APPLICATION NOTE

Functional safety and reliability data for Motor starting and protection.

B_{10} and B_{10D} values

Contents

Foreword

ABB is a pioneering technology leader in electrification products, robotics, motion, and industrial automation, serving customers in utilities, industry, transport, and infrastructure globally. Continuing a history of innovation spanning more than 130 years, ABB today is writing the future of industrial digitalization with two clear value propositions: bringing electricity from any power plant to any plug, and automating industries from natural resources to finished products.

All the information provided in this guide is only general and each application must be handled individually as a specific case, so be sure to always follow all national and local installation regulations/codes for your specific application.

Please note that the values given here are values that have been determined by ABB using a specific procedure and are subject to statistical expectation and corresponding scattering. We have carefully determined the data to the best of our knowledge. However, we would like to make it clear that the transmission of the data does not constitute an extension of the specification of the products nor a guarantee. In addition, we cannot accept any liability for any consequences of which the data communicated here are the cause or contributory cause. The supply relationships between ABB and the customer or the respective OEM continue to be governed exclusively by the framework supply agreements or other supply relationships agreed between these contractual partners.

The transmission of the data does not justify any additional claims against ABB since ABB reserves the right to make changes to the document at any time without notice. In the event of discrepancies between the data in this document and other ABB publications, such as catalogs, manuals, datasheets, the content of the other documentation takes precedence.

Irrespective of the legal basis, ABB excludes its liability, in particular for the usability, availability, completeness, and freedom from defects of the document, as well as associated notes, project planning, and performance data and any damage caused thereby. This does not apply if ABB is compulsorily liable, e.g., under the Product Liability Act, in cases of intent, gross negligence, culpable injury to life, body, or health, failure to comply with a guarantee given, fraudulent concealment of a defect or culpable breach of material contractual obligations. However, any claim for damages for the violation of essential contractual obligations is limited to the foreseeable damage typical for the contract, unless intent or gross negligence is involved or liability is assumed due to injury to life, body, or health. A change in the burden of proof to your disadvantage is not associated with the above provisions. Unless ABB is liable under mandatory law, you shall indemnify ABB against any claims of third parties existing or arising in this connection. By using the content of the document, you acknowledge that ABB cannot be held liable for any damages beyond the liability provisions described.

More information on manual motor starters as well as other ABB products is available at:
https://new.abb.com/low-voltage/products/motor-protection

1. General

1.1 Purpose of this document

The purpose of this document is to describe briefly and simply what represents safety and reliability for ABB motor starting products. Therefore ABB delivers safety values (e.g., B_{10D}) for motor starting products. The values in this document, which will be regularly updated and extended to include other ABB products, are values intended for use within the technical specification for each product.

1.2 Safety characteristics

To ensure the safety of the user, safety products are installed in machines or systems. The safety-related parameters of individual products are frequently required for safety-related applications, the requirements for which are derived from the relevant safety standards. Because the machinery directive 2006/42/EC has been applied since 2009, machine builders need to consider how to design safety systems and demonstrate conformity with the Machinery Directive (2006/42/EC), preferably by using the following harmonized standards:

- EN ISO 13849-1 Safety of machinery – Safety-related parts of control systems
  - Part 1: General principles for design
- IEC / EN 62061 Safety of machinery – Functional safety of safety-related electrical, electronic and programmable electronic control systems

Safety Integrity Level (SIL)

