IEC TS 63394

Edition 1.0 2023-02

TECHNICAL SPECIFICATION

colour inside

Safety of machinery – Guidelines on functional safety of safety-related control system

IEC TS 63394:2023-02(en)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC TS 63394

Edition 1.0 2023-02

TECHNICAL SPECIFICATION

colour inside

Safety of machinery – Guidelines on functional safety of safety-related control system

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110; 29.020; 25.040.99 ISBN 978-2-8322-6533-8

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

SAFETY OF MACHINERY – GUIDELINES ON FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS

FOREWORD

IEC TS 63394 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects. It is a Technical Specification.

The text of this Technical Specification is based on the following documents:

Draft	Report on voting
44/980/DTS	44/989/RVDTS

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Specification is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/standardsdev/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

In the context of the safety of machinery, the sector standard IEC 62061, along with ISO 13849-1, provides requirements and guidance to the manufacturers of machines to design, develop and integrate a safety-related control system (SCS) or safety-related parts of control systems (SRP/CS), respectively, including input devices and final elements whatever the technology (mechanical, pneumatic, hydraulic and electrical technologies).

The following aspects are relevant:

– the classification of safety functions,
– the architecture of the realization of safety functions,
– the modes of operation of safety functions,
– the calculation based on the used technology.

Therefore, safety functions can be classified as follows:

– Safety functions that stop the dangerous movement(s) of the machine and that are mainly performed by SCS or SRP/CS of machines for the protection of persons. Typical examples are interlocking guards, sensitive protective equipment, two-hand control devices and emergency stop.
– Safety functions that protect the integrity of the machine against its destruction and that in a second step can have an impact on the protection of persons. Typical examples are protective devices, devices for limiting pressure or temperature (also defined as "safety-related parameters", e.g. position, speed, temperature or pressure, deviate from limits defined in the control system).
– Other safety functions that are not covered by the two previous cases.

NOTE 1 The different kinds of safety functions are defined and in line with the classifications and definitions of ISO 12100 and ISO 13849-1.

The subsystem architectures to perform safety function(s) are considered.

NOTE 2 In IEC 62061:2021, information is introduced to map SIL (Safety Integrity Level) classification of IEC 62061/IEC 61508 and classification of ISO 13849-1 in terms of categories, architectures, designated architectures and PL (Performance Level). In order to allow backward compatibility, these different criteria are considered in this document.

Depending on the mode of operation of the safety function, criteria and calculations will be considered in order to fulfil the requirements of this document and in order to be in line with existing regulations (e.g. such as recommendations for use in Europe) and other requirements already defined in existing standards, for example on test periodicity.

In order to consider mechanical, pneumatic, hydraulic and electrical technologies, applications for the safety functions, architectures and mode of operation, the associated calculations are evaluated.

NOTE 3 For example, most calculations inside standards are based on the exponential law that is typically applicable to electronic technology. For mechanic or other technologies, Weibull distribution is applied and exponential distribution is not used, except under restrictions.

SAFETY OF MACHINERY – GUIDELINES ON FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS

1 Scope

In the context of the safety of machinery, the sector standard IEC 62061, along with ISO 13849-1, provides requirements to manufacturers of machines for the design, development and integration of safety-related control systems (SCS) or safety-related parts of control systems (SRP/CS), depending on technology used (mechanical, pneumatic, hydraulic or electrical technologies) to perform safety function(s). This document does not replace ISO 13849-1 and IEC 62061. This document gives additional guidance to the application of IEC 62061 or ISO 13849-1. This document:

- gives guidelines and specifies additional requirements for specific safety functions based on the methodology of ISO 12100, which are relevant in machinery and respecting typical boundary conditions of machinery;
- considers safety functions which are designed for high demand mode of operation yet are rarely operated, called rarely activated safety functions;

  NOTE 1 IEC 62061:2021 completely covers high demand. However, other safety functions related to the protection of the machine itself and indirectly of persons are considered more in detail in this document.

- gives additional information for the calculation of failure rates using other (non-electronic) technologies based e.g. on Weibull distribution, because all the formula defined in IEC 62061 and ISO 13849-1 are based on exponential distribution.

Therefore, the basis for these guidelines and additional requirements is

- a typical classification of safety functions;
- a consideration of typical architectures used for designing safety functions;
- a consideration of modes of operation of safety functions;
- the derivation and evaluation of PFH formulas for subsystems considering the used technology.

NOTE 2 These guidelines can also be used for application of ISO 13849-1 for the design process of SRP/CS.

This document does not address low demand mode of operation according to IEC 61508.

This document does not take into account either layer of protection analysis (LOPA) or basic process control system (BPCS), according to IEC 61511 as a risk reduction measure.

This document considers all lifecycle phases of the machine regarding functional safety, and SCS or SRP/CS.

NOTE 3 The user of the machine needs information from the machine manufacturer for the safe operation of the machine, e.g. useful lifetime of components, maintenance information, testing of safety functions if necessary.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62061:2021, *Safety of machinery – Functional safety of safety-related control systems*

IEC TR 63074:2019, *Safety of machinery – Security aspects related to functional safety of safety-related control systems*

ISO 12100:2010, *Safety of machinery – General principles for design – Risk assessment and risk reduction*

ISO 13849-1:2015, *Safety of machinery – Safety-related parts of control systems – Part 1: General principles for design*

ISO 13850:2015, *Safety of machinery – Emergency stop function – Principles for design*

ISO 13851:2019, *Safety of machinery – Two-hand control devices – Principles for design and selection*

ISO 14118:2017, *Safety of machinery – Prevention of unexpected start-up*

ISO 14119:2013, *Safety of machinery – Interlocking devices associated with guards – Principles for design and selection*

3 Terms and definitions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1.1
application software
software specific to the application, that is implemented by the designer of the SCS or SRP/CS, generally containing logic sequences, limits and expressions that control the appropriate input, output, calculations, and decisions necessary to meet the SCS or SRP/CS functional requirements

[SOURCE: IEC 62061:2021, 3.2.59, modified – "or SRP/CS" added to the definition]

3.1.2
architectural constraint
set of architectural requirements that limit the SIL that can be claimed for a subsystem

[SOURCE: IEC 62061:2021, 3.2.46]

3.1.3
architecture
specific configuration of hardware and software elements in an SCS or SRP/CS

[SOURCE: IEC 61508-4:2010, 3.3.4, modified – Terminology adapted to machinery]

3.1.4
average frequency of a dangerous failure per hour
PFH
average frequency of dangerous failure of an SCS or SRP/CS to perform a specified safety function over a given period of time

Note 1 to entry: The term PFH corresponds to the probability of dangerous failures per hour (PFH_D) of IEC 62061:2005, IEC 62061:2005/AMD1:2012, and IEC 62061:2005/AMD2:2015.

Note 2 to entry: The term "average probability of dangerous failure per hour" PFH_D is used in ISO 13894-1 and can be considered to be identical to the PFH according to the IEC 61508 series.

[SOURCE: IEC 61508-4:2010, 3.6.19, modified – Terminology adapted to machinery, existing notes deleted, new notes added]

3.1.5
common cause failure
CCF
failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel subsystem, leading to failure of a safety function

[SOURCE: IEC 61508-4:2010, 3.6.10, modified – Abbreviated term added, system failure replaced by failure of a safety function]

3.1.6
configuration management
discipline of identifying the components of an evolving system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the lifecycle

[SOURCE: IEC 61508-4:2010, 3.7.3, modified – Note removed]

3.1.7
continuous mode of operation
mode of operation where the safety function retains the machinery in a safe state as a part of normal operation

Note 1 to entry: Continuous mode means that a safety function is performed continuously, i.e., the SCS is continuously controlling the machine and a (dangerous) failure of its function can result in a hazard.

Note 2 to entry: The distinction between high demand and continuous mode is relevant for the qualification of diagnostic measures (refer to IEC 62061:2021, 7.4.3 and 7.4.4). It is not relevant for target failure measure and SIL assignment.

[SOURCE: IEC 61508-4:2010, 3.5.16, modified – The definition "continuous mode of operation" taken from the broader definition of "mode of operation", notes added]

3.1.8
dangerous failure
failure of an SCS or SRP/CS, a subsystem, or a subsystem element that plays a part in implementing the safety function that:

a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the machine is put into a hazardous or potentially hazardous state; or

b) decreases the probability that the safety function operates correctly when required

[SOURCE: IEC 61508-4:2010, 3.6.7, modified – Terminology adapted to machinery]

3.1.9
demand
event that causes the SCS or SRP/CS to perform a safety function

Note 1 to entry: Demand mode means that a safety function is only performed on request (demand) in order to transfer the machine into a specified state. The SCS or SRP/CS does not influence the machine until there is a demand on the safety function.

Note 2 to entry: Demand rate (DR) or the frequency of demands is one of the main factor that is considered for assessing the demand mode, low or high. For this particular purpose, the demand rate (DR) can be identified with the rate of events, where harm would occur without intervention of the safety function. This rate may be lower than an actual rate of triggering the safety function during operation.

Note 3 to entry: For an emergency stop function, the demand mode is not defined. To determine the achieved SIL, the principle for evaluation of the selected demand mode of the other functions is usually applicable.

[SOURCE: IEC 62061:2021, 3.2.25, modified – "or SRP/CS" added]

3.1.10
diagnostic coverage
DC
fraction of dangerous failures detected by automatic on-line diagnostic tests

Note 1 to entry: The fraction of dangerous failures is computed by using the dangerous failure rates associated with the detected dangerous failures divided by the total rate of dangerous failures.

Note 2 to entry: The dangerous failure diagnostic coverage is computed using the following equation, where DC is the diagnostic coverage, λ_{DD} is the detected dangerous failure rate and $\lambda_{\mathrm{Dtotal}}$ is the total dangerous failure rate:

$$\mathrm{DC} = \frac{\Sigma\lambda_{\mathrm{DD}}}{\lambda_{\mathrm{Dtotal}}} \quad (1)$$

Note 3 to entry: This definition is applicable providing the individual components have constant failure rates.

[SOURCE: IEC 61508-4:2010, 3.8.6, modified – The second part of the definition has been moved to a note to entry]

3.1.11
diagnostic function
function intended to detect faults in the SCS or SRP/CS and initiate a specified fault reaction function when a fault is detected

Note 1 to entry: This function is intended to detect faults that could lead to a dangerous failure of a safety function and initiate a specified fault reaction function.

[SOURCE: IEC 62061:2021, 3.2.19, modified – "or SRP/CS" added]

3.1.12
diagnostic test interval
interval between on-line tests to detect faults in a subsystem that has a specified diagnostic coverage

[SOURCE: IEC 61508-4:2010, 3.8.7, modified – Replacing safety-related system by subsystem]

3.1.13
embedded software
software, supplied as part of a pre-designed subsystem, that is not intended to be modified and that relates to the functioning of, and services provided by, the SCS or SRP/CS or subsystem, as opposed to the application software

Note 1 to entry: Firmware and system software are examples of embedded software.

[SOURCE: IEC 62061:2021, 3.2.60, modified – "or SRP/CS" added]

3.1.14
failure
termination of the ability of an item (SCS or SRP/CS, a subsystem or a subsystem element) to perform a required function

Note 1 to entry: Failures are either random (in hardware) or systematic (in hardware or software).

Note 2 to entry: After a failure, the item has a fault.

Note 3 to entry: "Failure" is an event, as distinguished from "fault", which is a state.

Note 4 to entry: The concept of failure as defined does not apply to items consisting of software only.

[SOURCE: ISO 12100:2010, 3.34, modified – "(SCS or SRP/CS, a subsystem or a subsystem element)" added and note 1 to entry added]

3.1.15
fault
abnormal condition that may cause a reduction in, or loss of, the capability of an SCS or SRP/CS, a subsystem, or a subsystem element to perform a required function

Note 1 to entry: In IEC 60050-192:2015, 192-04-01 a fault of an item is described as inability to perform as required, due to an internal state.

[SOURCE: IEC 61508-4:2010, 3.6.1, modified – Terminology adapted to machinery, note shortened]

3.1.16
fault reaction function
function that is initiated when a fault within an SCS or SRP/CS is detected by the SCS or SRP/CS diagnostic function

[SOURCE: IEC 62061:2021, 3.2.20, modified – "or SRP/CS" added to the definition]

3.1.17
fault tolerance
ability of an SCS or SRP/CS, a subsystem, or subsystem element to continue to perform a required function in the presence of faults or failures

[SOURCE: IEC 61508-4:2010, 3.6.3, modified – Terminology adapted to machinery, note to entry omitted]

3.1.18
full variability language
FVL
type of language that provides the capability to implement a wide variety of functions and applications

Note 1 to entry: Typical example of systems using FVL are general-purpose computers.

Note 2 to entry: FVL is normally found in embedded software and is rarely used in application software.

Note 3 to entry: FVL examples include: Ada, C, Pascal, Instruction List, assembler languages, C++, Java, SQL.

[SOURCE: IEC 61511-1:2016, 3.2.75.3, modified – First part of definition omitted and link to process sector deleted]

3.1.19
functional safety
part of the overall safety of the machine and the machine control system that depends on the correct functioning of the SCS or SRP/CS and other risk reduction measures

[SOURCE: IEC 61508-4:2010, 3.1.12, modified – Using terms machine, machine control system, SCS and SRP/CS]

3.1.20
hardware fault tolerance
HFT
property of a subsystem to potentially lose the safety function upon at least N+1 faults

Note 1 to entry: A hardware fault tolerance of N means that N+1 faults of a subsystem could cause a loss of the safety function.

[SOURCE: IEC 62061:2021, 3.2.35]

3.1.21
hardware safety integrity
part of the safety integrity of an SCS or its subsystems relating to random hardware failures in a dangerous mode of failure

Note 1 to entry: The term relates to failures in a dangerous mode, that is, those failures of a safety-related system that would impair its safety integrity.

Note 2 to entry: Hardware safety integrity includes architectural constraints.

[SOURCE: IEC 61508-4:2010, 3.5.7, modified – Terminology adapted to machinery, note 1 shortened, note 2 added]

3.1.22
harm
physical injury or damage to health

[SOURCE: ISO 12100:2010, 3.5]

3.1.23
hazard
potential source of harm

Note 1 to entry: The term "hazard" can be qualified in order to define its origin (for example, mechanical hazard, electrical hazard) or the nature of the potential harm (for example, electric shock hazard, cutting hazard, toxic hazard, fire hazard).

Note 2 to entry: The hazard envisaged by this definition either

- is permanently present during the intended use of the machine (for example, motion of hazardous moving elements, electric arc during a welding phase, unhealthy posture, noise emission, high temperature), or
- can appear unexpectedly (for example, 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).

Note 3 to entry: The French term "phénomène dangereux" should not be confused with the term "risque", which was sometimes used instead in the past.

[SOURCE: ISO 12100:2010, 3.6]

3.1.24
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]

3.1.25
hazard zone
danger zone
any space within and/or around machinery in which a person can be exposed to a hazard

[SOURCE: ISO 12100:2010, 3.11]

3.1.26
high demand mode of operation
mode of operation in which the frequency of demands of a safety function is greater than one per year

Note 1 to entry: Continuous mode means that a safety function is performed continuously, i.e., the SCS is continuously controlling the machine and a (dangerous) failure of its function can result in a hazard.

Note 2 to entry: The distinction between high demand and continuous mode is relevant for the qualification of diagnostic measures (refer to IEC 62061:2021, 7.4.3 and 7.4.4). It is not relevant for target failure measure and SIL assignment.

[SOURCE: IEC 61508-4:2010, 3.5.16, modified – The definition of "high demand mode of operation" taken from the definition of "mode of operation", notes added]

3.1.27
limited variability language
LVL
type of language that provides the capability to combine predefined, application specific, library functions to implement the safety requirements specifications

Note 1 to entry: A LVL provides a close functional correspondence with the functions required to achieve the application.

Note 2 to entry: Typical examples of LVL are given in IEC 61131-3. They include ladder diagram, function block diagram and sequential function chart. Instruction lists and structured text are not considered to be LVL.

Note 3 to entry: Typical example of systems using LVL: programmable logic controller (PLC) configured for machine control.

3.1.28
low demand mode of operation
mode of operation in which the frequency of demands of a safety function is no greater than one per year

[SOURCE: IEC 61508-4:2010, 3.5.16, modified – The definition of "low demand mode of operation" taken from the broader definition of "mode of operation"]

3.1.29
machinery
machine
assembly, fitted with or intended to be fitted with a drive system consisting of linked parts or components, at least one of which moves, and which are joined together for a specific application

Note 1 to entry: The term "machinery" also covers an assembly of machines which, in order to achieve the same end, are arranged and controlled so that they function as an integral whole.

[SOURCE: ISO 12100:2010, 3.1, modified – Note 2 to entry omitted]

3.1.30
machine control system
MCS
system that responds to input signals from the machinery and/or from an operator and generates output signals causing the machinery to operate in the desired manner

Note 1 to entry: The machine control system includes input devices and final elements.

[SOURCE: IEC 61508-4:2010, 3.3.3, modified – The term defined has been changed, "process" has been changed to "machinery"]

3.1.31
mean repair time
MRT
expected overall repair time after a fault has been detected in a safety function and machine continues to operate

Note 1 to entry: MRT encompasses:

- the time spent before starting the repair; and
- the effective time to repair; and
- the time before the component is put back into operation.

