean Operating Time Between Failures (MTBF) in the case of reparable components. • MTTF = 1/λ (MTTF is a statistical mean value but no guarantee for endurance) Electromechanical components are often irreparable components. In general, the failure rate of monitored units changes with age. $MTTF_D$ = MTTF / ratio of dangerous to all failures as a *EN ISO 13849-1 Annex C*
$MTTF_D$	$MTTF_D$ = MTTF / ratio of dangerous to all failures as a
FIT	Failure in Time Unit for expressing the expected failure rate of semiconductors and other electronic devices. One FIT equals one failure per billion (10^9) hours (once in about 114155 years) and is statistically projected from the results of accelerated test procedures. (http://www.businessdictionary.com/definition/failure-in-time-FIT.html) **FIT** Failure rates for components are often specified in FIT (failures in time unit): 1 FIT equals 10-9/h. From the failure rate it is possible to derive a (mathematical) distribution function of the failure probability: F(t) = 1 - exp(-λt), with λ as constant failure rate
□ DC **CCF**	**6.3.2 Basic characteristics of a subsystem** The PL/SIL of a subsystem shall be determined using the methods described in Clause 7. This requires the consideration of the following aspects: □ Category (architecture) (see 7.4); □ DC (see Annex E); □ CCF (see Annex F); □ MTTFd or λd or B10d value for single subsystem element (see 7.3.4.1 and Annex C); □ Behaviour of the safety function under fault condition(s) (see 7.3.3); □ Safety-related software (see Clause 8 and Annex J); □ Systematic failure (see 7.3.2); □ The ability to perform a safety function under expected environmental

	conditions.
FIT	FIT (Failures in Time) is a standard industry value defined as the Failure Rate (λ) per billion hours. 9 FIT = λFIT = λhours ×10 • MTTF (Mean Time to Failure or θ) is another standard industry value which provides the average time to failure of Non-repairable Items such as light bulbs and diodes or unserviceable systems such as satellites or other unmanned space craft. For items with long life expectancies, it is often a more useful to report MTTF in years rather than hours. hours MTTFhours λ = 1 or (24 365) 1 × × = hours MTTFyears λ • MTBF (Mean Time between Failures) is used to describe Repairable Items such as compressors and aircraft. MTBF uses MTTF as one factor and Mean Time to Repair (MTTR) as the other to capture the complete break-down and repair cycle. The primary purpose of MTBF is to identify appropriate preventive maintenance schedules to avoid, perhaps indefinitely, catastrophic failures due to predictable piece part wear-out. As a rule of thumb, component reliability centers around MTTF since most components cannot be repaired. MTBF is shown by: MTBF = MTTF + MTTR where: MTTR is the Mean Time to Repair. Reliability Calculation Tools Over the years, there have been several methods used to derive the value for X2 (Chisquared); everything from the use of probability tables to the application of
PFHD	PFHD average probability of dangerous failure per hour EN ISO 13849-1 Table 3 and Table K.1 PFHD Probability of Dangerous failure per hour λ Failure Rate λs Safe Failure Rate λD Dangerous Failure Rate C Number of operations per year λ = 1/MTTF λ = 0,1 x C/B10 λ = λs + λD λD = 1/MTTFD PFHD = λD x 1h = 1/MTTFD x 1h Ref: IEC 62061 / ISO 13849:
	Relationship of relevant parameters For subsystem elements constant failure rates (λ) of the subsystem elements are assumed. The following basic equations can be used:

$$\lambda = \frac{1}{\mathrm{MTTF}} \quad (1)$$

$$\lambda_D = \frac{1}{\mathrm{MTTF_D}} \quad (2)$$

MTTF and $MTTF_D$ are mostly indicated in years [a]. λ values are commonly indicatedinFIT (FIT = Failure In Time) where 1 FIT means one failure in 10^9 hours.

$$1\ \mathrm{FIT} = 1 \cdot 10^{-9}\mathrm{h}^{-1} \quad (3)$$

One year is approximately 8760 hours. Therefore a MTTF value can be converted into a λ value.

$$\lambda = \frac{1}{\mathrm{MTTF} \cdot 8760\frac{\mathrm{h}}{\mathrm{a}}} \quad (4)$$