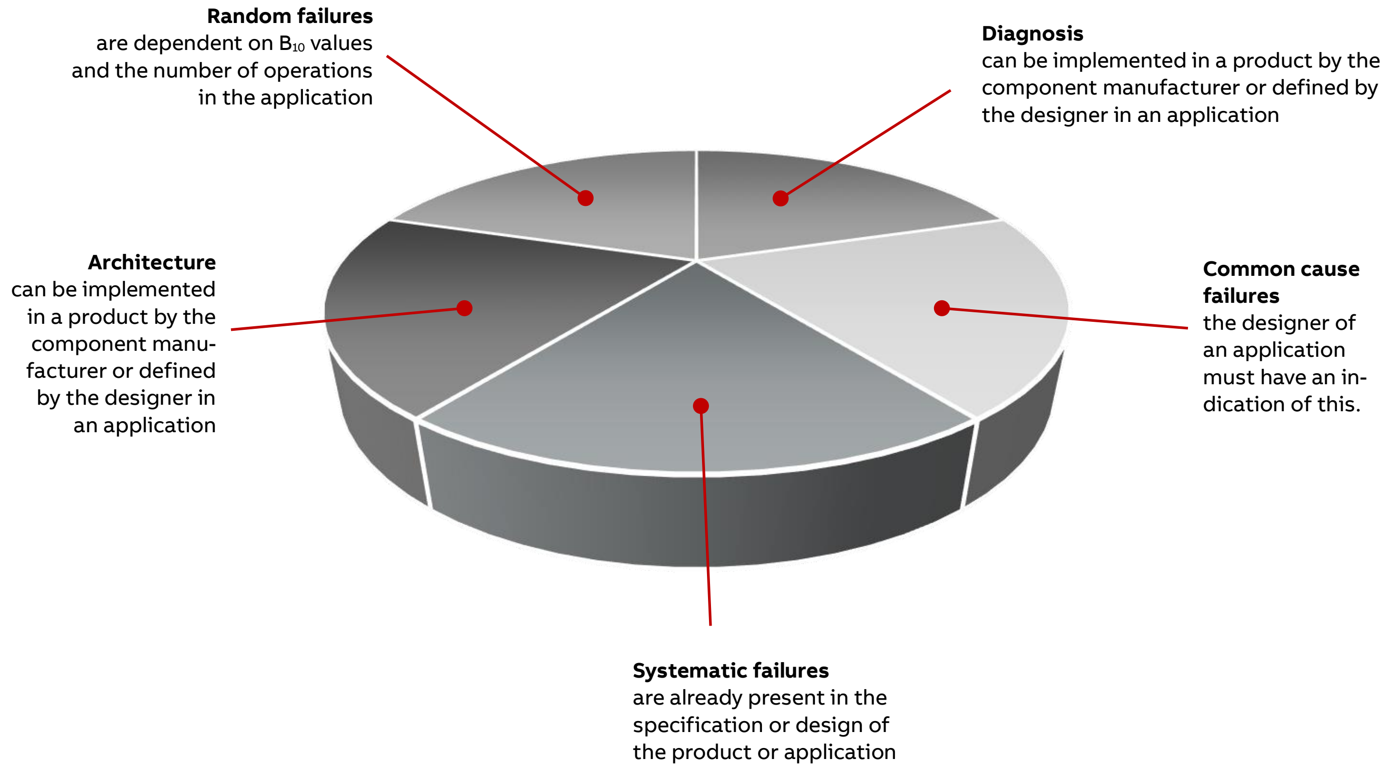
IEC / EN 62061 defines how to determine the Safety Integrity Level (SIL), which represents the reliability of safety functions. There are four SIL levels that are possible: 1, 2, 3, and 4: ‘SIL 4’ is the highest level of safety integrity and ‘SIL 1’ the lowest; only levels 1-3 are used for machinery applications. The aim of IEC / EN 62061 is to verify the required SIL of the safety functions. The architecture and system components are concerned with this calculation.

Performance Level (PL)

EN ISO 13849-1 defines how to determine the required Performance Level (PL) and how to verify the achieved PL of a safety function. PL specifically describes the ability of safety-related parts of a control system to perform a safety function under foreseeable conditions. There are five possible PLs available: a, b, c, d, and e, with PL e having the highest safety reliability, and PL a the lowest.

1.3 Functional safety factors for electromechanical products

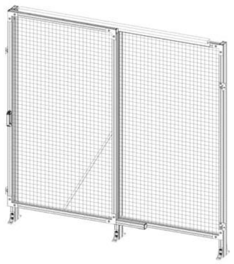
There can be many reasons for machine failures, each of which can also cause a chain reaction in some way, so it is very important to consider every single possible failure. To eliminate hazards as practicably as possible and to adequately reduce risks, it is necessary to consider several factors.

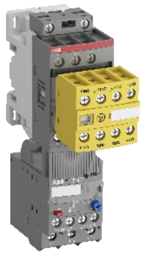


Systematic failures usually occur during the design of a system, and are usually present in the product or system from the very beginning (e.g., wrong requirements or specification, wrong dimensioning, software errors).

Because it is practically impossible to detect the failure before it occurs, random failures are difficult to predict, and therefore statistical methods are used here.

1.4 Levels of implementation of safety-related products





Guard door

To protect humans against dangerous motions in the machine area, a guard door is often used. To prevent dangerous motion, guarding is a part of the safety system.

Guard door monitoring

As access to the machine area, the guard door has to be monitored, and the number of contacts relates to the safety level.

Safety Logic

A safety subsystem which evaluates the monitoring switches.

Contactors for motor starter

Depending on the safety level, a motor starter can have more than one contact in a series.

Safety Control System

Example: Interlocked cover with monitoring and actuating function.

Safety subsystem

Examples: subfunction to prevent hazardous motion of a conveyor realized by a motor starter with integrated safety features, safety relay.

Safety element

Examples: contactor (with B_{10D}), contactor with mirror contacts, emergency stop device, interlocking device.

1.5 Which safety parameters for which products

In order for the machine manufacturer to be able to determine the required PL/SIL for the safety function, each implementation level requires different data. The following table shows the required information:

Information to be provided by the product manufacturer	**Implementation levels**					
	Safety control system		Safety subsystem		Safety element	
	TB	WB	TB	WB	TB	WB
SIL and/or PL	X	X				
SILCL and/or PL			X	X		
λ_D and/or PFD	X	X	X	X		
Operation limit		X		X		X
$MTTF_D$ or MTTF and RDF					X	
B_{10D} or B_{10} and RDF						X
T_M	X	X	X	X	X	X

X	Mandatory field, data required	TB	Time based, e.g., electronic products
		TM	Mission time (EN ISO 13849)
SIL	Safety Integrity Level (EN 62061 / EN 61508)	WB	Wear based, e.g., electromechanical products
PL	Performance Level (EN ISO 13849)	$MTTF_D$	Mean Time To Dangerous Failure (EN ISO 13849)
SILCL	Safety Integrity Level Claim Limit (EN 62061)	MTTF	Mean Time TO Failure (EN ISO 13849)
λ_D	Probability Failure per Hour (EN 62061)	RDF	Ratio of Dangerous Failures
PFD	Probability of Failure on Demand (EN 61511-1)	B_{10}	10% of the devices failed (EN ISO 13849)
Operation limit	the maximum number of operations that are used in the calculation	B_{10D}	10% of the devices failed dangerous (EN ISO 13849)

As this table shows, these are the necessary values that the manufacturer should provide. As an example, a contactor or pilot device manufacturer should only deliver (green marked in the table before) the following:

- Operation limit, the maximum number of operations that are used in the calculation
- B_{10D}, or B_{10} and RDF
- TM, Mission Time. According to IEC60947-1 annex K.4, the mission time for Low-voltage switchgear and controlgear is 20 years. This concerns all electromechanical elements, i.e., a “statistic reference”, not to be calculated by manufacturers. Periods of non-use are also covered.