Note 2 to entry: Depending on the type of detected fault and the fault reaction, the numerical values for MRT and MTTR can be different.

[SOURCE: IEC 61508-4:2010, 3.6.22, modified – Terminology adapted to machinery and more details added to the definition, Note 1 made similar to IEC 62061:2021, 3.2.39, Note 2 added]

3.1.32
mean time to failure
MTTF
average value of expectation of the time to failure

[SOURCE: IEC 60050-192, 192-05-11, modified – "operating" removed from the term, "average value" added to the definition, and Original notes removed]

3.1.33
mean time to dangerous failure
$MTTF_D$
expectation of the mean time to dangerous failure

Note 1 to entry: Definition derived from IEC 60050-192:2015, 192-05-11 but restricted to dangerous failures.]

3.1.34
mean time to restoration
MTTR
expected time to achieve restoration after a fault has occurred in a safety function

Note 1 to entry: MTTR encompasses:

- the time to detect the failure (a); and
- the time spent before starting the repair (b); and
- the effective time to repair (c); and
- the time before the component is put back into operation (d).

The start time for (b) is the end of (a); the start time for (c) is the end of (b); the start time for (d) is the end of (c).

[SOURCE: IEC 61508-4:2010, 3.6.21, modified – Terminology adapted to machinery and more details added to definition]

3.1.35
pre-designed SCS or subsystem
SCS or subsystem which meets the relevant requirements of a functional safety standard

[SOURCE: IEC 62061:2021, 3.2.5]

3.1.36
probability of dangerous failure on demand
PFD
safety unavailability (see IEC 60050-192) of an SCS or SRP/CS to perform the specified safety function when a demand occurs from the machinery or machinery control system

Note 1 to entry: The [instantaneous] unavailability (as per IEC 60050-192) is the probability that an item is not in a state to perform a required function under given conditions at a given instant of time, assuming that the required external resources are provided. It is generally noted by U (t).

Note 2 to entry: The [instantaneous] availability does not depend on the states (running or failed) experienced by the item before t. It characterizes an item which only has to be able to work when it is required to do so, for example, an SCS working in low demand mode.

Note 3 to entry: If periodically tested, the PFD of an SCS is, in respect of the specified safety function, represented by a saw tooth curve with a large range of probabilities ranging from low, just after a test, to a maximum just before a test.

[SOURCE: IEC 61508-4:2010, 3.6.17, modified – Terminology adapted to machinery]

3.1.37
process safety time
period of time between a failure, that has the potential to give rise to a hazardous event, occurring in the machinery or machinery control system and the time by which action has to be completed in the machinery to prevent the hazardous event occurring

Note 1 to entry: It is foreseen that the safety function detects the failure and completes its action soon enough to prevent the hazardous event taking into account any process lag (e.g. stopping times).

[SOURCE: IEC 61508-4:2010, 3.6.20, modified – Terminology adapted to machinery, note 1 added]

3.1.38
proof test
periodic test that can detect dangerous undetected faults and degradation in an SCS or SRP/CS and its subsystems so that, if necessary, the relevant parts of the SCS or SRP/CS and its subsystems can be restored to an "as new" condition or as close as practical to this condition

Note 1 to entry: A proof test is intended to confirm that relevant parts of an SCS or SRP/CS are in a condition that assures the specified safety integrity.

Note 2 to entry: The effectiveness of the proof test will be dependent both on failure coverage and repair effectiveness. In practice, detecting 100 % of the degradation that could lead to the hidden dangerous failures later on is not easily achieved. For complex elements or safety features that are difficult to verify, a proof test coverage of 100 % is usually not possible.

[SOURCE: IEC 61508-4:2010, 3.8.5, modified – Terminology adapted to machinery, notes 1, 3, and 4 deleted, new note 1 added, and note 2 shortened]

3.1.39
protective measure
measure intended to achieve risk reduction

[SOURCE: ISO 12100:2010, 3.19, modified – bullet list removed]

3.1.40
random hardware failure
failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware

[SOURCE: IEC 61508-4:2010, 3.6.5, modified – Notes removed]

3.1.41
rarely activated safety function
safety function designed for high demand mode of operation where the frequency of demands is presumed to be at least one time per year, but can be sometimes less than one time per year

Note 1 to entry: When estimating the demand mode of operation, the demand rate is assumed to be at least one time per year: Nevertheless, it is possible that the safety function will not be demanded over the course of one year. The term "rarely activated safety function" reflects this special circumstance.

3.1.42
ratio of dangerous failure
RDF
fraction of the overall failure rate of an element that can result in a dangerous failure

[SOURCE: IEC 62061:2021, 3.2.55]

3.1.43
risk
combination of the probability of occurrence of harm and the severity of that harm

[SOURCE: ISO/IEC Guide 51:2014, 3.9, modified – note to entry removed]

3.1.44
safe failure
failure of an SCS or SRP/CS, a subsystem, or a subsystem element that plays a part in implementing the safety function that:

a) results in the spurious operation of the safety function to put the machine (or part thereof) into a safe state or maintain a safe state; or
b) increases the probability of the spurious operation of the safety function to put the machine (or part thereof) into a safe state or maintain a safe state

[SOURCE: IEC 61508-4:2010, 3.6.8, modified – Terminology adapted to machinery]

3.1.45
safe failure fraction
SFF
fraction of the overall failure rate of a subsystem that does not result in a dangerous failure

Note 1 to entry: The diagnostic coverage (if any) of each subsystem in SCS is taken into account in the calculation of the probability of random hardware failures. The safe failure fraction is taken into account when determining the architectural constraints on hardware safety integrity (see IEC 62061:2021, 7.4).

Note 2 to entry: "No effect failures" and "no part failures" (see IEC 61508-4) is not used for SFF calculations.

[SOURCE: IEC 62061:2021, 3.2.54, modified – The abbreviated term "SFF" has been formatted as a non-variable term]

3.1.46
safe state
state of the machine when safety is achieved

Note 1 to entry: The safe state doesn't include the restoration of initial equipment failures.

Note 2 to entry: IEC 62061 considers "fault reaction function" in the context of "safe state" of the machine. For HFT = 0 and SFF < 60 %, when upon detection of a dangerous failure a "safe state" cannot be achieved, warnings (or alarms) can be sufficient to inform the user exposed to the risk.

[SOURCE: IEC 62061:2021, 3.2.68, modified – Note 2 added]

3.1.47
safety
freedom from unacceptable risk

[SOURCE: IEC 61508-4:2010, 3.1.11]

3.1.48
safety function
function implemented by an SCS or SRP/CS with a specified integrity level that is intended to maintain the safe condition of the machine or prevent an immediate increase of the risk(s) in respect of a specific hazardous event

Note 1 to entry: This term is used instead of "safety-related control function (SRCF)" of IEC 62061:2015. This definition differs from ISO 12100 because this document addresses risk reduction performed by SCS or SRP/CS.

Note 2 to entry: A safety function is typically starting with a detection and evaluation of an "initiation event" and ending with an output causing a reaction of a "machine actuator".

Note 3 to entry: Parts of machine operating function(s), e.g. the reaction of a machine actuator, can also be part of safety function(s).

[SOURCE: IEC 61508-4:2010, 3.5.1, modified – Terminology adapted to machinery, other risk reduction measures deleted, example deleted, notes added]

3.1.49
safety integrity
probability of an SCS or SRP/CS or its subsystem satisfactorily performing the required safety function under all stated conditions within a stated period of time

Note 1 to entry: The higher the level of safety integrity of the item, the lower the probability that the item will fail to carry out the required safety function.

Note 2 to entry: Safety integrity comprises hardware safety integrity and systematic safety integrity.

[SOURCE: IEC 61508-4:2010, 3.5.4, modified – Terminology adapted to machinery, notes 2, 3, and 5 deleted]

3.1.50
safety integrity level
SIL
discrete level (one out of a possible three) for describing the capability to perform a safety function where safety integrity level three has the highest level of safety integrity and safety integrity level one has the lowest

[SOURCE: IEC 62061:2021, 3.2.24]

3.1.51
safety-related control system
SCS
part of the control system of the machine which implements a safety function by one or more subsystems

[SOURCE: IEC 62061:2021, 3.2.3]

3.1.52
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).

[SOURCE: ISO 13849-1:2015, 3.1.1]

3.1.53
safety-related software
software that is used to implement safety functions in a safety-related system

[SOURCE: IEC 62061:2021, 3.2.63]

3.1.54
security

a) measures taken to protect a system
b) condition of a system that results from the establishment and maintenance of measures to protect the system
c) condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss
d) capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems
e) prevention of illegal or unwanted penetration of, or interference with, the proper and intended operation of an industrial automation and control system

Note 1 to entry: Measures can be controls related to physical security (controlling physical access to computing assets) or logical security (capability to login to a given system and application).

[SOURCE: IEC TS 62443-1-1:2009, 3.2.99]

3.1.55
sub-function
part of a safety function whose failure can result in a failure of the safety function

[SOURCE: IEC 62061:2021, 3.2.36, modified – Note to entry removed]

3.1.56
subsystem
entity of the top-level architectural design of a safety-related system where a dangerous failure of the subsystem results in dangerous failure of a safety function

Note 1 to entry: This definition differs from common language where "subsystem" may mean any sub-divided part of an entity, the term "subsystem" is used in this document within a strongly defined hierarchy of terminology: "subsystem" is the first level subdivision of a system. The parts resulting from further subdivision of a subsystem are called "subsystem elements".

Note 2 to entry: A complete subsystem can be made up from a number of identifiable and separate subsystem elements.

Note 3 to entry: The subsystem specification includes its role in the safety function and its interface with the other subsystems of the SCS.

Note 4 to entry: One subsystem can be part of several safety functions, e.g. the same combination of contactors can be used to de-energise a motor either in the event of detection of a person in a danger zone or also in the event of opening an interlock guard.

[SOURCE: IEC 61508-4:2010, 3.4.4, modified – Cross references removed and notes added]

3.1.57
subsystem element
part of a subsystem, comprising a single component or any group of components

Note 1 to entry: A subsystem element may comprise hardware and software.

Note 2 to entry: Elements that are not directly necessary for the safety function are not included, but may support it (for example, filters elements, protection against over-voltage).

Note 3 to entry: A subsystem element is the lowest level of detail to consider when ensuring that the requirements of a sub-function are met.

[SOURCE: IEC 62061:2021, 3.2.6]

3.1.58
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 and/or operation of the hardware;
- the design and/or implementation of the software.

[SOURCE: IEC 61508-4:2010, 3.6.6, modified – note 3 slightly changed, note 4 removed]

3.1.59
systematic safety integrity
part of the safety integrity of an SCS or SRP/CS or its subsystems relating to its resistance to systematic failures in a dangerous mode of failure

Note 1 to entry: Systematic safety integrity cannot usually be quantified precisely.

Note 2 to entry: Requirements for systematic safety integrity apply to both hardware and software aspects of an SCS or its subsystems.

[SOURCE: IEC 61508-4:2010, 3.5.6, modified – Terminology adapted to machinery, note 1 shortened, note 2 added]

3.1.60
target failure measure
intended PFH or PFD_{avg} to be achieved to meet a specific safety integrity requirement(s)

Note 1 to entry: Target failure measure is specified in terms of:

– the average probability of a dangerous failure of the safety function on demand, (for a low demand mode of operation);

– the average frequency of a dangerous failure [h^{-1}] (for a high demand mode of operation or a continuous mode of operation).

[SOURCE: IEC 61508-4:2010, 3.5.17, modified – "target probability of dangerous mode failures" changed to "intended PFH or PFD_{avg}", bullet list moved to note 1, existing note deleted]

3.1.61
useful lifetime
minimum elapsed time between the installation of the SCS or SRP/CS or subsystem or subsystem element and the point in time when component failure rates of the SCS or SRP/CS or subsystem or subsystem element can no longer be predicted, with any accuracy

Note 1 to entry: Typically it will be 20 years or less unless the manufacturers of the SCS and its subsystems can justify a longer lifetime by providing evidence, based on calculations, showing that reliability data is valid for the longer lifetime.

[SOURCE: IEC 61131-6:2012, 3.57, modified – The term "worst case" omitted, terminology adapted to machinery, note 1 added, example deleted]

3.1.62
validation
<of the safety function> confirmation by examination (e.g. tests, analysis) that the SCS or SRP/CS meets the functional safety requirements of the specific application

[SOURCE: IEC 61508-4:2010, 3.8.2, modified – The domain "of the safety function" added, Terminology adapted to machinery, notes deleted]

3.1.63
verification
confirmation by examination (e.g. tests, analysis) that the SCS or SRP/CS, its subsystems or subsystem elements meet the requirements set by the relevant specification

Note 1 to entry: Initial verification of safety-related control system (SCS) according to IEC 62061 or safety-related parts of a control system (SRP/CS) according to ISO 13849-1 is performed before being placed into service. Initial verification corresponds to the validation process described in IEC 62061:2021, Clause 9 or in ISO 13849-1:2015, Clause 10.

Note 2 to entry: Periodic verification of safety-related control system (SCS) according to IEC 62061 or safety-related parts of a control system (SRP/CS) according to ISO 13849-1 is performed at regular intervals during the operation of the SCS or SRP/CS. IEC 62061:2021, 6.9 "periodic tests" are part of periodic verification.

EXAMPLE: Verification activities include

- reviews on outputs (documents from all phases) to ensure compliance with the objectives and requirements of the phase, taking into account the specific inputs to that phase;
- design reviews;
- tests performed on the designed products to ensure that they perform according to their specification;
- integration tests performed where different parts of a system are put together in a step-by-step manner and by the performance of environmental tests to ensure that all the parts work together in the specified manner.

[SOURCE: IEC 62061:2021, 3.2.64, modified – "or SRP/CS", note 1 and note 2 added]

3.1.64
well-tried component
component for a safety-related application which has been either

a) widely used in the past with successful results in similar safety-related applications as given as well-tried components in the informative annexes of ISO 13849-2, or
b) made and verified using principles which demonstrate its suitability and reliability for safety-related applications

Note 1 to entry: ISO 13849-2 lists a variety of components and the conditions for specific technologies under which the component can be considered well-tried.

Note 2 to entry: Newly developed components may be considered as equivalent to "well-tried" if they fulfil the conditions of b).

Note 3 to entry: The decision to accept a particular component as being "well-tried" depends on the application, e.g. owing to the environmental influences and can be impacted by product or manufacturer changes.

Note 4 to entry: Complex electronic components (e.g. PLC, microprocessor, application-specific integrated circuit) cannot be considered as equivalent to "well tried".

Note 5 to entry: A well-tried component is not a proven in use component.

[SOURCE: IEC 62061:2021, 3.2.43]

3.1.65
well-tried safety principles
principles that have proved effective in the design or integration of safety-related control systems in the past, to avoid or control critical faults or failures which can influence the performance of a safety function

Note 1 to entry: Newly developed safety principles can be considered as equivalent to "well-tried" if they are verified using principles which demonstrate their suitability and reliability for safety-related applications.

Note 2 to entry: Well-tried safety principles are effective not only against random hardware failures, but also against systematic failures which may creep into the product at some point in the course of the product life cycle, e.g. faults arising during product design, integration, modification or deterioration.

Note 3 to entry: Tables A.2, B.2, C.2 and D.2 in the informative annexes of ISO 13849-2:2012 address well-tried safety principles for different technologies.

[SOURCE: IEC 62061:2021, 3.2.44]

3.2 Alphabetical list of terms, definitions and abbreviated terms

Terms used throughout this document are given in Table 1. Also included are some common abbreviated terms related to machinery safety.

Table 1 – Terms used in this document

Term	Definition number
application software	3.1.1
architectural constraint	3.1.2
architecture	3.1.3
average frequency of dangerous failure per hour (PFH)	3.1.4
common cause failure (CCF)	3.1.5
configuration management	3.1.6
continuous mode	3.1.7
dangerous failure	3.1.8
demand	3.1.9
diagnostic coverage (DC)	3.1.10
(SCS or SRP/CS) diagnostic function	3.1.11
diagnostic test interval	3.1.12
embedded software	3.1.13
failure	3.1.14
fault	3.1.15
(SCS or SRP/CS) fault reaction function	3.1.16
fault tolerance	3.1.17
full variability language (FVL)	3.1.18

Term	Definition number
functional safety	3.1.19
hardware fault tolerance (HFT)	3.1.20
hardware safety integrity	3.1.21
harm	3.1.22
hazard	3.1.23
hazardous situation	3.1.24
hazard zone	3.1.25
high demand mode of operation	3.1.26
limited variability language (LVL)	3.1.27
low demand mode	3.1.28
machinery (machine)	3.1.29
machine control system (MCS)	3.1.30
mean repair time (MRT)	3.1.31
mean time to failure (MTTF)	3.1.32
mean time to dangerous failure ($MTTF_D$)	3.1.33
mean time to restoration (MTTR)	3.1.34
pre-designed (SCS or subsystem)	3.1.35
probability of dangerous failure on demand (PFD)	3.1.36
process safety time	3.1.37
proof test	3.1.38
protective measure	3.1.39
random hardware failure	3.1.40
rarely activated safety function	3.1.41
ratio of dangerous failure (RDF)	3.1.42
risk	3.1.43
safe failure	3.1.44
safe failure fraction (SFF)	3.1.45
safe state	3.1.46
safety	3.1.47
safety function	3.1.48
safety integrity	3.1.49
safety integrity level (SIL)	3.1.50
safety-related control system (SCS)	3.1.51
safety-related parts of a control system (SRP/CS)	3.1.52
safety-related software	3.1.53
security	3.1.54
sub-function	3.1.55
subsystem	3.1.56
subsystem element	3.1.57
systematic failure	3.1.58
systematic safety integrity	3.1.59
target failure measure	3.1.60
useful lifetime	3.1.61
validation (of the safety function)	3.1.62

Term	Definition number
verification	3.1.63
well-tried component	3.1.64
well-tried safety principles	3.1.65

4 Typical classification of safety functions in safety of machinery

4.1 General

4.1.1 Overview

The risk assessment process is realized by applying ISO 12100 to define safety functions.