NOTE Example, MTTF = 1000a:

$$\lambda, \mathrm{example} = \frac{1}{1000\mathrm{a} \cdot 8760\,\frac{\mathrm{h}}{\mathrm{a}}}$$

$$\lambda, \mathrm{example} = \frac{1}{8760000\mathrm{h}}$$

$$\lambda, \mathrm{example} = \frac{1}{8760000}\,\mathrm{h}^{-1}$$

With B_{10D} and n_{op}, the mean number of annual operations, $MTTF_D$ for components can be calculated as

$$\mathrm{MTTF_D} = \frac{\mathrm{B_{10D}}}{0{,}1 \cdot \mathrm{n_{op}}} \quad (5)$$

where

$$\mathbf{n_{op}} = \frac{\mathbf{d_{op}} \cdot \mathbf{h_{op}} \cdot \mathbf{3600}\ \frac{\mathbf{s}}{\mathbf{h}}}{\mathbf{t_{cycle}}}$$

h_{op} is the mean operation, in hours per day;

d_{op} is the mean operation, in days per year;

t_{cycle} is the mean time between the beginning of two successive cycles of the component. (e.g. switching of a valve) in seconds per cycle.

In terms of failure rate λ the following relationship can be expressed as

$$\lambda_D = \frac{0{,}1 \cdot C}{B_{10D}} = \frac{0{,}1 \cdot n_{op}}{B_{10D} \cdot 8760\,\frac{h}{a}} \quad (7)$$

where C ($C = n_{op} / 8760$) is the duty cycle or mean operation per hour

The relation between B_{10D}, B_{10} and the ratio of dangerous failure (RDF) is

$$\mathrm{B_{10D}} = \frac{\mathrm{B_{10}}}{\text{ratio of dangerous failure}}$$

Definitions

1.1 safety–related part of a control system SRP/CS

part of a control system that responds to safety-related input signals and generates safety-related output signals

Note 1 to entry: The combined safety-related parts of a control system start at the point where the safety-related input signals are initiated (including, for example, the actuating cam and the roller of the position switch) and end at the output of the power control elements (including, for example, the main contacts of a contactor).

Note 2 to entry: If monitoring systems are used for diagnostics, they are also considered as SRP/CS.

1.2 category

classification of the safety-related parts of a control system in respect of their resistance to faults and their subsequent behaviour in the fault condition, and which is achieved by the structural arrangement of the parts, fault detection and/or by their reliability

1.3 fault

state of an item characterized by the inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources

Note 1 to entry: A fault is often the result of a failure of the item itself, but may exist without prior failure.

Note 2 to entry: In this part of ISO 13849, “fault” means random fault.

[SOURCE: IEC 60050‑191:1990, 05-01.]

1.4 failure

termination of the ability of an item to perform a required function

Note 1 to entry: After a failure, the item has a fault.

Note 2 to entry: “Failure” is an event, as distinguished from “fault”, which is a state.

Note 3 to entry: The concept as defined does not apply to items consisting of software only.

Note 4 to entry: Failures which only affect the availability of the process under control are outside of the scope of this part of ISO 13849.

1.5 dangerous failure

failure which has the potential to put the SRP/CS in a hazardous or fail-to-function state

Note 1 to entry: Whether or not the potential is realized can depend on the channel architecture of the system; in redundant systems a dangerous hardware failure is less likely to lead to the overall dangerous or fail-to function state.

Note 2 to entry: [SOURCE: IEC 61508–4, 3.6.7, modified.]

1.6 common cause failure CCF

failures of different items, resulting from a single event, where these failures are not consequences of each other

Note 1 to entry: Common cause failures should not be confused with common mode failures (see
ISO 12100:2010, 3.36).

[SOURCE: IEC 60050‑191-am1:1999, 04-23.]

1.7 systematic failure

failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors

Note 1 to entry: Corrective maintenance without modification will usually not eliminate the failure cause.

Note 2 to entry: A systematic failure can be induced by simulating the failure cause.

Note 3 to entry: Examples of causes of systematic failures include human error in

— the safety requirements specification,

— the design, manufacture, installation, operation of the hardware, and

— the design, implementation, etc., of the software.

[SOURCE: IEC 60050‑191:1990, 04-19.]