Furthermore, data such as λ_D, $MTTF_D$, SIL, PL are not only dependent on the individual device, but are related to the application (number of operating cycles, architecture, required SIL/PL, etc.). Therefore, each application should be individually calculated by the machine builder and/or the safety system builder, a small overview of which you will find in the following chapters.

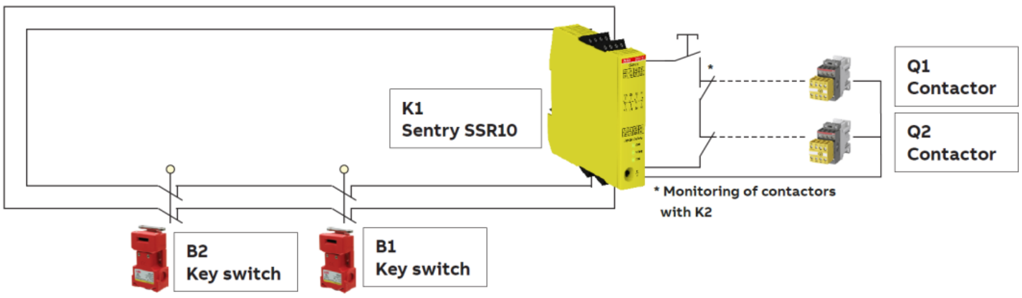
1.6 How to determine a SIL/PL of a safety function

A safety function is a function whose failure can result in an immediate increase in risk. Simply put, it is a measure taken to reduce the likelihood of an unwanted event from occurring and exposing a hazard. A safety function is not part of machine operation; if such a function fails, the machine can still operate normally, but the risk of injury from its operation increases. In the following chapters, a rough overview of a possible course of events is provided for you to understand the grand scheme of things.

Defining a safety function is a key issue, which always includes two components:

- Intended result (what the safety function performs to reduce the risk).
- Safety performance (SIL or PL – Safety Integrity Level and Performance Level respectively).

A rough example of a safety function:
Hazard: an exposed rotating shaft may cause injury if a person gets too close to it. Action: to prevent any risk of personal injury, the motor must stop within one (1) second from opening the interlocked door. After the safety function that executes the action has been identified, its required safety level is determined on chapter 1.6.1. This completes defining the safety function.



Shown here is a rough example of a machine in a manufacturing plant (only supposed to show a possible application). Around the machine is a fence to protect workers from injury. To provide safe access to the machine it should stop when the interlocked door is opened, which is realized with an interlocking device + one logic unit + two actuators.

1.6.1 Determine required SIL or PL

Safety integrity is the quantification of the performance of a safety function and quantifies the likelihood of the safety function being achieved when requested. The required safety integrity for a function is determined during risk assessment and is represented by the achieved SIL or PL, depending on the standard used. For a safety function, SIL and PL use different evaluation techniques, though their results are comparable, and the terms and definitions are similar for both.

Performance	λ_D Probability of dangerous failures per hour	PL Performance Level acc. to EN ISO 13849	SIL Safety Integrity Level acc. to IEC / EN 62061
Lowest	$\geq 10^{-5}$ up to $< 10^{-4}$	a	N/A
	$\geq 3 \times 10^{-6}$ up to $<10^{-5}$	b	1
	$\geq 10^{-6}$ up to $<3 \times 10^{-6}$	c	1
	$\geq 10^{-7}$ up to $<10^{-6}$	d	2
Highest	$\geq 10^{-8}$ up to $<10^{-7}$	e	3

1.6.2 How to determine the required SIL (IEC / EN 62061)

The process for determining the required safety integrity level (SIL) is as follows:

1. Determine the severity of the consequence of a hazardous event.
2. Determine the value for the frequency and duration the person is exposed to harm.
3. Determine the value for the probability of the hazardous event occurring when exposed to it.
4. Determine the value for the possibility of preventing or limiting the harm.

For each hazard, and – as applicable – for each severity level, the numbers from the duration Frequency (**Fr**), Probability of hazardous event (**Pr**), and Avoidance (**Av**) should be added to receive the resulting Class of probability of harm (**Cl**). To find the resulting SIL level based on the crossing point of Class of probability and Severity (**Se**), this Class of probability of harm should then be entered into this table.

