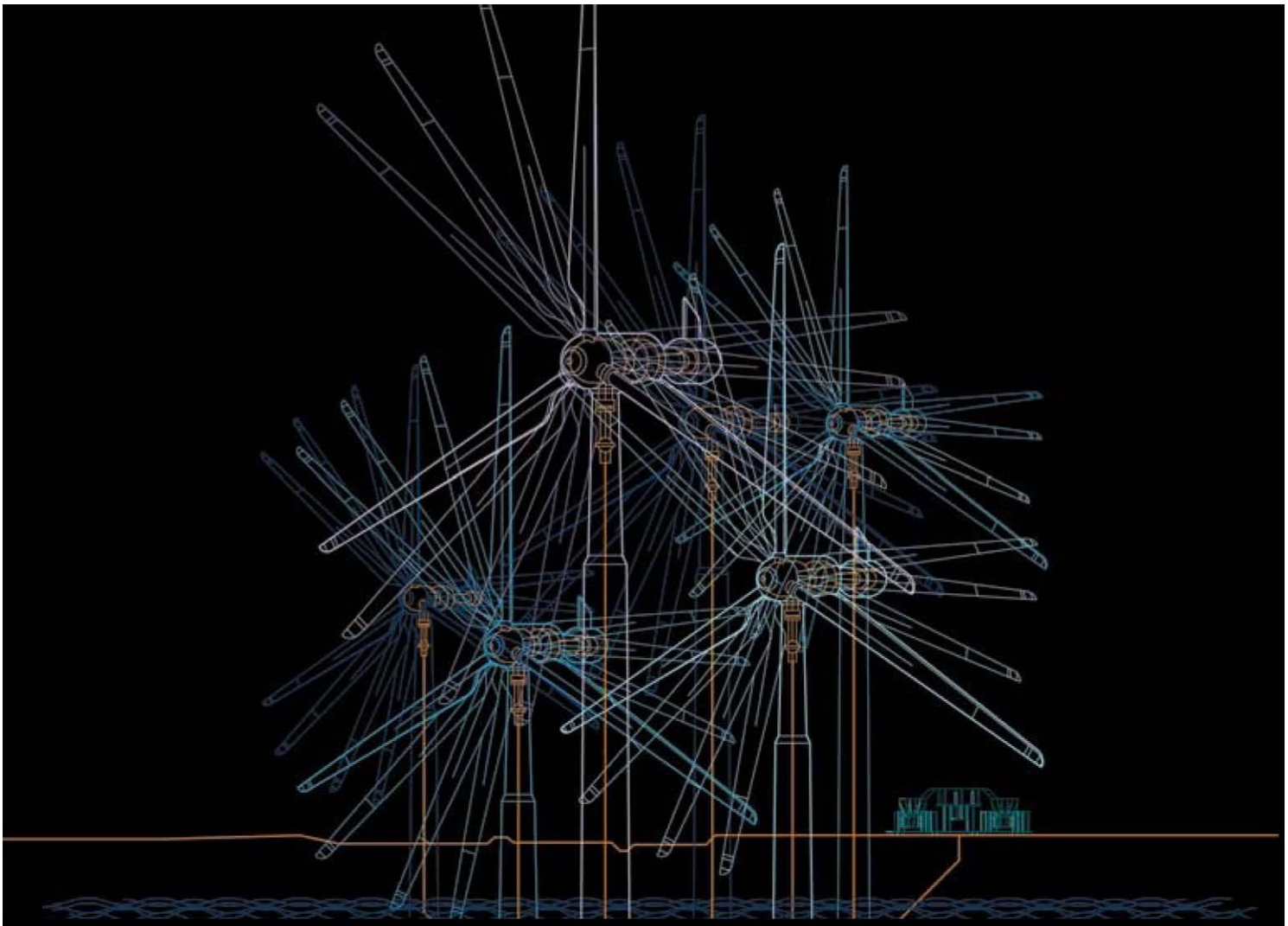

ABB Automation Products

Functional safety and reliability data

2CMT2016-005511 rev 4 2016-10-16 – Functional safety and reliability data:– Issued by SECRL Krister Linnarud (e-mail: krister.linnarud@se.abb.com)
This document replaces 2CMT002548 Nov 2009

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

Definitions

$\lambda\ (t)\ dt$ 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. 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:

$F(t) = 1 - \exp(-\lambda t)$, with λ as constant failure rate

• 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.

• $MTTF = 1/\lambda$ (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.

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.
T_M mission time (EN ISO 13849) or T_1 proof test interval or lifetime (IEC 62061) for these products is 20 years

Electromechanical components	**Contact load, utilization category**	**Typical lifetime (B_{10D} value)**	**RDF** (Ratio of Dangerous failures)	
Commanding and Detecting Devices (only devices with positive opening contacts allowed)				
EMERGENCY STOP mushroom pushbuttons - Turn-to-release (and key release) - Pull-to-release	 1) 1)	 100 000 100 000	 20% 20%	
Pushbuttons (momentary)	2)	100 000	20%	4)
Contactor Relays	3)	20 000 000	40%	
	AC-15/-14	400 000	73%	5) 6)
Contactors / Motor Starters - for motorswitching ≤ 100A	3)	20 000 000	40%	
	AC-3 (incl AC-1)	1 300 000	73%	5) 6)
Contactors / Motor Starters - for motorswitching >100A, ≤500A	3)	3 000 000	40%	
	AC-3 (incl AC-1)	400 000	73%	5) 6)

1) mainly limited by mechanical wear
2) mainly limited by contact wear
3) maximum value of B_{10D} 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. Mirror contacts are available for AF and NF range of contactors.
6) The values given are based on 50% of Ie (based on the common practice for output devices used in safety related systems)

3 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

4 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:Edition 3.1 (2012-07-20) : 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 13849-2:2012 Safety of machinery - Safety-related parts of control systems - Part 2: Validation (ISO 13849-2:2012)

EN ISO 13850:2015 **(new)** 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/A11:2013	28/11/2013

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

5 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

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