1.8 muting

temporary automatic suspension of a safety function(s) by the SRP/CS

1.9 manual reset

function within the SRP/CS used to restore manually one or more safety functions before restarting a machine

1.10 harm

physical injury or damage to health
[SOURCE: ISO 12100:2010, 3.5.]

1.11 hazard

potential source of harm
Note 1 to entry: A hazard can be qualified in order to define its origin (e.g. mechanical hazard, electrical hazard) or the nature of the potential harm (e.g. electric shock hazard, cutting hazard, toxic hazard, fire hazard).
Note 2 to entry: The hazard envisaged in this definition:
— either is permanently present during the intended use of the machine (e.g. motion of hazardous moving elements, electric arc during a welding phase, unhealthy posture, noise emission, high temperature);
— or may appear unexpectedly (e.g. explosion, crushing hazard as a consequence of an unintended/unexpected start-up, ejection as a consequence of a breakage, fall as a consequence of acceleration/deceleration).
[SOURCE: ISO 12100:2010, 3.6, modified.]

1.12 hazardous situation

circumstance in which a person is exposed to at least one hazard
Note 1 to entry: The exposure can result in harm immediately or over a period of time.
[SOURCE: ISO 12100:2010, 3.10.]

1.13 risk

combination of the probability of occurrence of harm and the severity of that harm
[SOURCE: ISO 12100:2010, 3.12.]

1.14 residual risk

risk remaining after protective measures have been taken
Note 1 to entry: See Figure 2.
[SOURCE: ISO 12100:2010, 3.13, modified.]

1.15 risk assessment

overall process comprising risk analysis and risk evaluation
[SOURCE: ISO 12100:2010, 3.17.]

1.16 risk analysis

combination of the specification of the limits of the machine, hazard identification and risk estimation
[SOURCE: ISO 12100:2010, 3.15.]

1.17 risk evaluation

judgement, on the basis of risk analysis, of whether risk reduction objectives have been achieved
[SOURCE: ISO 12100:2010, 3.16.]

1.18 intended use of a machine

use of the machine in accordance with the information provided in the instructions for use
[SOURCE: ISO 12100:2010, 3.23.]

1.19 reasonably foreseeable misuse

use of a machine in a way not intended by the designer, but which may result from readily predictable human behaviour
[SOURCE: ISO 12100:2010, 3.24.]

1.20 safety function

function of the machine whose failure can result in an immediate increase of the risk(s)
[SOURCE: ISO 12100:2010, 3.30.]

1.21 monitoring

safety function which ensures that a protective measure is initiated if the ability of a component or an element to perform its function is diminished or if the process conditions are changed in such a way that a decrease of the amount of risk reduction is generated

1.22 programmable electronic system PES

system for control, protection or monitoring dependent for its operation on one or more programmable electronic devices, including all elements of the system such as power supplies, sensors and other input devices, contactors and other output devices
[SOURCE: IEC 61508‑4:1998, 3.3.2, modified.]

1.23 performance level PL

discrete level used to specify the ability of safety-related parts of control systems to perform a safety
function under foreseeable conditions
Note 1 to entry: See 4.5.1.

1.24 required performance level PLr

performance level (PL) applied in order to achieve the required risk reduction for each safety function
Note 1 to entry: See Figures 2 and A.1.

1.25 mean time to dangerous failure MTTFD

expectation of the mean time to dangerous failure
[SOURCE: IEC 62061:2005, 3.2.34, modified.]

1.26 diagnostic coverage DC

measure of the effectiveness of diagnostics, which may be determined as the ratio between the failurerate of detected dangerous failures and the failure rate of total dangerous failures
Note 1 to entry: Diagnostic coverage can exist for the whole or parts of a safety-related system. For example, diagnostic coverage could exist for sensors and/or logic system and/or final elements.
[SOURCE: IEC 61508‑4:1998, 3.8.6, modified.]

1.27 protective measure

measure intended to achieve risk reduction
EXAMPLE 1 Implemented by the designer: inherent design, safeguarding and complementary protective measures, information for use.
EXAMPLE 2 Implemented by the user: organization (safe working procedures, supervision, permit-to-work systems), provision and use of additional safeguards, personal protective equipment, training.
[SOURCE: ISO 12100:2010, 3.19, modified.]