Fr **Frequency, duration**		**Pr** **Probability of a hazardous event**		**Av** **Avoidance**	
≥ 1 per h	5	Very high	5		
< 1 per h to ≥1 per day	5	Likely	4		
< 1 per day to ≥ 1 per 2 wks	4	Possible	3	Impossible	5
< 1 per 2 wks to ≥ 1 per yr	3	Rarely	2	Possible	3
< 1 per yr	2	Negligible	1	Likely	1

Total: : Cl = Fr + Pr + Av = 5 + 3 + 3 = 11

Se **Severity**		**Cl (Class of the probability of harm)** **4**	**5-7**	**8-10**	**11-13**	**14-15**
Death, loss of an eye or arm	4	SIL2	SIL2	SIL2	SIL3	SIL3
Permanent, loss of fingers	3			SIL1	SIL2	SIL3
Reversible, medical attention	2				SIL1	SIL2
Reversible, first aid	1					SIL1
						The SIL2 safety function is required

Table 2. Example of SIL assignment table (based on EN/IEC 62061, tables A.1-A.4; A.6).

In this example, the hazard analysis is carried out for an exposed rotating shaft.

1. Severity (Se) = 3. The consequence of the hazard is a permanent injury, possibly the loss of fingers.
2. Frequency (Fr) = 5. A person is exposed to the hazard several times a day.
3. Probability (Pr) = 3. It is possible that the hazard will occur.
4. Avoidance (Av) = 3. The hazard can be avoided.

⇨ 5 + 3 + 3 = 11, with the determined consequence, this equals SIL 2.

The tables used for determining the numbers are presented in the standard. After the required SIL has been defined, the implementation of the safety system can begin.

1.6.3 How to determine the required PL_r (EN ISO 13849-1)

To determine the required PL, select one of the alternatives from the following parameters and create a 'path' to the required PL, as a, b, c, d, or e, in the risk graph below:

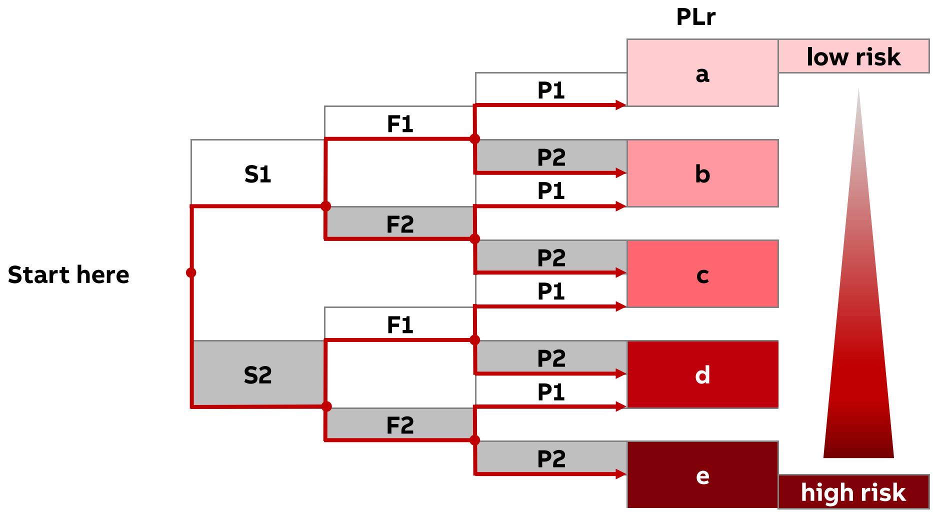
1. Determine the severity of injury/damage:
   - S1 Slight, usually a reversible injury
   - S2 Severe, usually an irreversible injury, including death
2. Determine the frequency and duration of exposure to the hazard:
   - F1 Rare to often, and/or short exposure
   - F2 Frequently to continuous, and/or long exposure
3. Determine the possibility of preventing the hazard or limiting the damage caused by the hazard:
   - P1 Possible under certain conditions
   - P2 Hardly possible

Example: Hazard analysis for an exposed rotating shaft.

- The consequence is severe, irreversible injury. Severity = S2.
- A person is exposed several times a day. Frequency = F2.
- It is possible to avoid or limit the harm caused. Possibility =P1.

This example results in PLr d.

The path leads to the required PL (PL_r) value, and as with SIL, the tables used to determine the safety integrity are presented in the standard. Similarly, once the PL_r has been defined, implementation of the safety function can begin.



1.6.4 Implement a functional safety system

To design a safety function, design it to meet the required SIL/PL specified in “1.5.1 Determine required SIL or PL”: Implementation and verification processes (see 1.5.5 Verifying a safety function) are iterative and run parallel with each other. To ensure that the defined safety level is reached with the implemented system, use verification as a tool during implementation. For more verification information, see the next chapter “Verify functional safety”. Using these programs makes creating and verifying the system more convenient.

The general steps for implementing a functional safety system include (example based on SIL level):

1. Defining the safety requirements according to the
    a) Safety Integrity Level SIL (according to IEC / EN 62061), **or**
    b) Performance Level PL (according to EN ISO 13849-1).
2. Selecting the system architecture to be used for the safety system.
    a) Determine category B, 1, 2, 3, or 4 as presented in EN ISO 13849-1, **or**
    b) Designated architecture A, B, C, or D as presented in IEC / EN 62061. Do this for the sub-systems
3. Constructing the system from safety-related sub-systems – sensor/switch, input, logic, output, and actuator. Either:
    - by using certified subsystems (recommended) or
    - by performing:
        a) SIL assessment and safety calculations for each subsystem, **or**
        b) PL assessment and safety calculations for each subsystem
4. Installing the safety system: to avoid common failure possibilities due to improper wiring, environmental, or other such factors, the system needs to be installed properly. A safety function that does not perform correctly due to careless installation is of little use and may even pose a risk in itself.
5. Verify the functionality of the system: the Lowest SIL or PL of the subsystem in the safety function will be the highest achievable a) SIL **or** b) PL for the safety function.