NOTE Additional guidance given in all subclauses of this document are based on safety functions designed according to IEC 62061 or ISO 13849-1.

4.1.2 Risk assessment and risk reduction according to ISO 12100

ISO 12100 is a fundamental safety standard that provides an overall framework and guidance for the design of machines that are safe for their intended use. It gives provisions:

– for identification of the hazards and for estimation and evaluation of the risks associated with the machine;
– on how to remove hazards or provide sufficient risk reduction:
– and guidance on the documentation and verification of the risk assessment and risk reduction achieved.

If the hazard cannot be removed and is necessary to reduce the risk associated with the hazard by implementing protective measures, such protective measures shall be applied in the following sequence, referred to as the three-step risk reduction strategy:

– Step 1: Inherently safe design measures;
– Step 2: Safeguarding and/or complementary protective measures;
– Step 3: Information for use.

ISO 12100 also provides a strategy for standards developers for the preparation of consistent and appropriate type-B and type-C standards.

ISO 12100 is a type-A standard and, according to this classification, IEC 62061 and ISO 13849-1, and ISO 13849-2 are type-B1 standards.

NOTE 1 ISO 12100 is the basis for a set of standards which has the following structure:

– Type-A standards (basic safety standards) giving basic concepts, principles for design and general aspects that can be applied to machinery;
– Type-B standards (generic safety standards) dealing with one safety aspect or one type of safeguard that can be used across a wide range of machinery:
  - Type-B1 standards on particular safety aspects (for example, safety distances, surface temperature, noise);
  - Type-B2 standards on safeguards (for example, two-hand controls, interlocking devices, pressure-sensitive devices, guards);
– Type-C standards (machine safety standards) dealing with detailed safety requirements for a particular machine or group of machines.

NOTE 2 Additional information on the relationship between ISO 13849-1 and ISO 12100 can be found in ISO/TR 22100-2. This relationship is also valid for IEC 62061.

NOTE 3 Many local regulations are referencing or linked to ISO 12100, IEC 62061 or ISO 13849-1. Annex I gives an overview of different regulatory approaches regarding safety of machinery.

When a type-C standard deviates from one or more technical provisions dealt with by this document or by a type-B standard, the type-C standard takes precedence.

Annex A describes the basic approach of ISO 12100 in the context of functional safety.

4.1.3 Risk reduction and interconnection to SCS and SRP/CS

IEC 62061, ISO 13849-1, ISO 13849-2, and this document are used in the context of the three-step risk reduction process as described in ISO 12100.

These standards provide requirements for the

– design of an SCS or SRP/CS and associated safety functions,
– calculation of the SIL or of the PL of the safety function based on the technology used,
– verification and validation of the SIL or PL reached,
– instructions for the safe use, and
– guidance for the determination of the safety integrity required.

Figure 1 shows the integration of SCS or SRP/CS within the risk reduction process as described in ISO 12100.

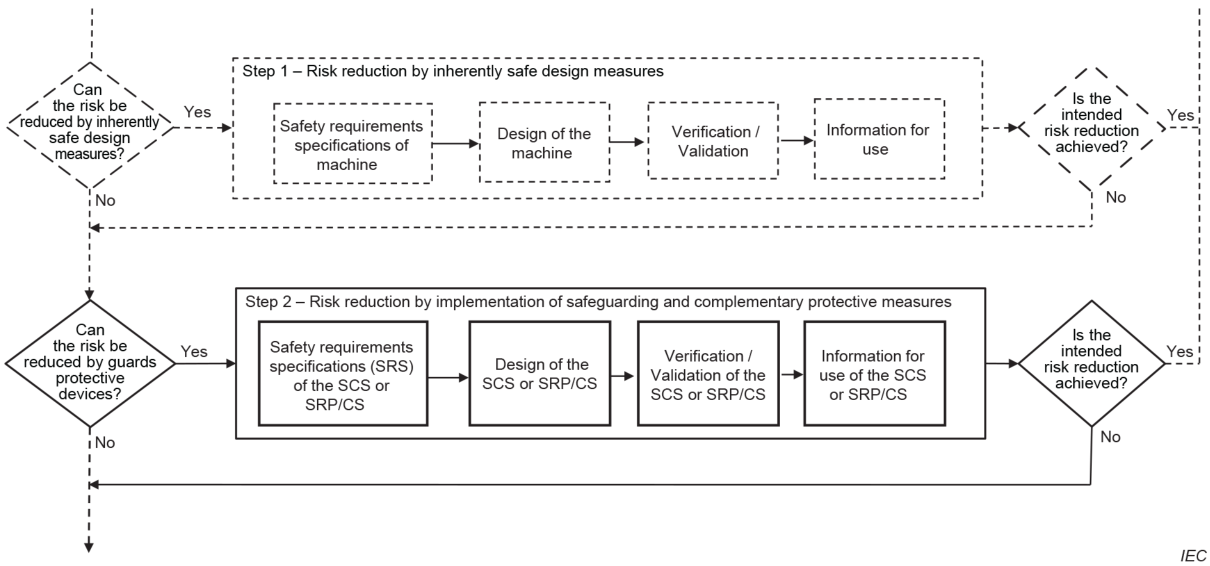


Figure 1 – Integration within the risk reduction process of ISO 12100

4.1.4 Basic assumptions for risk reduction in machinery

The following basic assumptions for applying risk reduction in machinery are:

– the non-safety-related parts of the machine control system (MCS) are not considered in the context of any kind of risk reduction;
– for direct or indirect protection of persons the demand of safety functions is estimated and high demand mode of operation is taken as the basis for evaluation;
– SCS or SRP/CS is the protective measure based on a control system to reduce risks;
– a restart of the machinery is allowed only if a safe condition is guaranteed.

4.2 Basic safety assumptions for the design and integration of the SCS or SRP/CS

For the design of the SCS or SRP/CS any of the technologies available (electric, hydraulic, pneumatic, mechanical, etc.) individually or in combination may be used.

An SCS or SRP/CS is usually made up of one or more sensors (or push-buttons or switches), a decision-making logic and one or more action devices.

Figure 2 shows a typical example of an SCS or SRP/CS decomposed into three subsystems performing respectively the tasks of detection, evaluation, and initiating action.

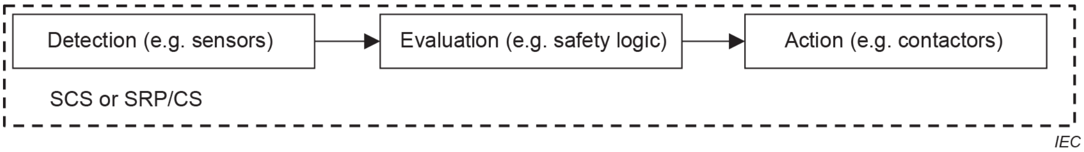


Figure 2 – Decomposition of an SCS or SRP/CS

For the integration of an SCS or SRP/CS the following principles shall be applied:

– The SCS or SRP/CS is separated and independent from the non-safety-related parts of the machine control system (MCS).

  NOTE In a few exceptions the SCS or the SRP/CS can perform safety functions which also control the process, e.g. two-hand control.

– The SCS or SRP/CS is only intended for direct or indirect protection of persons; it does not take an active part in the machine process and is activated only when a dangerous situation occurs.

– The reliability of the non-safety-related parts of the machine control system (MCS) are not included in the evaluation of the safety function. It is the reliability of the SCS or SRP/CS that is of concern.

– Upon detection of a dangerous fault in the SCS or SRP/CS the machine is brought to a safe state. Restarting the machine process is accepted only after repair and restoration of the SCS or SRP/CS.

4.3 Safety functions

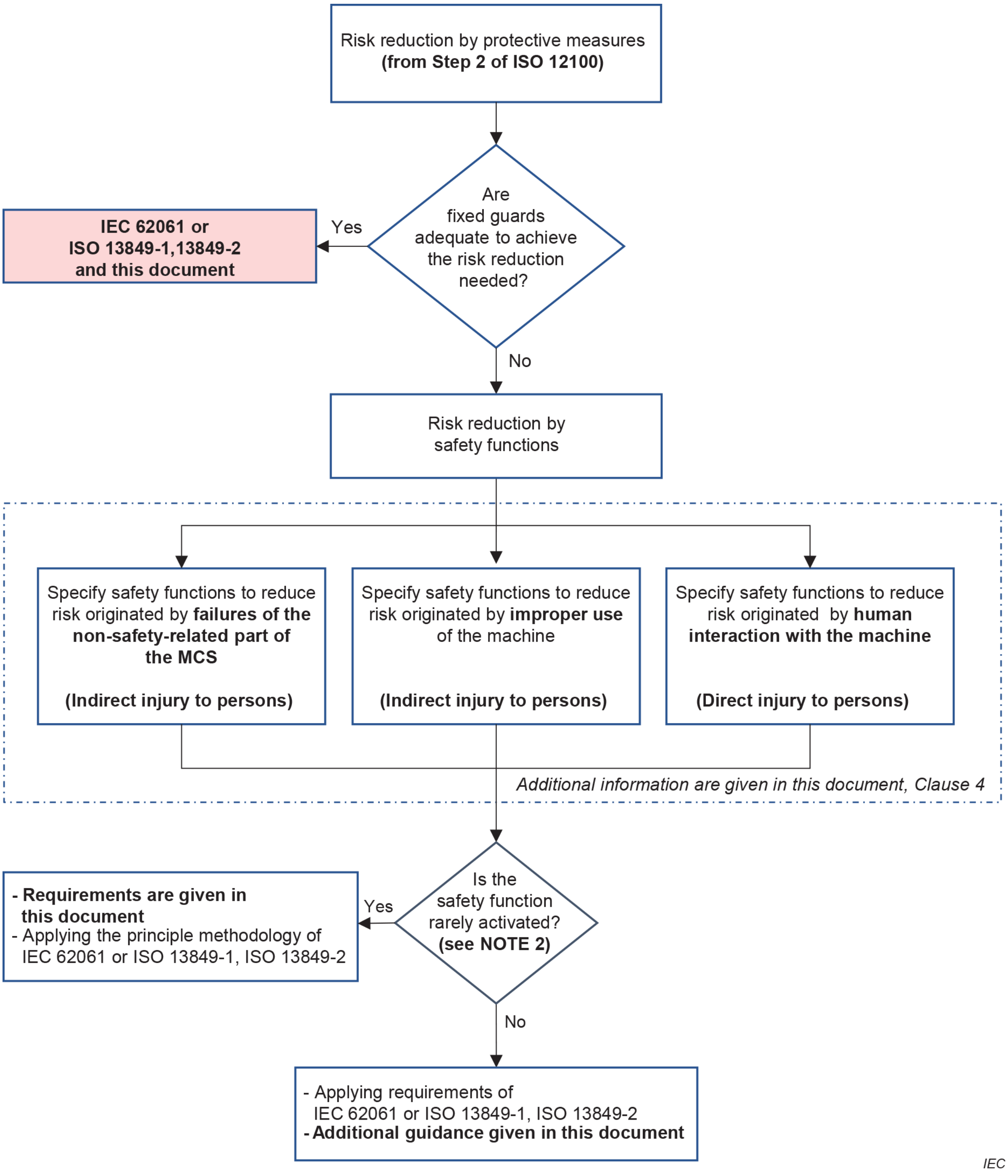
4.3.1 General

SCS or SRP/CS that perform one or more protective measures are said to perform a safety function.

When a safety function is activated, the machine shall be brought to a safe state before a hazardous situation can occur.

4.3.2 Risk reduction process by safety functions

Figure 3 shows the Step 2 of the iterative risk reduction process of ISO 12100 by means of safety functions as protective measures. Further information is given in Annex A.



MCS, machine control system

NOTE Depending on the protective measure selected, for the design of the SCS or SRP/CS application of additional International Standards such as IEC 62046, ISO 13851, ISO 14119, ISO 13856 can be necessary.

Figure 3 – Risk reduction process by safety functions

4.3.3 Typical classification of safety functions

In general, all safeguarding or complementary protective measures implemented according to ISO 12100 can be classified into three types of safety functions:

- Safety functions to reduce risks originated by man-machine interactions. They are employed as a means of protection of the human body or parts of the body and are intended to work immediately upon a specific initiating event. Their role is to ensure that the person is not injured by the dangerous parts of the machine (safety functions for protection of persons, see 4.5).
- Safety functions to reduce risks originated by failures of the MCS. They are employed as a means of prevention and are intended to work before a specific initiating event takes place. Their role is to ensure that the accident does not happen, or at least to slow down its development or to limit to an acceptable level the deviation of the process (other safety functions to prevent hazardous situations, see 4.6);
- Safety functions to reduce risks originated by improper use of the machine. They are intended to reduce the risk of mechanical catastrophic failures originated by high stress or excessive workload (safety functions for protection of the integrity of the machine, see 4.7).

Safety functions can be implemented individually or in combination according to the machine and to the process.

For complex machines a person may be exposed to risks of translation, rotation, clamping due to faults occurring in the MCS. Whether the faults can lead to a hazardous situation depends on the mutual position of the person and of the dangerous movements of the machine.

The result of the risk assessment will determine which safety function, or combination of safety functions need to be implemented and in which sequence.

4.4 Interrelation between ISO 12100 and IEC 62061 or ISO 13849-1

4.4.1 General

For the correct application of IEC 62061 or ISO 13849-1, input information resulting from the application of the overall risk assessment and risk reduction process for the particular machine design is necessary. Based on this input information the SCS or SRP/CS can be appropriately designed. Information resulting from a detailed design of the SCS or SRP/CS for its integration into the machine design shall then be considered in the overall risk assessment and risk reduction process according to ISO 12100.

4.4.2 Input information in accordance with IEC 62061 or ISO 13849-1

Table 2 gives an overview of the required input information for SCS or SRP/CS design according to IEC 62061 or ISO 13849-1.

This input information will be used to generate the safety requirements specification (SRS).

NOTE Table 2, Table 3, Table 4, Table 5 and Table 6 can be used as templates for documentation in which empty fields can contain specific information related to the application.

Table 2 – Input information for the safety requirements specification (SRS)

Information on (clause of ISO 12100)	**Main items to be considered**	**Input information** **Source of requirement**	**Output information** **Where information can be found**
Limits of the machine (ISO 12100:2010, 5.3)	1) use limits, 2) space limits, 3) time limits, 4) other limits (e.g. environmental conditions).		
The risk associated with a particular hazardous situation (ISO 12100:2010, 5.4, 5.5.2)	1) severity of harm; 2) probability of occurrence of that harm, which is a function of; • exposure of person(s) to the hazard, • occurrence of a hazardous event, • technical and human possibilities to avoid or limit the harm.		
Specifications for the intended performance of the related risk reduction/protective measure	1) general prescription of the intended function of the risk reduction / protective measure (relevant functional requirements), 2) specific safety-related characteristics for the risk reduction / protective measure (e.g. reaction time, operating modes, solicitation), 3) prescription of the environmental conditions relevant for the risk reduction / protective measure (e.g. space limitation, temperature, humidity, vibration), 4) prescription of other machine and/or process specific conditions (e.g. designated safety-related components).		

4.4.3 Output information from IEC 62061 or ISO 13849-1

Table 3 gives an overview of the required output information based on SCS or SRP/CS design according to IEC 62061 or ISO 13849-1.

Table 3 – Output information from SCS or SRP/CS design on overall risk assessment

Information on (clauses of IEC 62061 and ISO 13849-1)	**Main items to be considered**	**Input information** **Source of requirement**	**Output information** **Where information can be found**
Confirmation that the intended risk reduction is achieved by the technical solution (IEC 62061:2021, Clause 9) (ISO 13849-1:2015, Clause 9)	Results of the verification and validation of SCS according to IEC 62061 or SRP/CS of ISO 13849-1		
Technical documentation (IEC 62061:2021, Clause 10) (ISO 13849-1:2015, Clause 10)	Technical documentation for integration/assembly of the technical solution into the machine design		
Information for use (IEC 62061:2021, Clause 10) (ISO 13849-1:2015, Clause 11)	All relevant information to be given from the machine designer to the machine user to ensure the correct use SCS or SRP/CS and interrelated risk reduction/protective measures		

4.5 Safety functions for protection of persons

4.5.1 General

Guards and protective devices shall be used to protect persons whenever inherently safe design measures do not remove hazards or sufficiently reduce risks. Complementary protective measures involving additional equipment (for example, emergency stop equipment) may have to be implemented.

NOTE In Table 4, Table 5 and Table 6, the list of safety functions is based on ISO 12100 but other type-B standards (e.g. ISO 13849-1), type-C standards or other IEC International Standards also have similar definitions or requirements.