1.28 mission time TM

period of time covering the intended use of an SRP/CS

1.29 test rate rt

frequency of automatic tests to detect faults in a SRP/CS, reciprocal value of diagnostic test interval

1.30 demand rate rD

frequency of demands for a safety-related action of the SRP/CS

1.31 repair rate rr

reciprocal value of the period of time between detection of a dangerous failure by either an online test or obvious malfunction of the system and the restart of operation after repair or system/component replacement
Note 1 to entry: The repair time does not include the span of time needed for failure-detection.

1.32 machine control system

system which responds to input signals from parts of machine elements, operators, external control equipment or any combination of these and generates output signals causing the machine to behave in the intended manner
Note 1 to entry: The machine control system can use any technology or any combination of different technologies (e.g. electrical/electronic, hydraulic, pneumatic, mechanical).

1.33 safety integrity level SIL

discrete level (one out of a possible four) for specifying the safety integrity requirements of the safety functions to be allocated to the E/E/PE safety-related systems, where safety integrity level 4 has the highest level of safety integrity and safety integrity level 1 has the lowest
[SOURCE: IEC 61508‑4:1998, 3.5.6.]

1.34 limited variability language LVL

type of language that provides the capability of combining predefined, application-specific library functions to implement the safety requirements specifications
Note 1 to entry: Typical examples of LVL (ladder logic, function block diagram) are given in IEC 61131–3.
Note 2 to entry: A typical example of a system using LVL: PLC.
[SOURCE: IEC 61511‑1:2003, 3.2.80.1.2, modified.]

1.35 full variability language FVL

type of language that provides the capability of implementing a wide variety of functions and applications

EXAMPLE C, C++, Assembler.

Note 1 to entry: A typical example of systems using FVL: embedded systems.

Note 2 to entry: In the field of machinery, FVL is found in embedded software and rarely in application software.

[SOURCE: IEC 61511‑1:2003, 3.2.80.1.3, modified.]

1.36 application software

software specific to the application, implemented by the machine manufacturer, and generally containing logic sequences, limits and expressions that control the appropriate inputs, outputs, calculations and decisions necessary to meet the SRP/CS requirements

1.37 embedded software, firmware, system software

software that is part of the system supplied by the control manufacturer and which is not accessible for modification by the user of the machinery

Note 1 to entry: Embedded software is usually written in FVL.

1.38 high demand or continuous mode

mode of operation in which the frequency of demands on a SRP/CS is greater than one per year or the safety related control function retains the machine in a safe state as part of normal operation

[SOURCE: IEC 62061:2012, 3.2.27, modified.]

1.39 proven in use

demonstration, based on an analysis of operational experience for a specific configuration of an element, that the likelihood of dangerous systematic faults is low enough so that every safety function that uses the element achieves its required performance level (PLr)

[SOURCE: IEC 61508‑4:2010, 3.8.18, modified.]

Table 1 — Symbols and abbreviated terms

Symbol or abbreviation	Description
a, b, c, d, e	Denotation of performance levels
AOPD	Active optoelectronic protective device (e.g. light barrier)
B, 1, 2, 3, 4	Denotation of categories
B_{10D}	Number of cycles until 10 % of the components fail dangerously (for pneumatic and electromechanical components)
Cat.	Category
CC	Current converter
CCF	Common cause failure
DC	Diagnostic coverage
DC_{avg}	Average diagnostic coverage
F, F1, F2	Frequency and/or time of exposure to the hazard
FB	Function block
FVL	Full variability language
FMEA	Failure modes and effects analysis
I, I1, I2	Input device, e.g. sensor
i, j	Index for counting
I/O	Inputs/outputs
i_{ab}, i_{bc}	Interconnecting means
K1A, K1B	Contactors
L, L1, L2	Logic
LVL	Limited variability language
M	Motor
MTTF	Mean time to failure
$MTTF_D$	Mean time to dangerous failure
n, N, $\tilde{N}$	Number of items
N_{low}	Number of SRP/CS with PL_{low} in a combination of SRP/CS
n_{op}	Mean number of annual operations
O, O1, O_2, OTE	Output device, e.g. actuator
P, P1, P2	Possibility of avoiding the hazard
PES	Programmable electronic system
PFH_D	average probability of dangerous failure per hour
PL	Performance level
PLC	Programmable logic controller
PL_{low}	Lowest performance level of a SRP/CS in a combination of SRP/CS
PL_r	Required performance level
r_D	Demand rate
r_t	Test rate
RS	Rotation sensor
S, S1, S2	Severity of injury
SW1A, SW1B, SW2	Position switches