Gate limit switches	Safety logic and I/O	Actuator
		
Subsystem 1	Subsystem 2	Subsystem 3

Tip:
Verifying the achieved SIL or PL can be conveniently done with the ABB Functional safety design tool (FSDT) PC-tool. As required, it is also important to take into account systematic failures, which are common human mistakes in the design process. To take care of these, it is normally necessary to have functional safety and quality management systems to ensure that all system failures can be minimized.

1.6.5 Verifying a safety function

Verification of the safety function demonstrates and ensures that the implemented safety system meets the requirements specified for the safety function in the safety requirements phase.

In addition to verifying the achieved SIL or PL of the system, the correct operation of the safety function must also be verified by carrying out functionality testing.

1.6.5.1 Verifying the safety function SIL (IEC/EN 62061)

Verify safety integrity levels by showing that the safety performance of the designed safety function, i.e., its reliability, is equal to or greater than the required performance target set during risk evaluation.

To verify the safety system SIL where certified sub-systems are used:

1. Determine the systematic safety integrity level (SIL) for each subsystem by
    a. Using certified safety components, which already have the SIL and PFH_D -value defined by the manufacturer, or
    b. Using components, where a manufacturer has not defined the SIL and PFH_D -value. In this case, the designer must determine the SIL and PFH_D-value for the subsystem through architectural structures, component reliability data, etc. These values will eventually define which SIL can be reached with that subsystem when these values are compared to tables 3 and 5 in EN/IEC 62061. Chapter 2 shows you how to calculate λ_D.
2. Use the Common Cause Failure (CCF) checklist to ensure that all necessary aspects of creating the safety systems have been considered. CCF checklist tables can be found in the IEC/EN 62061 standard, Annex F
3. Calculate the random hardware safety integrity for the system using 'Probability of a dangerous Failure per Hour' values defined for the sub-systems. PFH_D is the random hardware failure value that is used for determining the SIL.
4. Compare the overall PFH_D-value of the safety function to the table below (table 3 in EN/IEC 62061) to verify, what SIL or PL the safety function is fulfilling. Determine the achieved SIL from the below table.

Performance	PFH_D (1/h)	SIL Safety Integrity Level
Low	$\geq 10^{-6}$ up to $< 10^{-5}$	SIL 1
	$\geq 10^{-7}$ up to $<10^{-6}$	SIL 2
Highest	$\geq 10^{-8}$ up to $<10^{-7}$	SIL 3

Table for determining SIL (based on EN/IEC 62061, table 3)

In addition, it is important to take into account systematic failures as required in IEC/EN 62061. (These are common human mistakes in the design process.) To take care of these, it is normally necessary to have functional safety and quality management systems to ensure that all system failures can be minimized.

Example:

Verifying SIL for the rotating shaft functional safety system.

Gate limit switches	**Safety logic and I/O**	**Actuator**
		
Subsystem 1	Subsystem 2	Subsystem 3
SIL = 3	SIL = 3	SIL = 3
PFH_{D1} = 4.5 x 10^{-9}	PFH_{D2} = 4.9 x 10^{-9}	PFH_{D3} = 9.06 x 10^{-10}.

Systematic safety integrity:

SIL sys ≤ (SIL sub-system) lowest **->** SIL 3

Random hardware safety integrity:

$PFH_D = PFH_{D1} + PFH_{D2} + PFH_{D3}$ = 1 x 10^{-8}

Determine SIL according to the PFH_D value obtained from the safety function. In the example above, the safety function meets SIL 3.

1.6.5.2 Verifying the PL of a safety function (EN ISO 13849-1)

To verify the performance level, it must be established that the achieved PL of the corresponding safety function matches the required PL. If several subsystems form one safety function, their performance levels must be equal or greater than the performance level required for the safety function in question.

1. Determine performance level (PL) for each subsystem by
   a. Using certified safety components which already have the PL and PFH_D value defined by the manufacturer, or
   b. Using components, where a manufacturer has not defined the PL and PFH_D-value. In this case, the designer must determine the PL and - PFH_D value for the subsystem.

2. Use the Common Cause Failure (CCF) checklist to ensure that all the necessary aspects to prevent common cause failure in the safety circuit have been considered. CCF checklist tables can be found in EN ISO 13849-1 standard, Annex F. The required minimum score is 65 points.
3. When all subsystems have PL and PFH_D values, calculate the overall - PFH_D value for the safety functions by summing up the -PFH_D values of each subsystem.
4. Compare the overall - PFH_Dvalue of the safety function to the table below (table 3 in EN ISO 13849-1) to verify, what PL the safety function is fulfilling.

Performance	**PFH_D (1/h)**	**PL**
Lowest	$\geq 10^{-5}$ up to $< 10^{-4}$	a
	$\geq 3 \times 10^{-6}$ up to $<10^{-5}$	b
	$\geq 10^{-6}$ up to $<3 \times 10^{-6}$	c
	$\geq 10^{-7}$ up to $<10^{-6}$	d
Highest	$\geq 10^{-8}$ up to $<10^{-7}$	e

Table for determining the PL (based on EN ISO 13849-1, table 2)

It is also important to take into account systematic failures as required in EN ISO 13849-1. These are common human mistakes in the design process. To take care of these, it is normally necessary to have functional safety and quality management systems to ensure that all system failures can be minimized.