4.5.2 Safety functions for protection of persons based on guards and protective devices

Based on guards and protective devices, the safety functions designed to protect persons can include, but are not limited to those in Table 4.

Table 4 – Safety functions for protection of persons

Safety functions for protection of persons	Main items to be considered Initiation by	Demand rate (low, high, rarely activated)	Input information Source of requirement	Output information Where information can be found
Safety-related stopping Guards (ISO 12100:2010, 6.3.2.3)	Access to the hazard zone is required during normal operation – Interlocking Guard – Interlocking Guard with guard locking – Interlocking guard with a start function (with manual reset function)		ISO 14119	
Safety-related stopping Protective devices (ISO 12100:2010, 6.3.2.2)	Access to the hazard zone can be required during normal operation: – Sensitive protective equipment (SPE) – Sensitive protective equipment (SPE), muting – Pressure-sensitive protective devices		IEC 61496 IEC TS 62998-1 IEC 62046 ISO 13856	
Manually operated control system Manual handling (ISO 12100:2010, 6.3.2.3)	Access to the hazard zone is required during normal operation – Device with reset (push button) – Hold-to-run control device – Two-hand control device		ISO 11161 IEC 60947-5-8 ISO 13851	
Adjusting, teaching, retooling, fault finding, maintenance, cleaning Manual control (ISO 12100:2010, 6.3.2.4)	Access to the hazard zone is required during specific operation, like machine setting, teaching, etc. – Enabling device – Limited movement control device for reduced speed or power/force		IEC 60947-5-8 IEC 61800-5-2	

4.6 Other safety functions to prevent hazardous situations

4.6.1 General

In addition to safety functions which protect persons directly due to interaction, other safety functions exist, which can be indirectly important to prevent hazardous situations and which shall be considered in addition to the safety functions for the protection of persons.

4.6.2 Other safety functions

Other safety functions can include, but are not limited to those listed in Table 5.

Table 5 – Other safety functions

Other safety functions	**Main items to be considered** **Initiation by**	**Demand rate** **(low, high, rarely activated)**	**Input information** **Source of requirement**	**Output information** **Where information can be found**
Local control function Selecting of local control (ISO 13849-1:2015, 5.2.4)	Access to the hazard zone is required during normal operation or specific operation, like machine setting, teaching, etc. – Manual local control device (and procedure)			
Safety-related parameters Selecting of parameters (ISO 12100:2010, 6.3.2.7)	Access to the hazard zone is required during normal operation or specific operation, like machine setting, teaching, etc.; complementary protective measures – Manual parameter selection device (and procedure)			
Requirements for operating mode selection Control and operating modes (ISO 12100:2010, 6.2.11.10)	Access to the hazard zone is required during normal operation or specific operation, like machine setting, teaching, etc. – Manual operating mode selection device (and procedure)			
Emergency stop functions Emergency situations (ISO 12100:2010, 6.3.5.2)	Additional complementary protective measure to avert emergency situations (is considered as a safety function) – Emergency stop device		ISO 13850	
Fluctuations, loss and restoration of power sources Control measures related to energy sources (ISO 12100:2010, 6.2.11.5, 6.3.2.4, 6.3.5.4)	Access to the hazard zone is required during normal operation or specific operation, like machine setting, teaching, etc.; general consideration regarding control measures related to energy sources – Energy control device (and procedure)		ISO 14118	

4.7 Safety functions for protection of the integrity of the machine

4.7.1 General

When a machine requires continuous control by the operator (for example, mobile machines, cranes) and an error of the operator can generate a hazardous situation, this machine shall be equipped with the necessary devices to enable the operation to remain within specified limits, in particular

- when the operator has insufficient visibility of the hazard zone,
- when the operator lacks knowledge of the actual value of a safety-related parameter (distance, speed, mass, angle, etc.), and
- when hazards can result from operations other than those controlled by the operator.

Automatic protective measures triggered by such devices that take operation of the machinery out of the control of the operator (for example, automatic stop of hazardous movement) should be preceded or accompanied by a warning signal to enable the operator to take appropriate action (see ISO 12100:2010, 6.3.2.7).

4.7.2 Safety functions for the protection of integrity of the machine

The following safety functions for the protection of integrity of the machine can include, but are not limited to, those listed in Table 6.

Table 6 – Safety functions for the protection of integrity of the machine

Safety functions for protection of integrity of the machine	Main items to be considered Initiation by	Demand rate (low, high, rarely activated)	Input information Source of requirement	Output information Where information can be found
Limited Operation Other protective devices (ISO 12100:2010, 6.3.2.7)	Hazards can result from operations and protective measures are triggered automatically (independent of the operator) – Devices to prevent collisions or interference with other machines – Devices to ensure that components are in a safe position before travelling			
Operation to remain within specified limits Other protective devices (ISO 12100:2010, 6.3.2.7)	Hazards can result from operations which indirectly can harm persons and protective measures are triggered automatically (independent of the operator) – Torque limiting devices, and breakage points to prevent excessive stress of components and assemblies – Devices for limiting parameters of movement (distance, angle, velocity, acceleration) – Overloading and moment limiting devices – Devices for limiting pressure or temperature – Devices for monitoring emissions			

4.8 Safety functions and Type-C standards

Type-C standards can define safety functions where technical requirements can deviate from ISO 12100. In this case type-C standards take precedence.

5 Demand mode of operation related to safety functions

5.1 General

Each safety function to be performed by an SCS (designed according to IEC 62061) or SRP/CS (designed according to ISO 13849-1) shall be considered to operate in either high demand mode of operation (see 5.2) or low demand mode of operation (see 5.3).

NOTE 1 Information given in this Clause 5 is based on safety functions designed according to IEC 62061 or ISO 13849-1.

NOTE 2 Owing to the variety of machines, the demand rate of safety functions to protect persons is not known (it varies between on time per hour and one time per year). Safety functions are therefore assumed to be in high demand mode of operation.

Functions to protect the machine are typically demanded less than one time per year because the machine is designed by incorporating some safety basic principles in order to comply with the requirements of ISO 12100.

These protection functions can be classified as safety functions when the consequence of the risk is a direct or indirect injury to persons in the environment of the machine.

NOTE 3 These protection/safety functions are assumed to be in high demand mode of operation because the hazardous situation will be prevented immediately by e.g. stopping dangerous movements of the machine and also because these safety functions in machinery are the only risk reduction measure and no other "layer of protection" is considered.

Because of these differences between safety functions to protect persons against direct injuries and protection functions to protect persons against indirect injuries, the test criteria of the safety/protection functions can deviate from the those defined in IEC 62061:2021, 7.3.3.4.

NOTE 4 When a functional test for non-electronic technology is necessary to detect a possible accumulation of faults or an undetected fault before the next demand, IEC 62061, 7.3.3.4 requires the following test intervals:

– at least every month for SIL 3;
– at least every 12 months for SIL 2.

5.2 High demand or continuous mode of operation

5.2.1 General

The machine control system (MCS) performing the manufacturing process is considered to be independent of the SCS or SRP/CS. There may be an interaction, but no account is taken of the machine control system to reduce the risk evaluation of SCS or SRP/CS and to be part of risk reduction measures(s).

The interaction of the operator of a machine is assumed as not being part of any kind of protection of layer view, as applied in low demand mode of operation (see Figure 4).

The following reasons are applied:

– Safety functions implemented for machines are mainly intended to protect persons;
– Operators do not need detail information of the design of the safety function and its related SCS or SRP/CS;
– Safety functions can be manually operated, e.g. two-hand control;
– Demand rate of a safety function is high, at least one time per year;
– Reaction time of safety function is typically short.

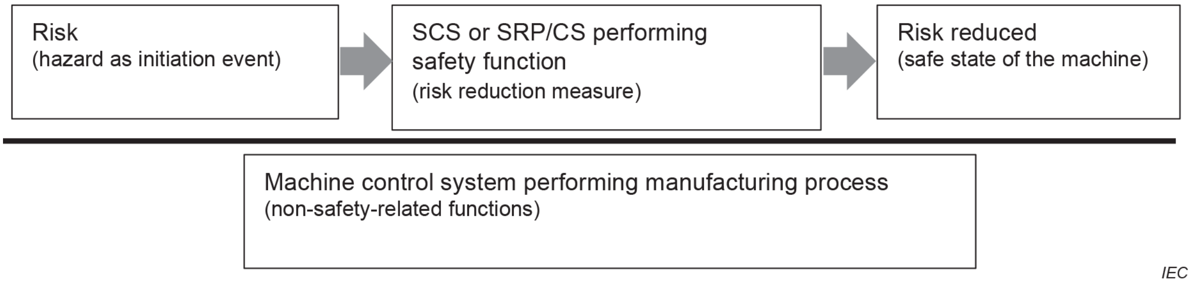


Figure 4 – High demand mode of operation

5.2.2 Approach of IEC 62061 and ISO 13849-1

Design, integration and installation of SCS or SRP/CS are based on high demand or continuous mode of operation. Evaluation of PFH or PFH_D values for subsystems is based on high demand or continuous mode of operation.

5.2.3 Rarely activated safety functions

5.2.3.1 General

Where high demand mode of operation is used, a high demand rate of a safety function is assumed in terms of "average". Nevertheless, it can occur that the assumed demand of a safety function is not performed in one year; this may occur when the machine manufacturer is presuming the average demand rate to ensure the safety integrity as a kind of worst-case consideration when determining the required safety integrity.

Those safety functions which are designed for high demand mode of operation but which sometimes might not be demanded during one year are called "rarely activated safety functions".

Rarely activated safety functions are designed, implemented and integrated as safety functions in high demand mode of operation.

Rarely activated safety functions (see B.12.2.5) which are event triggered require measures against fault accumulation and undetected faults.

Periodic verification is necessary to ensure the safety integrity of these not-yet-demanded safety functions, see also 7.5.2.

For the demand mode of operation for rarely activated safety functions, additional information is provided in Clause 6 and Clause 7 of this document.

5.2.3.2 Basic requirements

NOTE 1 For rarely activated safety functions the evaluation of PFH value based on the B_{10}/B_{10D} value will not limit the reachable SIL or PL as $MTTF_D$ is higher than 2 000 years or λ_D smaller than 5E-08, see IEC 62061:2021, Table H.2.

The diagnostic test interval of a safety function is linked to the demand rate and the diagnostics only occur when a safety function is demanded. Therefore, periodic verification procedures are necessary to detect an accumulation of undetected faults, see Clause 7.

For safety functions protecting the machine a diagnostic test interval of up to 2 years may be used if the following conditions are met to minimize the possibility of accumulation of faults or an undetected fault before the next demand:

a) provide justification that environmental effects do not reduce the lifetime of the components, e.g., corrosions, leakage, problems on sealings;

AND

b) for each subsystem SIL 1 / PL_r c and SIL 2 / PL_r d use a minimum architecture of HFT = 1 / Category 3;

OR

c) for each subsystem SIL 3/PL_r e use a minimum architecture of HFT = 1 / Category 3 and apply additional design measures, i.e. diversity among channels or continuous fault detection by use of dynamic signals.

EXAMPLE: "Continuous fault detection by use of dynamic signals" means that monitoring of speed is realized by using sensors providing digital or analogic values (not binary) that are continuously compared with a nominal value (speed), and not only at the moment where overspeed is given (event triggered).

When the simplified formulas of Annex H are used, T_2 shall be 17 520 hours (2 years).

NOTE 2 ISO 13849-1:2015, Annex K does not address the boundary conditions of the diagnostic test interval when the test interval is higher than 1 year.

Figure 5 shows the overview of the process for determining high demand mode of operation.

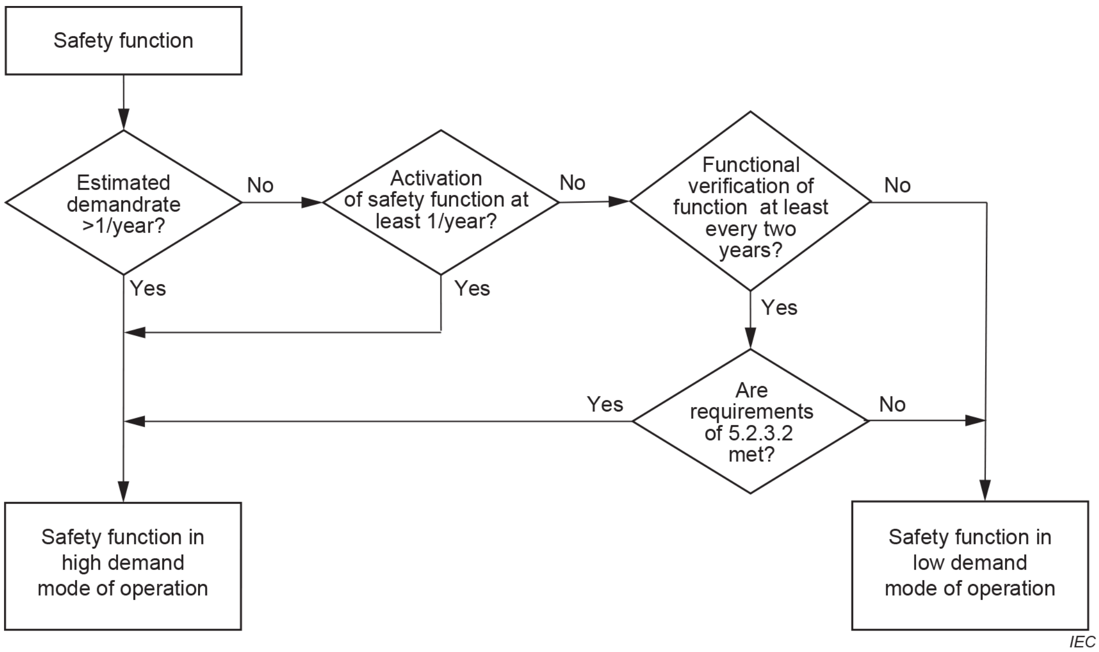


Figure 5 – Process for determining high demand mode of operation

The "rarely activated safety function" shall be verified according to Clause 7.

5.2.3.3 Approach of IEC 62061 and ISO 13849-1

ISO 13849-1 and IEC 62061 do not consider rarely activated safety functions.

5.3 Low demand mode of operation

5.3.1 General

This mode of operation is typically used in the process industry (see IEC 61511). The interaction of the operator is assumed to be part of a kind of protection of layer view.

Principally the reasons for this approach are (see representation in Figure 6):

– Safety instrumented functions (SIF) according to IEC 61511 implemented are mainly intended to protect the process;
– Operators have detail information of the design of safety instrumented functions (SIF) and the control system and the process control itself;
– The layers of protection approach is used and is based on the use and evaluation of the control system performing the process control;
– Demand rate of safety instrumented functions (SIF) can be low and is expected to occur over an interval in terms of one or several years;
– Reaction time of safety instrumented functions (SIF) is much higher than in high demand mode of operation.

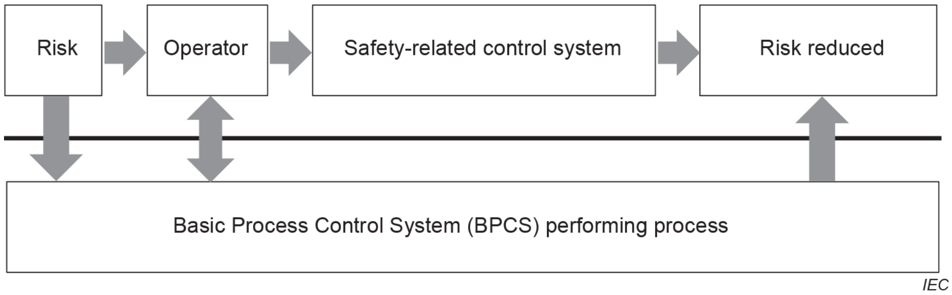


Figure 6 – Low demand mode of operation

5.3.2 Approach of IEC 62061 and ISO 13849-1

IEC 62061 and ISO 13849-1 exclude low demand mode of operation.

NOTE A future amendment of IEC 62061 is planned to consider possible integration of low demand mode of operation.

Annex J gives guidance on how to design safety instrumented functions (SIF) by combining subsystems designed for low demand mode of operation and subsystems designed for high demand mode of operation.

6 Design process of safety functions

6.1 General

This Clause 6 defines the basic design activities for SCS (designed according to IEC 62061) or SRP/CS (designed according to ISO 13849-1) performing a safety function.

NOTE Information given in this Clause 6 is based on safety functions designed according to IEC 62061 or ISO 13849-1.

The manufacturer of a machine will integrate some of the requirements based on the design process into the information for use of the machine.

The principles of verification activities described in this Clause 6 are linked to the basic requirements of proof-test as described in the IEC 61508 series. The term proof-test is not used because it is strongly related to the IEC 61508 series and it is recommended to use a neutral term in the context of machinery.

6.2 Design procedure

The SCS or SRP/CS performing a safety function is designed by using the methodology for high demand mode of operation, see basic procedure detailed in Annex B.

NOTE See Annex F for guidelines for software design.

6.3 Evaluation of required safety integrity

Annex A gives an overview of different methodologies to evaluate the required safety integrity of a safety function.