Annex D

Rev 3 Västerås 2019-01-07/SKj

Contactors suitable for Safety applications

Safety components

The Machinery Directive (2006/42/EC) gives the following definition of a safety component:
"Safety component" means a component:
1. which serves to fulfil a safety function,
2. which is independently placed on the market,
3. the failure and/or malfunction of which endangers the safety of persons, and
4. which is not necessary in order to the machinery to function, or for which normal components may be substituted in order to the machinery to function

When a manufacturer declares a product as being a "safety component", the product shall satisfy all applicable requirements of the Machinery Directive.

However, some CAPIEL contactors may not meet the above definition for a "safety component" but may nevertheless have documented features or functionality that can be used by the machine builder to determine whether they are suitable for functional safety related use in an application.

From the MD Guide

Safety components are components intended by the component manufacturer to be fitted to machinery specifically to fulfil a protective role, in addition to any operational duty.

Product standards for contactors

EN 60947-4-1 (IEC 60947-4-1:2018) is the harmonized product standard for contactors
Annex K gives the procedure to determine contactors suitability for safety applications

Annex K
(normative)
Procedure to determine data for electromechanical contactors used in functional safety applications
K.3 Characterization of a failure mode

Table K.1 gives the typical failure modes of a contactor.

Failure modes	Characteristics for a normally open contactor
Failure to open	– current remaining after the electromagnet is de-energised
Failure to close	– no current in one or more poles after the electromagnet is energised
Short-circuit between poles	– insulation failure between poles
Short-circuit between pole and any adjacent part	– insulation failure with any adjacent part

Table K.2 – Typical failure ratios for normally open contactors

Failure modes	Typical failure ratios F associated with AC-3 electrical durability test results for normally open contactors[a]	Typical failure ratios F associated with mechanical durability test results for normally open contactors[a]
Failure to open [b]	73 %	50 %
Failure to close	25 %	50 %
Short-circuit between poles	1 %	0 %
Short-circuit between poles and any adjacent part (e.g. auxiliary, earth plate, coil)	1 %	0 %
If a contactor is used in such a way that a hazardous situation can be caused by a failure mode for which the failure ratio is above 40 %, the system may need a diagnostic function and appropriate fault reaction function(s).		
[a] The typical values result from tests performed on different contactors. [b] The diagnostic coverage of the subsystem incorporating a contactor with mirror contacts can be 99 % if an appropriate fault reaction function(s) is provided.		

The hardware fault tolerance for one contactor is generally zero.

NOTE in IEC 62061, a hardware fault tolerance of N means that N+1 faults can cause a loss of the function.

Features for contactors to be used in safety applications

Contactors suitable for safety applications (some time called:" safety contactor") have the following features.

-fulfill EN60947-4-1 (IEC60947-4-1)
-mirror contacts
-information on B_{10d} value

What is a Contactor suitable for safety application ("safety contactor")?

- It is a safety element,i.e. not ready to use directly in a safety application.
- In the harmonized standard EN ISO 13849-2 there is a good interpretation of which component is useful for safety applications and not, e.g. a contactor is a well-tried component, if the product standard EN 60947-4-1 is fulfilled.
- Depending on the PL/SIL of the safety function one or two contactors with or without monitoring will be used. Contactors with the features of mirror contacts and B_{10d} value given, can be used in a safety function with any PL/SIL.

Normal features for "Safety Contactors"

- Easy identification by color
- Contactor status guaranteed:
    - Factory-mounted and permanently fixed mirror contacts. Positively guided/mechanically linked auxiliary contacts
    - Marking (front face) of mirror and mechanically linked contacts
- Prevent manual operation (safety cap integrated)
- Simplify calculation of your installation safety level (better service):
    - Library with safety values in Sistema software
    - B10d published in standard catalog