2. Failure rates of safety elements for high demand application – B_{10} and B_{10D}

2.1 What are B_{10} and B_{10D} values

The IEC / EN 62061 standard "Safety of machinery - Functional safety of electrical, electronic and programmable controllers of machines" also requires failure rates for electromechanical components. These failure rates enable the probability of dangerous failure per hour PFH_D of a safety function to be calculated. The B_{10} value is used to calculate the failure rate of electromechanical components.

The B_{10} value is the minimum number of switching cycles until 10% of the devices fail. This value is therefore a statistical expectation value, and applies only under defined conditions. A failure is defined as one that exceeds defined limit values (switching time, leakage, switching pressure, etc.). However, it should be noted that a component can also fail before the B_{10} value is reached. Therefore, the specified survival probability does not constitute a manufacturer's guarantee.

The B_{10D} value is the number of switching cycles after which dangerous failures occur in 10% of the units under consideration, where the addition "D" represents "dangerous". The value is relevant when verifying the required Performance Level/Safety Integrity Level for a specific safety function when electromechanical components are used. The PL/SIL is estimated as a part of the overall risk assessment of a machine, related to its contribution to the reduction.

Note that it is not necessary to calculate B_{10}/B_{10D} values for safety components that already have a SIL/PL value stated by the manufacturer.

Why do I need the B_{10} and B_{10D} values?

The B_{10} value can be used to calculate the total failure rate of a component using a simplified formula (see section 6.7.8.2.1 of IEC / EN 62061): $\lambda = \frac{0.1 \times C}{B_{10}} \; [failure\ /\ h]$

C = operating cycle per hour (user's indication)

The failure rate is composed of safe (λ_S) and dangerous (λ_D) failures: $\lambda = \lambda_S + \lambda_D$

λ_D *= The rate of dangerous failures*

λ_S *= The rate of safe failures*

Besides this, there is the possibility to calculate the meantime to failure (MTTF) of irreparable components (63.2% of all components fail before the meantime to failure): $\mathrm{MTTF} = \frac{1}{\lambda} = \frac{B_{10}}{0.1 \times C} \; [h]$

The MTTF is a statistical mean value, but not a guaranteed lifetime.

The B_{10D} value can be calculated by using the Ratio of Dangerous Failures (RDF); in EN ISO 13849-1, it can be determined as follows: $B_{10D} = \frac{B_{10}}{RDF}$

The B_{10D} value can be used to calculate the dangerous failure rate of a component, which is needed to determine the SIL or PL, by using a simplified formula: $\lambda_D = \frac{0.1 \times C}{B_{10D}} \; [dangerous\ failure\ /\ h]$

In addition, there is the possibility to calculate the dangerous mean time to failure ($MTTF_D$): $MTTF_D = \frac{1}{\lambda_D} = \frac{B_{10D}}{0.1 \times C} \; [h]$

Note: its not required to calculate B10/B10D values for safety components that already have a SIL/PL value stated by the manufacturer.

2.2 B_{10} and B_{10D} values

The values given are target values that components are expected to achieve based on testing, and are for the operation in high or continuous demand applications. A high-demand safety function is for a demand which occurs more often than once per year (e.g., once per day). In the following table, which contains data based on functional safety and reliability calculations done by ABB for product groups, failure to open the circuit is considered a dangerous failure:

ABB Electromechanical components	Contact load, Utilization category	B_{10} values	B_{10D} values	RDF
(only devices with positive opening contacts allowed)				
MPE, MPM, CE EMERGENCY STOP DEVICES	(1)	45 000	225 000	20%
Cable-operated switches for EMERGENCY STOP function	(1)	20 000	100 000	20%
Hinge switches	(1)	20 000	100 000	20%
Limit switches				
LS2	(2)	10 000 000	20 000 000	50%
LS3, LS4	(2)	> 5 000 000 (4)	> 10 000 000 (4)	50%
3-pole AFS contactors				
AFS09 / 12 / 16 / 26 / 30 / 38	AC-3 / AC-3e	1 000 000	1 300 000	73% (5) (6)
AFS40 / 52 / 65 / 80 / 96	AC-3 / AC-3e	1 000 000	1 300 000	73% (5) (6)
AFS116 / 146 / 190 / 205	(3)	5 000 000	10 000 000	50%
	AC-3 / AC-3e	1 000 000	1 300 000	73% (5) (6)
AFS265 / 305 / 370	(3)	3 000 000	6 000 000	50%
	AC-3 / AC-3e	1 000 000	1 300 000	73% (5) (6)
AFS400 / 460	(3)	2 000 000	4 000 000	50%
	AC-3 / AC-3e	500 000	680 000	73% (5) (6)
AFS580 / 750	(3)	1 000 000	2 000 000	50%
	AC-3 / AC-3e	500 000	680 000	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 the rated value (Ie)
4) For detailed B_{10} value, please refer to “mechanical durability” in the online product datasheet
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)

RDF Ratio of Dangerous Failures B_{10} 10% of the devices failed (EN ISO 13849)
B_{10} 10% of the devices failed (EN ISO 13849)
B_{10D} 10% of the devices failed dangerous (EN ISO 13849)

Note: The ratio of dangerous failures is a minimum of 20%

Example to calculate λ_D, the rate of dangerous failures per hour:

An AFS contactor > 100A ≤ 205A is used 10 times an hour, switching a motor to start and stop.
B_{10D} for AFS116 is 1.3×10^6, which will give

$$\lambda_D = \frac{0.1 \times C}{B_{10D}} = \frac{0.1 \times 10}{1.3 \times 10^6} \approx 7.7 \times 10^{-7}$$

This gives a λ_D of 7.7×10^{-7} of dangerous failure per hour for the single contactor.