Table H.1 of IEC 62061:2021 shows for all technologies the PFH evaluation based on $MTTF_D$. Table H.2 of IEC 62061:2021 shows for non-electronic technologies the relationship between B_{10D} and $MTTF_D$. When the calculations are done according to Table H.2 of IEC 62061:2021 with a duty cycle (based on B_{10D} criteria) lower than 1 time per 4 hours, then the evaluation of PFH (Table H.1 of IEC 62061:2021) is not a limiting factor for reaching the required SIL.

NOTE Example of a single contactor, with a B_{10D} = 1 300 000 (cycles) and duty cycle of 1 time per hour leads to a $MTTF_D$ = 1 484 years and PFH = 7,70E-08 << 1,0E-05 (SIL 1), and if the duty cycle is 1 time per day, $MTTF_D$ = 35 616 years and PFH = 3,20E-09 << 1,0E-05 (SIL 1).

6.4 Decomposition of a safety function

Safety functions will be performed by SCS or SRP/CS which is decomposed into subsystems, see Clause 5.

Annex B gives an overview of the methodology of SCS or SRP/CS design.

6.5 Subsystem design

6.5.1 Architectural constraints

As the diagnostic test interval is linked to the demand rate, some diagnostics are only possible when the safety function is demanded (see Annex D for examples of diagnostic coverage). Based on accumulation of faults (see 6.5.2) the architectural constraints should be evaluated depending on the mode of operation. In high demand mode of operation, the following Table 7 applies, based on IEC 62061:2021, Table 6.

Table 7 – Architectural constraints for high demand mode of operation

	Hardware fault tolerance (HFT) [a]				**Basic requirements**[d]
	Single channel subsystem HFT = 0 [c]		**Dual channel subsystem HFT = 1**		
***DC_{avg}* (ISO 13849-1)**[b]	**Max. PL**	**Category (ISO 13849-1)**	**Max. PL**	**Category (ISO 13849-1)**	
***SFF* (IEC 62061)**	**Max. SIL**	**Basic subsystem architecture (IEC 62061)**	**Max. SIL**	**Basic subsystem architecture (IEC 62061)**	
"None"	PL a	Category B	–	–	Basic safety principles [e]
–	No SIL (OM)	–	*No SIL (OM)*	–	
"None"	PL b	Category B	–	–	
–	–	–	–	–	
"None"	PL c	Category 1	–	–	Basic safety principles and well-tried safety principles
< 60 %	SIL 1	Architecture A – well-tried components – CCF not relevant	SIL 1	Architecture B – well-tried components – CCF relevant	
"Low"	PL c	Category 2	PL d	Category 3	
60 % to < 90 %	SIL 1	Architecture C – CCF relevant	SIL 2	Architecture D – CCF relevant	
"Medium"	PL d	Category 2 (see NOTE 6)	PL e	Category 3	
90 % to < 99 %	SIL 2	Architecture C – CCF relevant	SIL 3	Architecture D – CCF relevant	
"High"	–	No equivalent Category	PL e	Category 4	
≥ 99 %	SIL 3	Architecture C – CCF relevant	SIL 3	Architecture D – CCF relevant	

OM Other measures will be applied where no SIL is required.

CCF Common cause failures will be considered whether HFT = 0 and DC > 60 % or whether HFT = 1.

[a] A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.

[b] "Low", "medium" and "high" is the denomination used in ISO 13849-1 in the context of quantification and classification of DC_{avg} ranges.

[c] For HFT 0 and SFF ≥ 99 %, the following limitations can be relevant:

– It is highly recommended to limit the maximum of SIL 2 where fault exclusions have been applied to faults that could lead to a dangerous failure; for some applications, it is not expected that all failures can be excluded with sufficient confidence for SIL 3 (see IEC 62061:2021, 7.3.3.3); SIL 3 can only be claimed when there is continuous monitoring of the correct functioning of the element. Typically, electronic technology will be required to achieve this.

[d] Basic safety principles and well-tried safety principles are required independent of selected architecture. For basic requirements see also ISO 13849-2:2012, Annex A to Annex D. Examples are

– for basic safety principles, the selection and use of suitable materials;

– for well-tried safety principles, the use of deenergizing principle;

– for well-tried components, the use of contactors or position switches.

[e] Where product standards, e.g. IEC 61800-5, IEC 61131-2, etc. are used, it can be assumed that basic safety principles can be fulfilled.

[f] According to ISO 13849-1, PL d can only be reached when the output (OTE, as fault reaction function) initiates a safe state that is maintained until the fault is cleared. It is not sufficient that output of the test equipment OTE provides only a warning. For "safe state" see 3.1.46.

For a single channel subsystem (HFT = 0):

$$SFF \approx DC_{avg} = \frac{\lambda_{DD1}}{\lambda_{D1}} = \frac{DC_1 \times \lambda_{D1}}{\lambda_{D1}} = DC_1$$

For a dual channel subsystem (HFT = 1):

$$SFF \approx DC_{avg} = \frac{\lambda_{DD1} + \lambda_{DD2}}{\lambda_{D1} + \lambda_{D2}} = \frac{DC_1 \times \lambda_{D1} + DC_2 \times \lambda_{D2}}{\lambda_{D1} + \lambda_{D2}} = \frac{\frac{DC_1}{MTTF_{D1}} + \frac{DC_2}{MTTF_{D2}}}{\frac{1}{MTTF_{D1}} + \frac{1}{MTTF_{D2}}}$$

where

λ_{DD1}, λ_{DD2} are the rates of dangerous failure of subsystem element 1 and 2 which is detected by the diagnostic functions;

λ_{D1}, λ_{D2} are the rates of dangerous failure of subsystem element 1 and 2;

DC_1, DC_2 are the diagnostic coverages of subsystem element 1 and 2.

6.5.2 Fault accumulation and undetected faults

In high demand mode of operation, a functional testing is required to detect dangerous faults and accumulation of dangerous faults (see also B.12.1).

For safety functions protecting persons (directly or indirectly) using subsystems with non-electronic technology and with automatic monitoring to achieve the necessary diagnostic coverage for the required safety performance, the monitoring function cannot be possible unless there is a change of state, e.g. at every operating cycle. If there is only infrequent operation, the probability of accumulation of an undetected fault is increased.

When a functional test is necessary to detect a possible accumulation of faults or an undetected fault before the next demand, it shall be made within the following test intervals:

– at least every month for SIL 3;

– at least every 12 months for SIL 2.

NOTE Local regulations can require other periodic test intervals, see also Annex I.

Event triggered rarely activated safety functions (see B.12.2.5) will define measures against fault accumulation and undetected faults. A periodic verification shall be performed, see also 7.5.2.

Common cause failures (CCF) shall be taken into account. Annex E of IEC 62061:2021, Annex E of ISO 13849-1:2015 and Annex E of this document give guidance on measures to avoid and control common cause failures.

6.5.3 Evaluation of PFH

6.5.3.1 General

Annex H gives information on evaluation of the PFH value of a subsystem and the respective boundary conditions. The formulas can be used for high demand mode of operation.

NOTE The limiting factor will be the systematic integrity and the verification procedures will become more relevant.

Annex C gives examples of $MTTF_D$ values for single components that can also be used for rarely activated safety functions.

The demand rate of a safety function has a significant impact on evaluation of PFH values of a subsystem.

6.5.3.2 Influence of B_{10D} values

In practice the PFH value based on B_{10D} and duty cycles does not limit the reachable SIL or PL:

– with a duty cycle of once per day the PFH value ≪ max. PFH value of required SIL or PL;

– architectural constraints are the limiting factor of reachable SIL.

When the duty cycle is higher than one time per hour T_{10D} becomes important, see 6.5.3.3.

Table H.7 shows the typical values using a worst case B_{10D} = 1 000 000 cycles (e.g. contactor or position switch).

6.5.3.3 Influence of T_{10D} value

The useful lifetime is limited to T_{10} and components shall be replaced when T_{10} has elapsed if no other information is given by product standards.

Under specific conditions Clause H.6 gives the rationale for the limitation of T_1 to T_{10} for components based on any kind of cumulative distribution function (CDF), non-electronic technologies, see also H.5.2.

The T_{10D} value limits the useful lifetime of components that are characterized by Weibull distribution: The unavailability of a component increases significantly after the time T_{10D}.

NOTE T_{10} is the limit up to which a constant λ can be assumed (also called "bath curve"). The product data B_{10} (number of cycles where T10 is reached) is typically for components based on Weibull distribution.

PFH formulas are valid up to T_{10D} because the PFH formulas are based on exponential distribution, see Clause H.6 and Clause H.7. The useful lifetime T_1 is typically assumed to be equal to 20 years (or 175 200 h).

When T_{10D} is smaller than T_1, PFH formulas are used by limiting T_1 to

$$T_1 = T_{10D} \tag{2}$$

T_{10D} can be evaluated as follows:

$$\lambda_D \approx 0{,}1 \times \frac{C}{B_{10D}} = 0{,}1 \times \frac{C}{B_{10}} \times \mathrm{RDF}\left[\frac{1}{h}\right] \tag{3}$$

$$\mathrm{MTTF_D} \approx \frac{B_{10D}}{0{,}1 \times n_{op}} = \frac{B_{10}}{0{,}1 \times n_{op} \times \mathrm{RDF}}[a] \tag{4}$$

$$T_{10D} \approx 0{,}1 \times \frac{1}{\lambda_D}[h] \text{ or } T_{10D} \approx 0{,}1 \times \frac{1}{8\,760 \times \lambda_D}[a] \tag{5}$$

$$T_{10D} \approx 0{,}1 \times \text{MTTF}_D \, [a] \tag{6}$$

where

λ_D is the dangerous failure rate of the component, expressed in failures per hour;

C is the duty cycle, expressed in cycles per hour;

B_{10D} is the mean number of cycles until 10 % of the components fail dangerously, expressed in cycles;

B_{10} is the mean number of cycles until 10 % of the components fail, expressed in cycles;

RDF is the ratio of dangerous failure $\frac{B_{10}}{B_{10D}}$, expressed in percent;

n_{op} is the mean number of annual cycles, expressed in cycles.

Table H.8 shows an example.

6.6 Examples of safety functions

Annex G gives examples of safety functions including

– basic information, and
– evaluation of PFH values, using MTTF_D values listed in Annex C.

These examples are classified according to Clause 4.

7 Verification procedures for safety functions

7.1 General

A distinction is made between highly demanded safety functions and rarely activated safety functions designed according to IEC 62061 or ISO 13849-1. "Highly" means a demand of at least once a year, "rarely" means a possible demand rate of less than one time per year.

NOTE 1 Information given this Clause 7 is based on safety functions designed according to IEC 62061 or ISO 13849-1.

Depending on the design of the safety function, infrequent actuation can lead to a loss of the safety function, e.g. due to gumming, contamination, environmental conditions, oils, grease or also due to the influence of the supply voltage.

NOTE 2 For example, a hazardous area is accessible via several frequently opened guard doors yet there is one which is used rarely (less than one time per year).

By frequent demand, the risk of accumulation of faults will be reduced, if diagnostics depending on state change are implemented. This applies to all safety functions in high demand or continuous mode of operation.

7.2 Verification of the test interval of a safety function

Today's technology makes it possible to document the requirement of a safety-related device in the SCS or SRP/CS. If the documented results can be compared with the real values, it is possible to indicate to the operators that they shall test certain safety functions.

If this is not implemented, the requirements shall be carried out at regular time intervals according to a maintenance plan or information for use.

7.3 Verification procedures

Each safety function shall be tested regarding correct functioning before initial start-up (see 7.4, initial verification), at regular (frequent) intervals and after repair (and maintenance) (see 7.5, periodic verification). The degree and extent of the test is determined by the requirements in the operating instructions (information for use).

NOTE 1 The terms "initial verification" or "periodic verification" are used in the context of electrical equipment of machines (see IEC 60204-1:2016, Clause 18, IEC 60204-1:2016/AMD1:2021, Clause 18, and in IEC 60364-1:2005, 134.1 and 134.2). These terms are also used in the context of putting a machine into service.

A general distinction is made between two types of tests:

– Testing of the safety function by a person who is competent in safety function verification. During this test only the result, i.e., the response of the safety system, is checked.
– Testing of the effectiveness of the safety function by a person competent on safety functions and in charge of the verification process; during this test, the entire safety-related system is verified; the person in charge of the verification shall determine the degree and extent of the test based, e.g., on the manufacturer's safety-related instructions.

NOTE 2 Requirements for qualification of persons competent on safety function in charge for the verification can be a matter covered in national regulations.

NOTE 3 The person competent on safety functions could be the representative of an authority body, a person representing the manufacturer of the machine or a person external to the company of the machine manufacturer; it is opportune to document the competence of the person and body (or both).

7.4 Initial verification

The machine shall be examined during installation, as far as reasonably practicable, and on completion, before being put into service.

Initial verification shall include a comparison of the results with relevant criteria to confirm that the requirements of IEC 62061 or ISO 13849-1 have been met. This activity corresponds to the validation process (see IEC 62061:2021, Clause 9 and ISO 13849-1:2015, Clause 10) and is intended to confirm that the SCS or SRP/CS complies with the safety requirements specification (SRS).

NOTE 1 The validation to be applied to the SCS includes inspection (e.g. by analysis) and testing of the SCS or SRP/CS to ensure that it achieves the requirements stated in the safety requirements specification (SRS). Therefore, initial verification can include intervention in the machine control system, e.g., faults are simulated, and the resulting reaction is evaluated.

Precautions shall be taken to ensure that the verification shall not cause danger to persons, animals or livestock and shall not cause damage to property and equipment.

Initial verification shall be made by a person who is competent on safety function verification.

NOTE 2 Requirements as to the qualifications of the organization and persons carrying out the verification process can be covered in national consideration.

NOTE 3 Requirements as to the qualifications of persons competent on safety functions in charge of the verification process can be covered in national consideration.

NOTE 4 Validation consists of applying analysis (also by inspection) (see IEC 62061:2021, 9.2 or ISO 13849-1:2015, 10.1.1) and executing functional tests (see IEC 62061:2021, 9.3 or ISO 13849-1:2015, 10.3) under foreseeable conditions in accordance with the validation plan. The balance between the analysis and testing will be justified.

Initial verification shall precede testing and shall be carried out prior to the first use of the machine for production.

Initial verification shall be carried out to confirm that the SCS or SRP/CS which is part of the machine control system is:

– in compliance with the safety requirements specification (SRS);
– correctly implemented (as installed or erected) according to the relevant requirements of IEC 62061 or ISO 13849-1 and according to the instructions of the manufacturer's components, if applicable;
– not visibly damaged.

The initial verification procedure shall include at least the checking of the following, where relevant:

a) documentation;
b) labelling fixed on the machine (e.g. safety-related information, indications, warnings, type plates);
c) erection and erection information provided by the manufacturer of safety-related components and the manufacturer of the machine (based on hardware of safety-related components depending on the technologies, e.g., light curtains, cartridge or single valves) (see information for use provided by the manufacturers);
d) response times and behaviour of the safety-related function(s) (e.g. parameter and parametrization, test of dynamic of the frequency inverter functions, etc.);
e) prevention of manipulation or motivation to defeat safeguards;
f) safety-related behaviour under fault conditions;
g) description of the residual risks.

NOTE 5 Further information is given in IEC 62061:2021, 9.1.1, 9.1.4 and 9.4, or in ISO 13849-1:2015, 10.1.2, 10.1.5 and 10.5).

Initial verification shall include all (particular) requirements for special installations or locations.

7.5 Periodic verification

7.5.1 General

All safety functions shall be tested at periodic intervals.

Where a safety function has not been demanded over the course of one year, systematic aspects and fault accumulation can lead to the loss of the safety function performed by an SCS or SRP/CS.

NOTE 1 The time periods are implemented by the country-specific implementation of national occupational health and safety regulations. Local authorities can require additional verifications, as well as the insurer of the property can require additional verifications.

Wherever possible, the records and recommendations of previous periodic verifications shall be considered.

Periodic verification comprising a detailed examination of the installation shall be carried out to show that the requirements of IEC 62061 or ISO 13849-1 are still fulfilled.

The degree and extent of the periodic verification shall be such that it can be confirmed that there is no hazardous situation arising from the machine. The periodic verification shall at least include the verification of the safety-related behaviour and the residual risk.

Precautions shall be taken to ensure that the verification shall not cause danger to persons, animals or livestock and shall not cause damage to property and equipment.

Periodic verification procedure shall include at least the checking of the following, where relevant:

a) availability of the documentation;
b) labelling fixed on the machine (e.g. safety-related information, indications, warnings, type plates);
c) availability of specific test procedure(s) (e.g. based on hardware, degree and extent of the test, information of the manufacturer of the machine);
d) response times and behaviour of the safety-related function(s) (e.g. parameter and parametrization, test of dynamic of the frequency inverter functions, etc.);
e) prevention of manipulation, motivation;
f) evaluation and description of the residual risks during the verification;
g) check that no modification to hardware or software has been performed;
h) check whether modifications have been verified and validated;
i) maintenance performed, maintenance records made;
j) documentation of (daily) tests by the operator as required by the manufacturer (light curtain test with test rod, etc.).

NOTE 2 Additional requirements for testing under fault condition can be defined in type-C standards or in national regulations.

NOTE 3 The previous investigation report can be used as reference.

The extent and results of the periodic verification of an SCS or SRP/CS, or any part of an SCS or SRP/CS, shall be recorded.