3. Failure rates of safety elements for the low demand application - PFD

The SIL classification of a device involves distinguishing between low demand mode and high demand mode applications. This classification, primarily linked to EN 61511-1 standards for safety instrumented systems in the process industry, derives the SIL value from the probability of failure on demand (PFD) for low demand applications. Low demand scenarios typically occur in process industry plants, such as emergency shutdown systems activated only when the normal process fails, with an expected demand rate of less than once per year (e.g., once every 10 years). The average probability of failure on demand (PFD_{avg}) for a protective device can be calculated based on failure rates. Electromechanical components are recommended to undergo a functional repeat test annually to identify passive faults.

3.1 Failure rates for calculation of PFD_{avg}

This table contains general data based on functional safety and reliability calculations done by Capiel for ABB prod-ucts.

Product group	Normal failure rate (FIT)	RDF (Ratio of dangerous failures)	Safety function
Emergency stop control devices	100	20%	Circuit disconnected when actuated
Pushbuttons	100	20%	Circuit disconnected when actuated
AFS Contactors	100	40%	The main circuit disconnected after the coil is de-energized in a given time

4. ABB and tools for safety applications

4.1 ABB Functional safety design tool (FSDT-01)

The functional safety design tool (FSDT-01) is used for calculating safety functions in machine applications. It is an MS-Windows application, which is a support tool for performing functional safety modeling, design, calculations, and verification for machine functional safety.

The tool supports both standards, EN ISO 13849-1 and IEC / EN 62061, and is aimed to simplify the process of safety function design and verification, and to generate documentation to support compliance to the requirements of the mentioned standards and the European Machine Directive for safety.

Functional safety design tool - FSDT-01

Product libraries for ABB products can be downloaded as well. There are two versions of libraries; one version exclusively for use with FSDT and another that is usable with several on the market existing FS tools (VDMA-format).

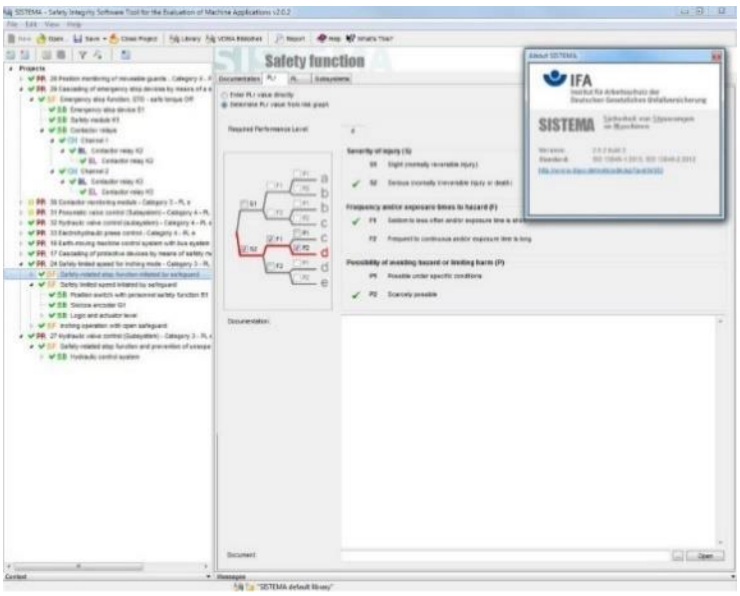
4.2 SISTEMA

Data for ABB safety products are available as library files for use with the SISTEMA calculation tool. They can either be in a format only for use with SISTEMA only or in XML format (for use with any FS calculation tool)

SISTEMA software provides comprehensive support in the evaluation of safety in the context of EN ISO 13849-1 for developers and testers of safety-related machine controls. This tool enables you to model the structure of the safety-related control components based upon the designated architectures, thereby permitting automated calculation of the reliability values with various levels of detail, including that of the attained Performance Level (PL).

Risk parameters for determining the required performance level (PL_r), the category, the measures against common cause errors (CCF) in multi-channel systems, the Mean To Dangerous Failure per component ($MTTF_D$), and the mean diagnostic Coverage (DC_{avg}) of components or blocks can be recorded step by step. The effect of each parameter change on the overall system is displayed directly and can be printed out as a report.

Further information on SISTEMA and the SISTEMA software download can be found directly at IFA.



5. References

5.1 Normative references

Directive	Title
2006/42/EC	Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC.

Applicable Standards

Standards	Title
EN ISO 13849-1	Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
EN ISO 13849-2	Safety of machinery - Safety-related parts of control systems - Part 2: Validation
EN ISO 13850	Safety of machinery - Emergency stop function - Principles for design
IEC / EN 60947-1	Low-voltage switchgear and control gear - Part 1: General rules
IEC / EN 60947-4-1 Annex K	Low-voltage switchgear and controlgear - Part 4-1: Contactors and motor-starters - Electromechanical contactors and motor-starters. Annex K, shows the possible or the specification of how the manufacturer reaches the possible B10 value.
IEC / EN 60947-5-1	Low-voltage switchgear and controlgear - Part 5-1: Control circuit devices and switching elements - Electromechanical control circuit devices. Specifically Annex N
IEC / EN 60947-5-5	Low-voltage switchgear and controlgear - Part 5-5: Control circuit devices and switching elements - Electrical emergency stop device with mechanical latching function
IEC / EN 61508 *(all parts)*	Functional safety of electrical/electronic/programmable electronic safety-related systems
IEC /EN 61511-1	Functional safety - Safety instrumented systems for the process industry sector - Part 1: Framework, definitions, system, hardware and application programming Re-quirements
IEC / EN 62061	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems

5.2 Other references

Low voltage switchgear and controlgear - functional safety aspects

Functional safety is an important part of machine safety, for which the European Machinery Directive together with the harmonized standards IEC/EN 62061 and EN ISO 13849-1 provide specific requirements.

This brochure provides information concerning the application of these standards and the European Machinery. The directive, relevant to the implementation of low voltage switchgear and control gear in functional safety applications. Together with important facts, it provides examples of low and high-demand applications.

Functional Safety

The white paper from the CAPIEL is the Coordinating Committee for the Associations of Manufacturers of Switchgear and Controlgear equipment for industrial, commercial, and similar use in the European Union, that work in the range of voltages until 1 kV a.c. of 1,5 kV d.c. 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 application, and this presentation explains the basics of Functional Safety.
https://www.capiel.eu/

ABB Safety Products develop, deliver and support products and solutions for machine safety. We have a long history of helping machine builders creating production friendly and safe work environments for operators.

You can find an overview and other useful information in the Main catalog - Safety Products

6. Glossary

Description Definition

λ (PFH)	The total failure rate of an electromechanical component is also named PFH. The PFH value is used for subsystems and safety functions. Lambda values (λ) are used on a component level.
λ_S	The rate of safe failures.
λ_D	The rate of dangerous failures. The average probability of dangerous failure taking place during one (1) hour.
B_{10}	The parameter for devices where 10% of the devices are likely to fail. (The B_{10} value is the value for all failures, no matter if the failure in the application concerned is a dangerous or a safe failure.)
B_{10D}	The number of cycles until 10 % of the components fail dangerously.
C	The number of operations per hour.
FIT	Failure in Time. A 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. Standard industry value defined as the Failure Rate (λ) per billion hours.
Functional safety	Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.
MTBF	MTBF (Mean Time Between Failures) is used to describe repairable parts such as compressors, motors, or, as in this case, AFS Contactors > 100A (for the AFS Contactors ≤ 100A, this is not possible as there are no repairable parts). MTBF uses MTTF as one factor and Mean Time to Repair (MTTR) as the other to capture the complete break-down and repair cycle. As a rule of thumb, component reliability centers around MTTF since most components cannot be repaired. MTBF is shown by: MTBF = MTTF + MTTR
MTTF	Meantime to failure. MTTF 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 spacecraft. For items with long life expectancies, it is often more useful to report MTTF in years rather than hours. See EN ISO 13849-1 Annex C.
PL	Performance Level, Levels (a, b, c, d, e), for specifying the capability of a safety system to perform a safety function under foreseeable conditions.
PL_r	Required Performance Level (based on risk evaluation).
RDF	The ratio of dangerous failure, according to IEC / EN 60947-4-1 Annex K
Risk	A combination of how possible it is for the harm to occur and how severe the harm would be.
SIL, Safety Integrity Level	A discrete level (one out of a possible three) for specifying the safety integrity requirements of the safety-related control functions to be allocated to the SRECS, where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest (IEC/EN 62061).
SILCL, SIL Claim Limit	Maximum Safety Integrity Level (SIL) can be claimed for an electrical safety system, taking account of architectural constraints and systematic safety integrity.
Sub-system	An element or group of elements of a safety function that has a safety level (SIL/PL) that affects the safety level of the whole safety function. If any of the sub-systems fail, the whole safety function fails.
T_M	Mission time. For the designated architectures (categories) according to EN ISO 13849-1, a mission time of 20 years is assumed.

—
ABB France
2 rue d'Arsonval
F-69687 Chassieu cedex / France

—
ABB STOTZ-KONTAKT GmbH
Eppelheimer Straße 82
69123 Heidelberg, Germany

—
ABB Electrification Sweden AB
Motor Starting and Safety
721 61 Västerås, Sweden

You can find the address of your local sales organization on the ABB home page

http://www.abb.com/contacts -> Low-voltage products

Note
We reserve the right to make technical changes or modify the contents of this document without prior notice. Concerning purchase orders, the agreed particulars shall prevail. ABB does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

Exclusion of liability
ABB is not responsible for the implementation, verification, and validation of the overall safety system. It is the responsibility of the system integrator (or another party) who is responsible for the overall system and system safety. The system integrator (or other responsible parties) must make sure that the entire implementation complies with all relevant standards, directives, and local electrical code, and that the system is tested, verified, and validated correctly.

1SBC100226M0201 (05.2022)