Any damage, deterioration, defects or dangerous condition shall be recorded. Furthermore, significant limitations of the periodic verification in accordance with this document and the reasons for such limitations shall be recorded.

The periodic verification shall be carried out by a person who is competent on the verification of safety functions.

NOTE 4 Requirements concerning the relevant qualifications for enterprises and persons can be covered in national consideration.

NOTE 5 Requirements concerning the relevant qualifications of persons competent on safety function in charge of the verification can be covered in national consideration.

7.5.2 Frequency of periodic verification

7.5.2.1 General

The frequency of periodic verification of an installation shall be determined having regard to the type of installation and the SCS or SRP/CS, its use and operation, the frequency and quality of maintenance and the external influences to which it is subjected.

NOTE 1 The maximum periodic verification interval between periodic verifications can be defined by legal or other national regulations.

The periodic verification report should recommend to the person carrying out the periodic verification the interval to the next periodic verification.

The periodic verification interval may be longer than one year, with the exception of the following cases where a higher risk of accumulation of faults for the machinery may exist and shorter periods may be required, e.g. workplaces or locations and construction sites.

The results and recommendations of the previous reports, where available, shall be considered.

7.5.2.2 Interval between periodic verifications

Conditions under which the interval for periodic verification can be defined up to 2 years are described in 5.2.3.

NOTE The definition of the time intervals depends on safety parameters of the safety protection device. The definition of the "adequate" periodicity can be identified according to formulas or tables of Annex H.

7.6 Verification reporting

Upon completion of the verification of an existing installation, a report shall be provided. Such documentation shall include details of those parts of the installation, the SCS or SRP/CS and other limitations of the verification covered by the report, together with a record of the inspection.

The report may contain recommendations for repairs and improvements, such as upgrading the installation or retrofitting the facility.

The report shall be completed by the person responsible for carrying out the verification, or a person authorized to act on their behalf, to the person ordering the verification.

The records of test results shall record the results of the appropriate tests.

Reports shall be compiled and signed.

The documentation shall include at least the following items:

– day of the test;
– who performed the verification;
– participants at the verification;
– verification documentation;
– scope of the verification;
– deviations;
– test results.

The verification result shall describe whether safety-related operation is possible. If this is only possible under certain conditions, the operator shall be informed of this in writing.

Annex A
(informative)

Risk assessment and risk reduction according to ISO 12100

A.1 General

The approach of ISO 12100 related to functional safety is described in this Annex A.

The tables in this Annex A can help to implement the ISO 12100 requirements.

These tables are not exhaustive (except for Table A.4 and Table A.6) and other information may be necessary depending on the specific machine.

The "Comments" column in Table A.1 to Table A.5 can be used to refer to the source information or to the document reference, as appropriate.

NOTE This approach applies to safety functions designed according to IEC 62061 or ISO 13849-1.

A.2 Risk assessment principles

A.2.1 General

The following activities will be carried out to perform a risk assessment and risk reduction:

– Risk analysis by
  a) determining the limits of the machinery, which include the intended use and any reasonably foreseeable misuse thereof;
  b) identifying the hazards and associated hazardous situations;
  c) estimating the risk for each identified hazard and hazardous situation;
– Risk evaluation by
  d) evaluating the risk and taking decisions about the need for risk reduction;
– Risk reduction by
  e) eliminating the hazard or reducing the risk associated with the hazard by means of protective measures.

A.2.2 Basic information to be available (as input to risk assessment)

The information to be available for the risk assessment should include the information listed in Table A.1.

Table A.1 – Basic information for risk assessment according to ISO 12100

Information for risk assessment (references are to ISO 12100:2010, 5.2)	**Comments (e.g. source of information, document reference)**
Machinery description: 5.2 a)	
User specifications	
Machinery specifications: Description of life cycle phases	
Machinery specifications: Design drawings	
Machinery specifications: Required energy sources	
Documentation on previous designs of similar machinery	
Information for use of the machinery	
Regulations, standards and other applicable documents: 5.2 b)	
Applicable regulations	
Relevant standards	
Relevant technical specifications	
Relevant safety data sheets	
Experience of use: 5.2 c)	
Any accident, incident or malfunction history	
History of damage to health	
Experience of users of similar machines	
Ergonomic principles: 5.2 d)	
Comparisons between similar hazardous situations associated with different types of machinery	

A.2.3 Risk analysis

A.2.3.1 Determination of limits of machinery

Use limits include the intended use and the reasonably foreseeable misuse. Aspects to be considered are listed in Table A.2.

Table A.2 – Determination of limits of machinery according to ISO 12100

Determination of limits (references are to ISO 12100:2010, 5.3)	**Comments (e.g. source of information, document reference)**
Use limits:	
Different machine operating modes and different intervention procedures for users, including interventions required by malfunctions of the machine	
The use of the machinery by persons identified by sex, age, dominant hand usage, or limiting physical abilities	
The anticipated levels of training, experience or ability of users (operators, maintenance personnel or technicians, trainees and apprentices, and general public)	
Exposure of other persons to the hazards associated with the machinery (persons likely to have a good awareness, persons with little awareness, persons likely to have very little awareness)	
Space limits:	
The range of movement	
Space requirements for persons interacting with the machine, such as during operation and maintenance	
Human interaction such as the operator–machine interface	
The machine–power supply interface	
Time limits:	
The life limit of the machinery and/or of some of its components (tooling, parts that can wear, electromechanical components, etc.), considering its intended use and reasonably foreseeable misuse	
Recommended service intervals	
Other limits:	
Properties of the material(s) to be processed	
Housekeeping – the level of cleanliness required	
Environmental (recommended minimum and maximum temperatures, in dry or wet weather, in direct sunlight, tolerance to dust and wet, etc.)	

A.2.3.2 Hazard identification

The essential step in any risk assessment of the machinery is the systematic identification of reasonably foreseeable hazards (permanent hazards and those which can appear unexpectedly), hazardous situations and/or hazardous events during all phases of the machine life cycle. Table A.3 can help the designer to identify hazards.

Table A.3 – Principles of hazard identification according to ISO 12100

Hazard identification (references to ISO 12100:2010,5.4)	**Comments (e.g. source of information, document reference)**
Human interaction during the whole life cycle of the machine:	
Task identification should consider all tasks associated with every phase of the machine life cycle:	
setting	
testing	
teaching/programming	
process/tool changeover	
start-up	
all modes of operation	
stopping the machine	
restart after unscheduled stop	
cleaning and housekeeping	
preventive and corrective maintenance	
Possible states of the machine:	
The machine performs the intended function (the machine operates normally)	
The machine does not perform the intended function (i.e., it malfunctions) due to a variety of reasons (e.g., variation of a property or of a dimension of the processed material, failure of one or more of its component parts or services, external disturbances, disturbance of its power supply, etc.)	
Unintended behaviour of the operator or reasonably foreseeable misuse of the machine:	
The life limit of the machinery and/or of some of its components (tooling, parts that can wear, electromechanical components, etc.), considering its intended use and reasonably foreseeable misuse	
Recommended service intervals	
Other limits:	
Examples include:	
loss of control of the machine by the operator (especially for hand-held or mobile machines)	
reflex behaviour of a person in the event of malfunction	
behaviour resulting from lack of concentration or carelessness, from pressures to keep the machine running	
behaviour of certain persons	

A.2.3.3 Risk estimation

After hazard identification, risk estimation should be carried out for each hazardous situation by determining the elements of risk listed in Table A.4.

Table A.4 – Risk estimation according to ISO 12100

Elements of risk (references to ISO 12100:2010, 5.5.2)	**Comments (e.g. source of information, document reference)**
The severity of harm:	
The severity of injuries or damage to health, e.g. slight, serious, death	
The probability of occurrence of that harm:	
Exposure of persons to the hazard	
Occurrence of a hazardous event	
Possibility of avoiding or limiting harm	

In addition to Table A.4 the following Table A.5 will be considered.

Table A.5 – Additional considered aspects during risk estimation according to ISO 12100

Aspects to be considered during risk estimation (reference to ISO 12100:2010, 5.5.3)	**Comments (e.g. source of information, document reference)**
Persons exposed:	
All persons (operators and others)	
Type, frequency and duration of exposure:	
The needs for access during loading/unloading, setting, teaching, process changeover or correction, cleaning, fault-finding and maintenance	
Tasks, for which it is necessary to suspend protective measures	
Relationship between exposure and effects:	
Exposure to a hazard and its effects for each hazardous situation	
Human factors:	
Interaction of person(s) with the machinery	
Interaction between persons	
Stress-related aspects	
Ergonomic aspects	
The capacity of persons to be aware of risks	
Suitability of protective measures:	
The circumstances which can result in harm	
Possibility of defeating or circumventing protective measures:	
The protective measure slows down production or interferes with another activity or preference of the user	
The protective measure is difficult to use	
Persons other than the operator are involved	
The protective measure is not recognized by the user or not accepted as being suitable for its function	
Ability to maintain protective measures:	
Condition necessary to provide the required level of protection, if not easily possible then encourage of defeating of the protective measure	
Information for use:	
Relevant information to ensure risk reduction measure	

A.2.3.4 Risk evaluation

Risk evaluation should be carried out to determine if risk reduction is required. If risk reduction is required, appropriate protective measures should be selected and applied. The application of the three-step method according to ISO 12100 allows adequate risk reduction to be achieved. During the process of risk evaluation, the risks associated with the machinery or parts of machinery can be compared with those of similar machinery or parts of machinery.

A.3 Risk reduction by means of safeguarding and complementary protective measures

A.3.1 General

Risk reduction should be implemented by applying a hierarchical approach referred to as the three-step method:

1) Step 1: Inherently safe design measures
2) Step 2: Safeguarding and/or complementary protective measures
3) Step 3: Information for use

NOTE Step 2 is relevant for application of IEC 62061 or ISO 13849-1, see Clause 4.

Step 1 inherently safe design measures are the first and most important step in the risk reduction process. This should be achieved by avoiding hazards or reducing risks by a suitable choice of design features for the machine itself and/or interaction between the exposed persons and the machine.

The information for classification of safety functions contained in the safeguarding and complementary protective measures described in ISO 12100:2010, 6.3.

Where inherently safe design is not possible other measures will be implemented.

Therefore, risk reduction, according to Step 2 of the iterative risk reduction process described in ISO 12100, can be achieved by designing, for each hazard, adequate safeguarding and complementary protective measures in order to:

a) lower the likelihood of a hazardous event, or
b) limit the duration or the rise of a hazardous event, or
c) reduce the consequences of a hazardous event.

The priority in the risk reduction process is the removal of the hazards by means of inherently safe design measures.

Removing hazards during the design phase is the most effective method of reducing risk because it eliminates the source of harm.

If the hazards cannot be removed or the risks cannot be adequately reduced by inherently safe design measures, additional protective measures will be applied taken in such a way as:

a) to reduce the probability of occurrence of the hazardous event by suppressing probable causes, or
b) to impose a limitation on exposure to the hazards, or
c) to enhance the possibility of avoiding the harm or at least by reducing its intensity.

A.3.2 Inherently safe design measures

These are protective measures which either eliminate hazards or reduce the risks associated with hazards by changing the design or operating characteristics of the machine without the use of guards or protective devices.

A.3.3 Selection of safeguarding and complementary protective measures

A.3.3.1 General

Protective measures can be passive or active.

A.3.3.2 Fixed guards as "passive" protective measures

A fixed guard prevents access to a hazard and is effective continuously. It is independent from the machine control system (MCS) and does not need to be activated to achieve the risk reduction. Such a guard is a "passive" protective measure.

Examples of "passive" protective measures are:

– fences;
– non-movable protections to prevent access to dangerous areas.

They provide protection by reducing the duration of exposure to the hazard. Only marginal risk reduction is given with respect to the severity of the harm.

NOTE IEC 61508 uses the term "other risk reduction measures" that are not based on any safety-related system, see IEC 61508-1:2010, 7.6.2.1.

Passive protective measures are not within the scope of IEC 62061, ISO 13849-1, or ISO 13849-2.

A.3.3.3 Safety functions as "active" protective measures

A.3.3.3.1 General

A safety function performed by an SCS is triggered in response to a defined change in a measurable property of an input (e.g., a sensor or a switch). Such a safety function is an "active" protective measure.

They are intended to reduce the risk generated, for example, by the following events:

a) human interaction with the machine (operations) (see A.3.3.3.2);
b) failures of the machine automation control system (see A.3.3.3.3);
c) improper use of the machine (see A.3.3.3.4).

Typically, of all the complementary protection measures, they have the most effect on reducing the probability of occurrence of the harm.

NOTE IEC 61508 uses the term "E/E/PE safety-related systems", which are not based on any safety-related system, see IEC 61508-1:2010, 7.6.2.1.

A.3.3.3.2 Human interaction with the machine (operations)

It is possible that persons may expose themselves to a hazard when performing a certain task or machine operation.

Examples of devices used for active protective measures suitable to reduce risks generated by human interaction with the machine are:

- sensitive protective devices to detect persons entering or present in the dangerous area (e.g., photoelectric safety barriers, laser scanners, sensitive mats);
- devices associated with the commands of the machine (e.g., enabling device, hold-to-run control devices);
- interlocking guards.

They are intended to work immediately upon a specific initiating event. Their role is to ensure that persons or parts of the human body are not injured by the dangerous parts of the machine.

The "demand" of protection is generated by the person with their interaction (operations) with the machine process.

A.3.3.3.3 Failures of the machine automation control system

It is possible that a failure of a component of the machine control system which is involved in a certain machine process can generate dangerous situations such hot surfaces, flames, excessive vibrations, explosions, etc.

Examples of devices used for active protective measures suitable to reduce risk due to component failures are:

- torque limiters;
- pressure or temperature limiting devices;
- overspeed limiters;
- monitoring devices for the emission of radiation or gas;
- fire and smoke detectors.

They are employed as a means of prevention and are intended to work before a specific initiating event takes place. Their role is to ensure that the accident does not happen, or at least to slow down its development or to limit to an acceptable level the deviation of the process.

The malfunction of the machine control system can trigger the safety function.

A.3.3.3.4 Foreseeable misuse of the machine

It is possible that intense usage of the machine due to time pressure or high stress due to excessive loads or due to the processing of unsuitable material can bring the machine to work outside its design limits which in turn can generate mechanical failures of the machine itself or damage to the goods to be processed and, in a second step, can generate risks to the persons.

Examples of devices used for active protective measures suitable to reduce risk due to foreseeable misuse are:

- torque limiters;
- pressure limiting devices;
- overspeed limiters;
- strain gauge sensors;
- current overload sensors.

The "demand" is generated by the overload of the machine because of its foreseeable misuse.

A.3.3.3.5 Risk reduction by means of complementary protective measures

To achieve further risk reduction, it may be necessary to use complementary protective measures considering the intended use and reasonably foreseeable improper use of the machine.

Complementary protective measures whose main effect is to avoid or limit the harm are:

- emergency stop;
- measures to allow a safe access to machinery;
- measures for the escape and rescue of trapped people.

Complementary protective measures whose main effect is to reduce the duration of exposure to the hazard are:

- devices suitable for energy isolation like isolation valves and isolation switches;
- devices suitable for energy dissipation like pressure relief valves;
- mechanical locks to prevent movements.

A.4 Other protective measures (procedure based)

A.4.1 General

To ensure that passive, active and complementary protective measures implemented remain effective all over the machine life cycle, additional actions based on procedures and organization are needed.

NOTE It is important to mention these aspects, even if they are out of the scope of this document, because they play an important role in keeping the workplace safe.

A.4.2 Procedures for maintenance

It is possible that a lack of maintenance can lead to mechanical failures or errors of some parts of the machine, this can lead to risks to persons.

Example of failures due to lack of maintenance are:

- poor lubrication or
- loss of cooling liquids.

To reduce these types of hazards, detailed maintenance instructions should be developed and implemented.

A.4.3 Organizational work procedures

As a minimum the following organizational measures should be operative:

- well defined roles and responsibilities of workers, supervisors and management;
- a plan for periodic trainings of workers;
- availability of suitable tools for maintenance and verifications;
- a plan for periodic inspections to check the integrity of the protections;
- a plan for escape and for emergency procedures;
- a means to keep track of periodic verifications.

A.5 Guards and protective devices according to ISO 12100

A.5.1 General

Guards and protective devices will be used to protect persons whenever an inherently safe design measure does not reasonably make it possible either to remove hazards or to sufficiently reduce risks. Complementary protective measures involving additional equipment (for example, emergency stop equipment) may have to be implemented.

Guards are a physical barrier and are designed as part of the machine to provide protection and can be classified as listed in Table A.6.

Table A.6 – Guards according to ISO 12100

Safeguarding and complementary measures (reference to ISO 12100:2010, 6.3)	Comments (e.g. source of information, document reference)
Movable guard (see ISO 12100:2010, 3.27.2):	
Can be opened without the use of tools	
Adjustable guard (see ISO 12100:2010, 3.27.3):	
Fixed or movable guard which is adjustable as a whole	
Interlocking (see ISO 12100:2010, 3.27.4):	
Guard associated with an interlocking device, where	
hazardous machine functions are "covered" by the guard	
opening of the guard is giving a stop command	
only closed guard can allow hazardous machine functions	
Interlocking guard with guard locking (see ISO 12100:2010, 3.27.5):	
Guard associated with an interlocking device and a guard locking device, where	
hazardous machine functions can operate only if guard is closed and locked	
guard remains closed and locked until the risk due to the hazardous machine functions disappeared	
only closed and locked guard can allow hazardous machine functions	
Interlocking guard with a start function (see ISO 12100:2010, 3.27.6):	
Special form of interlocking guard which, once it has reached its closed position, gives a command to initiate the hazardous machine function(s) without the use of a separate start control	

A.5.2 Interlocking guard with a start function, with manual reset function

The re-establishment of the safety function by resetting of the safeguard cancels the stop command. If indicated by the risk assessment, this cancellation of the stop command will be confirmed by a manual, separate and intended action (manual reset).

The manual reset function will:

– be provided through a separate and manually operated device which is separate from the start command within the SCS or SRP/CS,
– only be achieved if all affected safety functions and safeguards are operative,
– not initiate a hazardous situation by itself,
– be activated by intended action,
– enable the control system to accept a separate start command,

– be accepted by signal change.

NOTE A risk assessment can determine if a manual reset safety function is required and if the SIL or PL_r differs from the associated safety function.

A.5.3 Protective device according to ISO 12100

A protective device is a safeguard other than a guard; examples are listed in Table A.7.

Table A.7 – Examples of protective devices according to ISO 12100

Safeguarding and complementary protective measures (reference to ISO 12100:2010, 6.3)	Comments (e.g. source of information, document reference)
Interlocking device (see ISO 12100:2010, 3.28.1):	
Mechanical, electrical or other type of device preventing hazardous machine functions (generally as long as a guard is not closed)	
Enabling device (see ISO 12100:2010, 3.28.2):	
Additional manually operated device used in conjunction with a start control and which, when continuously actuated, allows a machine to function	
Hold-to-run control device (see ISO 12100:2010, 3.28.3):	
Control device which initiates and maintains machine functions only as long as the manual control (actuator) is actuated	
Two-hand control device (see ISO 12100:2010, 3.28.4):	
Control device which requires at least simultaneous actuation by both hands in order to initiate and to maintain hazardous machine functions, thus providing a protective measure only for the person who actuates it	
Sensitive protective equipment (SPE) (see ISO 12100:2010, 3.28.5):	
Equipment for detecting persons or parts of persons which generates an appropriate signal to the control system to reduce risk to the persons detected	
Active optoelectronic protective device (AOPD) (see ISO 12100:2010, 3.28.6):	
Device whose sensing function is performed by optoelectronic emitting and receiving elements detecting the interruption of optical radiation, generated within the device, by an opaque object present in the specified detection zone	
Mechanical restraint device (see ISO 12100:2010, 3.28.7):	
Device which introduces into a mechanism a mechanical obstacle (for example, wedge, spindle, strut, scotch) which, by virtue of its own strength, can prevent any hazardous movement	
Limiting device (see ISO 12100:2010, 3.28.8):	
Device which introduces into a mechanism a mechanical obstacle (for example, wedge, spindle, strut, scotch) which, by virtue of its own strength, can prevent any hazardous movement	
Limited movement control device (see ISO 12100:2010, 3.28.9):	
Control device, a single actuation of which, together with the control system of the machine, permits only a limited amount of travel of a machine element	

A.5.4 Manual local control device (and procedure)

When a machine is controlled locally, e.g. by a portable control device or pendant, the following requirements apply:

– the means for selecting local control will be situated outside the danger zone;

– it is only possible to initiate command by a local control in a zone defined by the risk assessment in order to avoid hazardous situations;

– switching between local and another control does not create a hazardous situation;
– the control system will be designed in such a way that the initiation of commands from different control stations does not lead to a hazardous situation. It can be necessary to preclude use of other controls when the local control is operated.

A.5.5 Manual parameter selection device (and procedure)

When safety-related parameters, e.g. position, speed, temperature, time, torque or pressure, deviate from pre-set limits, the SCS or SRP/CS will initiate appropriate measures (e.g. actuation of stopping, warning signal, alarm).

If errors in manual inputting of safety-related data in programmable or configurable electronic systems can lead to a hazardous situation, then a data checking system within the SCS or SRP/CS should be provided, e.g. check of limits, format and/or logic input values.

Product and C-type standards can require a data checking system for some or all manual parameters.

A.5.6 Manual operating mode selection device (and procedure)

The following systematic aspects are recommended:

– only one operating mode can be active at a time; each selected operating mode will be clearly identifiable or indicated;
– mode selection by itself will not initiate machine operation. A separate actuation of the start control will be required.
– when changing from one operating mode to another, safety functions and/or risk reduction measures necessary for the selected operating mode are activated; without any loss of protection coverage during the transition.

A.5.7 Energy control device (and procedure)

When fluctuations in energy levels outside the design operating range occur, including loss of energy supply, the SCS or SRP/CS continue to provide or initiate output signal(s) which will enable other parts of the machine system to maintain a safe state (see also ISO 14118).

A.6 Matrix assignment approach

A.6.1 Overview

Risk estimation of safety functions will be carried out for each hazard by determining the risk parameters as defined in ISO/TR 14121-2 shown as follows:

– severity of harm, Se; and
– probability of occurrence of that harm, which is a function of:
  - frequency and duration of the exposure of persons to the hazard, Fr;
  - probability of occurrence of a hazardous event, Pr; and
  - possibilities to avoid or limit the harm, Av.

If the estimated risk will be reduced by implementing an SCS or SRP/CS the risk estimation allows the determination of a required safety integrity for such SCS or SRP/CS. The required safety integrity is called a required SIL in accordance with IEC 62061 or PL_r in accordance with ISO 13849-1.

The approaches for determining the required SIL or PL_r are described in more details in IEC 62061:2021, Annex A (matrix assignment) and ISO 13849-1:2015, Figure A.1 (risk graph).

Other approaches can be found in IEC 61508. In terms of machinery, the LOPA approach is not applicable or appropriate because the machinery environment in terms of the user is different compared to that in the process industry approach, e.g., in IEC 61511.

A.6.2 General

The matrix assignment methodology allows an estimation of the risk parameters by using a scaled numbering. The main difference between ISO 13849-1:2015, Figure A.1 and the matrix approach of IEC 62061 is the risk parameter Severity. IEC 62061 has four levels for estimation while ISO 13849-1 only offers two levels.

Furthermore, the matrix assignment allows the estimation of PL_r, based on the PFH target values, in addition to the estimation of the SIL. As PL_r c is < 3,0 E-06 (or 30 % of 1,0 E-05) SIL 1 can be spliced respectively into PL_r c and PL_r b. PL_r a corresponds to "Other Measures" (OM) and is based on the basic engineering design requirements like basic safety principles. Systematic aspects are dominant and no required PFH value is needed.

NOTE Less than SIL 1 is not defined and would not have any added value, therefore other measures are sufficient.

A.6.3 Methodology of IEC 62061:2021, Annex A

The entry point is the estimation of the risk parameter Severity, Se. Based on the selected row for Se the next step is to estimate the three other risk parameters by selecting the appropriate value between 1 and 5.

The addition of these values allows the Class Cl = Fr + Pr + Av to be defined.

The intersection between the Se row and the Cl column leads to the required SIL and PL_r.

Figure A.1 shows all risk parameters as a summary of Table A.1 to Table A.6 of IEC 62061:2021.

<table>
<tr><th rowspan="2">Consequences</th><th rowspan="2">Severity Se</th><th colspan="13">Class Cl = Fr + Pr + Av</th></tr>
<tr><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th></tr>
<tr><td rowspan="2">Death, losing an eye or arm</td><td rowspan="2">4</td><td colspan="2">SIL 1</td><td colspan="3">SIL 2</td><td colspan="3">SIL 2</td><td colspan="3">SIL 3</td><td colspan="2">SIL 3</td></tr>
<tr><td>PL_r b</td><td>PL_r c</td><td colspan="3">PL_r d</td><td colspan="3">PL_r d</td><td colspan="3">PL_r e</td><td colspan="2">PL_r e</td></tr>
<tr><td rowspan="2">Permanent injury, losing fingers</td><td rowspan="2">3</td><td colspan="2" rowspan="2"></td><td colspan="3">OM</td><td colspan="3">SIL 1</td><td colspan="3">SIL 2</td><td colspan="2">SIL 3</td></tr>
<tr><td colspan="3">PL_r a</td><td>PL_r b</td><td colspan="2">PL_r c</td><td colspan="3">PL_r d</td><td colspan="2">PL_r e</td></tr>
<tr><td rowspan="2">Reversible injury, medical attention</td><td rowspan="2">2</td><td colspan="5" rowspan="2">No SIL (or PL) required</td><td colspan="3">OM</td><td colspan="3">SIL 1</td><td colspan="2">SIL 2</td></tr>
<tr><td colspan="3">PL_r a</td><td>PL_r b</td><td colspan="2">PL_r c</td><td colspan="2">PL_r d</td></tr>
<tr><td rowspan="2">Reversible injury, first aid</td><td rowspan="2">1</td><td colspan="8" rowspan="2">OM: Other Measures
(e.g. basic safety principles, Table 7 of IEC 62061:2021)</td><td colspan="3">OM</td><td colspan="2">SIL 1</td></tr>
<tr><td colspan="3">PL_r a</td><td>PL_r b</td><td>PL_r c</td></tr>
</table>

Frequency and duration of exposure (Fr)		
Frequency of exposure	**Frequency, Fr**	
	Duration of exposure ≥ 10 min	Duration of exposure < 10 min
≥ 1 per h	5	5
< 1 per h to ≥ 1 per day	5	4
< 1 per day to ≥ 1 per 2 weeks	4	3
< 1 per 2 weeks to ≥ 1 per year	3	2
< 1 per year	2	1

Probability of occurrence	**Probability (Pr)**
Very high	5
Likely	4
Possible	3
Rarely	2
Negligible	1

Probabilities of avoiding or limiting harm (Av)	
Impossible	5
Rarely	3
Probable	1

Figure A.1 – SIL assignment approach

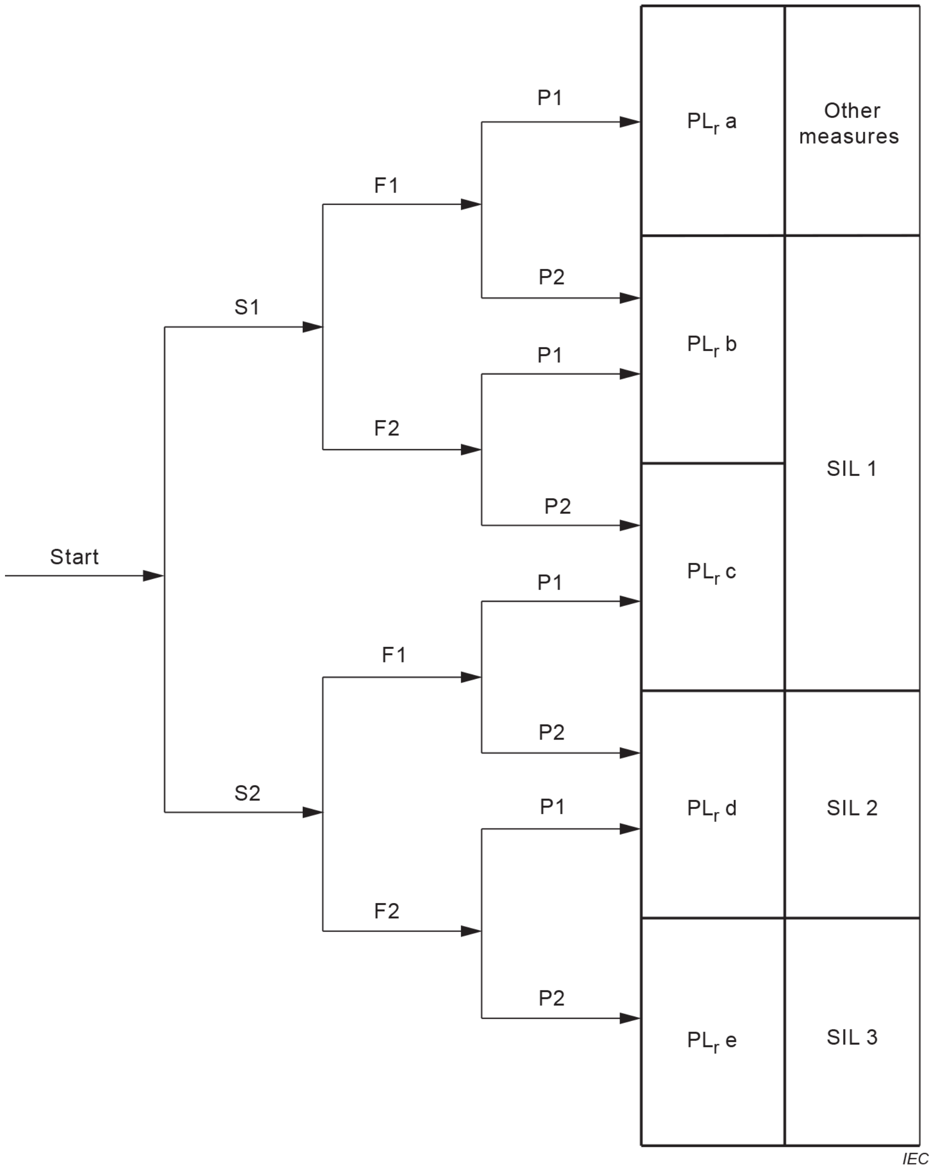
A.7 Risk graph approach

A.7.1 General

The risk graph is based on the risk parameters where the probability of occurrence is not represented and considered to be high.

A.7.2 Methodology of ISO 13849-1:2015, Annex A with assigned SIL

The risk graph is represented in Figure A.2.



S severity of injury	F frequency and/or exposure to hazard	P possibility of avoiding hazard or limiting harm
S1 slight (normally reversible injury)	F1 seldom-to-less-often and/or exposure time is short	P1 possible under specific conditions
S2 serious (normally irreversible injury or death)	F2 frequent-to-continuous and/or exposure time is long	P2 scarcely possible

Figure A.2 – Risk graph approach of ISO 13849-1:2015, Figure A.1 with assigned SIL

Annex B
(informative)

Methodology of SCS or SRP/CS design

B.1 General

Safety functions which will be implemented by SCS or SRP/CS, can be realized by

– using an already developed SCS or SRP/CS that meets the required safety integrity, or
– designing a new SCS or SRP/CS using pre-designed subsystems or designing new subsystems, or a combination of both.

NOTE 1 The methodology of SCS design is in accordance with IEC 62061 and the methodology of SRP/CS design is in accordance with ISO 13849-1.

NOTE 2 The design of complex programmable electronic subsystems or subsystem elements is not within the scope of IEC 62061.

B.2 Functional safety plan

In this context a functional safety plan specifies the overall management and technical activities necessary to design, implement and integrate one or more SCS or SRP/CS used for safety of machinery.

Table B.1 gives an overview of the basic requirements of the functional safety plan.

Table B.1 – Overview functional safety plan

Activity	**Relevant clause/subclause of IEC 62061:2021**	**Input information** **Source of requirement**	**Output information** **Where information can be found**
Activities (i.e. SCS design, software, validation)	Clause 4		
Policy and strategy	Clause 4		
Strategy for application software	Clause 8		
Responsible persons, departments (or other units)	Clause 4		
Record and maintaining information relevant to each SCS	Clause 10		
Configuration management (i.e. identification of the architecture of the SCS, controlling, recording/reporting, review)	Subclause 4.4, Clause 10		
Modification management (and impact analysis where modified SCS)	Subclause 4.5, Clause 10		
Verification plan (i.e. who, techniques, test equipment, acceptance criteria)	Clause 9, Clause 10		
Validation plan (i.e. requirements to be validated, results of verification, operating modes, acceptance criteria	Clause 9, Clause 10		

NOTE The functional safety plan can be part of the overall technical machine documentation and is not necessarily a single document.

B.3 Safety requirements specification

B.3.1 General

This Clause B.3 sets out the procedures to specify the requirements of safety function(s) to be implemented by the SCS or SRP/CS.

Each safety function will be specified by:

– functional requirements specification;

– safety integrity requirements specification.

B.3.2 Functional requirements

The input information resulting from the application of the overall risk assessment and risk reduction process for the particular machine design is necessary and is described in 4.1 of this document. This information will be available to produce both the functional requirements specification (see Table B.2) and the safety integrity requirements specification of the SCS or SRP/CS.

Table B.2 – Overview of basic functional requirements

Functional requirements	Main items to be considered	Input information Source of requirement	Output information Where information can be found
Description of safety function	– Limits of the machine according to ISO 12100 – The risk associated with a particular hazardous situation according to ISO 12100 [a]		
Operating environment	– Limits of the machine according to ISO 12100 (e.g. electromagnetic immunity, temperature, humidity, dust, chemical substances, mechanical vibration and shock) [a]		
Condition(s) (e.g. operating mode) of the machine	– Specifications for the intended performance of the related risk reduction/protective measure according to ISO 12100 [a]		
Priority			
Reset			
Frequency of operation			
Response time			
Fault reaction	Restart conditions, constraints		
Interfaces to other machine functions			
Tests	Test equipment		
Other specific requirements			

[a] For input information coming from the risk assessment process according to ISO 12100, see 4.4 of this document.

B.3.3 Safety integrity requirements

The required safety integrity for each safety function to be carried out by an SCS or SRP/CS will be specified in terms of SIL according to Table B.3 and documented.

Table B.3 – SIL and limits of PFH values

SIL	Limits of PFH values (1/h)
1	$< 10^{-5}$
2	$< 10^{-6}$
3	$< 10^{-7}$

B.4 Protection against unexpected start-up

The unexpected start-up of a machine is relevant during all design activities and the relevant requirements of ISO 14118 will be considered. While designing a safety-related stopping function, for example, the prevention of unexpected start-up will be considered in the context of this safety function: this does not mean that the prevention of unexpected start-up is a separate or additional safety function, but that it will be considered in addition to the design of a safety function.

Further examples of unexpected start-up are when:

- there could be a danger of unexpected restarting of the machine while the operator readjusts the workpiece or during maintenance activities;
- the function "manual reset" is required to be a safety function;
- the interlocking device associated with the interlocking guard with a start function is designed such that its failure cannot lead to an unintended/unexpected start-up.

B.5 Decomposition of the safety function

B.5.1 General

Based on the safety requirements specification, SCS or SRP/CS can be designed by:

- selection of subsystems,
- determining the safety integrity,
- complying with the requirements of the systematic safety integrity of the SCS or SRP/CS, including, where applicable, electromagnetic immunity, security, periodic testing and, software.

B.5.2 Subsystem architecture based on top-down decomposition

An SCS can include:

- one or several pre-designed subsystem(s), and/or
- one or several subsystem(s) developed according to this document, based on subsystem element(s).

B.6 Design of the SCS by using subsystems

Each safety function will be decomposed to a structure of sub-function(s). Each sub-function will be performed by a subsystem (allocation to subsystem).

A typical decomposition of a safety function is represented in Figure B.1.

As represented in Figure B.1 the SIL(s) that can be achieved by the SCS will be considered separately for each safety function and will be determined from the SIL and the PFH value of each subsystem, as follows:

– the SIL that is achieved is equal to or less than the lowest SIL of any of the subsystems, and
– the SIL is limited by the summation of PFH values of all subsystems.

	Safety function to be performed by SCS or SRP/CS, required safety integrity		
1.	**Input sub-function** (initiation event, cause)	**Logic sub-function**	**Output sub-function(s)** (machine actuator, effect)
2.	**Subsystem performing the sub-function** (allocation of subsystem)	**Subsystem performing the sub-function** (allocation of subsystem)	**Subsystem(s) performing the sub-function** (allocation of subsystem)
3. a	**Selecting of pre-designed subsystem** according to IEC 62061 or IEC 61508 or IEC 61496, or ISO 13849-1 – SIL or PL and – PFH	Pre-designed subsystem according to IEC 61508 or IEC 61496	**Selecting of pre-designed subsystem** according to IEC 62061 or IEC 61508 or IEC 61496, or ISO 13849-1 – SIL or PL and – PFH
	OR		**OR**
3. b	**Design of subsystem** according to IEC 62061 or ISO 13849-1 – Architecture constraints (SFF) or Category – SIL or PL PFH	– SIL or PL – PFH	**Design of subsystem** according to IEC 62061 or ISO 13849-1 – Architecture constraints (SFF) or Category – SIL or PL PFH
4.	**SCS performing a safety function, achieved safety integrity** – Achieved SIL or PL is equal the lowest SIL or PL of all subsystems – Achieved PFH value of the SCS is the summation of PFH values of all subsystems		

Figure B.1 – Example of decomposition of a safety function

B.7 Requirements for systematic safety integrity

B.7.1 General

These requirements apply to the SCS or SRP/CS level and subsystem level.

B.7.2 SCS level

Measures on the SCS or SRP/CS level are summarized in Table B.4 and Table B.5.

Table B.4 – Avoidance of systematic failures (SCS or SRP/CS level)

Avoidance of systematic failure (Use of adequate components)	Main items to be considered	Input information Source of requirement	Output information Where information can be found
Functional safety plan			
Appropriate selection, combination, arrangements, assembly and installation	– Wiring interconnection of subsystems	Subsystem design (7.3.3)	
SCS within the manufacturer's specification	– Manufacturer's information (see specification and installation instructions)	Manufacturer	
Electrical safety	– Wiring and cabling	IEC 60204-1	
Foreseeable misuse, environmental changes or modification(s)			
Manufacturer's instructions	– hardware aspects (and interconnections) – Software aspects – Diagnostic coverage aspects	Manufacturer	
Final design steps			
Hardware design review	– Inspection or walk-through – Analysis to reveal discrepancies between the specification and implementation	Validation (verification)	
Simulation or analysis	– Using Software tools if helpful – Functional performance and the correct dimensioning of components – Interactions of subsystems	Validation (verification)	

Table B.5 – Control of systematic failures (SCS or SRP/CS level)

Control of systematic failure (application measures)	Main items to be considered	Input information Source of requirement	Output information Where information can be found
Control the effect of temporary subsystem failures	– Supply variation – Electromagnetic interference	IEC 60204-1	
Basic safety principles (ISO 12100, ISO 13849-2)			
Use of de-energization	– Loss of power supply leads to safe state	Manufacturer Product standards	
Control of data communication process	– Error detection	Product standards	
Well-tried safety principles (ISO 12100, ISO 13849-2)			
Dangerous fault at an interface (cabling of inputs and outputs of subsystems)	– Diagnostic function and DC evaluation – Fault reaction function to be performed before the hazard		

B.7.3 Subsystem level

Measures on the subsystem level are summarized in Table B.6 and Table B.7.

Table B.6 – Avoidance of systematic failures (subsystem level)

Avoidance of systematic failure **(Use of adequate components)**	**Main items to be considered**	**Input information** **Source of requirement**	**Output information** **Where information can be found**
Appropriate selection, combination, arrangements, assembly and installation	– Manufacturer's information (see application user manual, installation instructions, specifications) – Use of good engineering practice (e.g. IEC 60204-1)	Manufacturer ISO 13849-2	
Subsystem and subsystem elements within the manufacturer’s specification	– Manufacturer's information (see specification and installation instructions)	Manufacturer	
Components with compatible operating characteristics	– Previous design experience	Design experience	
Environmental conditions specified	– Especially temperature, humidity, vibration and electromagnetic fields	ISO 12100	
Components used in accordance with product standard	– Electromechanical – Hydraulics – Pneumatics	Manufacturer Product standards	
Use of suitable materials and adequate manufacturing	General requirements for the machine design, see ISO 12100	ISO 12100	
Correct dimensioning and shaping			
Final design steps			
Hardware design review	– Inspection or walk-through – Analysis to reveal discrepancies between the specification and implementation	Validation (verification)	
Simulation or analysis	– Using Software tools if helpful – Functional performance and the correct dimensioning of components	Validation (verification)	

Table B.7 – Control of systematic failures (subsystem level)

Control of systematic failure (application measures)	Main items to be considered	Input information Source of requirement	Output information Where information can be found
Control of change of voltage	– Effects of insulation breakdown – Voltage variations and interruptions, overvoltage and undervoltage – Use of PELV/SELV power supply	IEC 60204-1	
Control of effects of physical environment	– temperature, humidity, water, vibration, dust, corrosive substances – electromagnetic interference and its effects	Manufacturer	
Control of change of temperature	– over-temperature to be detected where not avoided	ISO 12100	
Control of change of pressure	– hose breakdown – pressure variations and interruptions	ISO 4414 (pneumatics) ISO 4413 (hydraulics)	
Basic safety principles (ISO 12100, ISO 13849-2)			
Use of de-energization	– Loss of power supply leads to safe state	Manufacturer Product standards	
Control of data communication process	– Error detection	Product standards	
Well-tried safety principles (ISO 12100, ISO 13849-2)			
Failure detection by automatic tests	– Diagnostic function and DC evaluation – Redundant hardware (dual channel)		
Diverse hardware			
Operation in the positive mode	E.g. position switch for guard interlocking	Product standards	
Mechanically linked contacts	E.g. mirror contacts of contactors	Product standards	
Direct opening action			
Over-dimensioning	E.g. 50 %		

B.8 Electromagnetic immunity

The function of electrical or electronic safety-related systems should not be affected by external influences in a way that could lead to an unacceptable risk.

Additional guidance is given in this document in Clause E.2 (Measures to reduce the effects of EMI based on IEC 60204-1:2016, Annex H and IEC 60204-1:2016/AMD1:2021, Annex H).

B.9 Software-based manual parameterization

The objective of these requirements is to guarantee that the safety-related parameters specified for a safety function or for a sub-function are correctly transferred into the hardware performing the safety function or the sub-function. This Clause B.9 is limited in scope to only manual, software-based parameterization that is performed and controlled by an authorized person.

Where a subsystem is capable of providing a software based manual parameterization performed by application software level 1, the fulfilment of requirements is necessary to prevent dangerous failure due to the influences listed below (see also 6.7.2 of IEC 62061:2021) or any other influence that is reasonably foreseeable:

– data entry errors by the person responsible for parameterization;
– faults of the software of the parameterization tool;
– faults of further software and/or service provided with the parameterization tool;
– faults of the hardware of the parameterization tool;
– faults during transmission of parameters from the parametrization tool to the SCS or SRP/CS or a subsystem;
– faults of the SCS or a subsystem to store transmitted parameters correctly;
– systematic interference during the parameterization process, e.g. by electromagnetic interference or loss of power;
– interference due to external influences or factors, such as electromagnetic interference or (random) loss of power.

Where a parameterization tool is used, the relevant requirements for a subsystem according to IEC 61508 to ensure correct parameterization should be fulfilled.

NOTE This is typically the case when a component manufacturer provides this tool in conjunction with the subsystem, e.g. parameterization of drive functions of IEC 61800-5-2.

Table B.8 gives an overview of the main items to be considered for software-based manual parameterization.

Table B.8 – Software-based manual parameterization

Measures	**Main items to be considered**	**Input information** **Source of requirement**	**Output information** **Where information can be found**
Safety requirements specification	– Software safety requirements specification		
Check of data plausibility	– Checks of data limits, format and/or logic input values		
Integrity of all data used	– Control the range of valid inputs; – Control data corruption before transmission; – Control the effects of errors from the parameter transmission process; – control the effects of incomplete parameter transmission; – Control the effects of faults and failures of hardware and software of the parameterization; and – Control the effect of interruption of the power supply		
Special procedure (when tool is not designed according to IEC 61508)	– Retransmitting of modified parameters to the parameterization tool; or – Other means to confirm the integrity of the parameters or subsequent confirmation – New values of safety-related parameters shall not be activated before the changes are acknowledged and confirmed		

B.10 Security aspects

When security countermeasures are applied, they shall not adversely affect safety integrity (e.g. increase in response time, etc.). This can require an iterative multi-disciplinary team analysis.

Security risks will be evaluated by using a security risk assessment in order to identify the security objectives.

A security risk assessment is based on a product or system in its environment on which threats and known vulnerabilities are applied. The aim of this activity is to derive relevant security countermeasures applied for a machine to fulfil the overall security objectives.

When security countermeasures implemented within the SCS are declared, then information shall be provided as appropriate.

In the context of safety of machinery, the security countermeasures are intended to protect the ability to maintain safe operation of a machine and their implementation should not adversely affect any safety function.

Figure 2 of IEC TR 63074:2019 shows in this context the possible effects of security risk(s) to an SCS, as shown in Figure B.2.

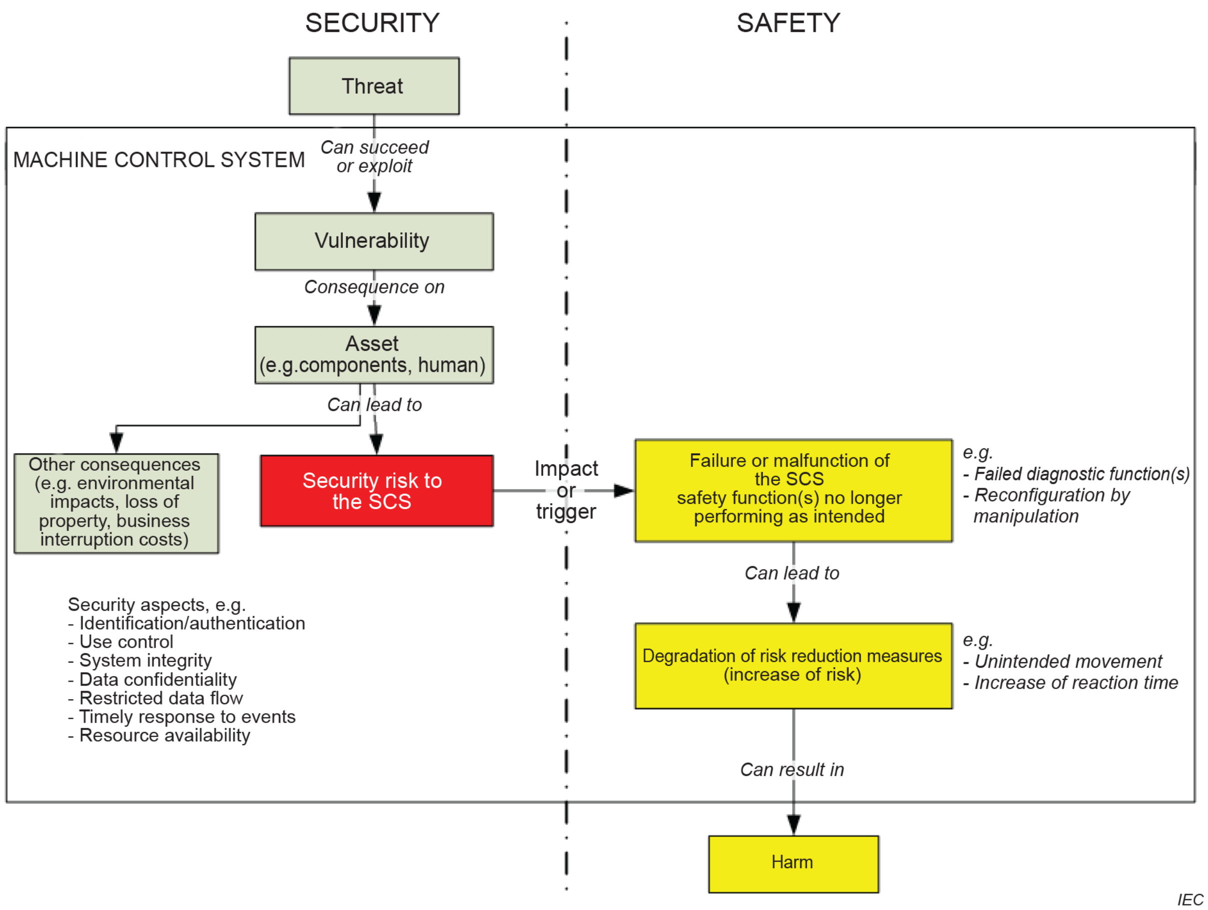


Figure B.2 – Possible effects of security risk(s) to a SCS (IEC TR 63074:2019, Figure 2)

B.11 Aspects of testing

Depending on the mode of operation, two types of testing types exist:

– for safety functions, diagnostic tests are carried out automatically (initiated automatically or manually) and frequently (related to the process safety time and demand rate); and
– for rarely activated safety functions, initial and periodic verification tests in addition to diagnostic tests (see Clause 7).

B.12 Design and development of a subsystem

B.12.1 General

There are two types of requirements to subsystems and subsystem elements:

– qualitative requirements:
  - for the avoidance and the control of systematic failures (see Clause B.7);
  - fault consideration(s) and fault exclusion(s) (see B.12.3);
– quantitative requirements:
  - failure rate (λ (Lambda), MTTF (mean time to failure) or B_{10});
  - and other relevant parameters (e.g. useful lifetime T_{10}).

For non-electronic components the following requirements especially will be considered:

a) the useful lifetime is limited to T_{10} and components will be exchanged if no other information is given by product standards (see also 6.5.3.2);
b) when a functional test for non-electronic technology is necessary to detect a possible accumulation of faults or an undetected fault before the next demand, it will be made within the following test intervals:
   – at least every month for SIL 3;
   – at least every 12 months for SIL 2.

This requirement is based on the experience that subsystems with non-electronic technology, e.g. guard door monitoring, where infrequent operation is likely and the monitoring function cannot be possible unless there is a change of state and meanwhile an accumulation of faults is possible.

B.12.2 Subsystem architecture design

B.12.2.1 General

Any subsystem based on one or several subsystem elements is performing a sub-function of a safety function and the failure of a subsystem leads to a loss of the safety function.

Subsystem(s) incorporating complex components will comply with appropriate product standards or IEC 61508-2 and IEC 61508-3 as appropriate for the required SIL and the design will use Route 1_H (see IEC 61508-2:2010, 7.4.4.2) for high demand and/or continuous mode.

Where a subsystem design includes such a complex component as a subsystem element, it can be considered as a low complexity component. For example, where a PDS is used for STO according to IEC 61800-5 with a safety integrity of SIL 2, this can be used in a subsystem basic architecture D as a one subsystem element, and by using an additional subsystem element, e.g. contactor, this subsystem can claim SIL 3.

B.12.2.2 Monitoring of initiation event (cause)

Two possible cases for detection of a demand of a safety function exist:

- Case 1, continuous mode of operation

The initiation event is realized in continuous mode of operation.

EXAMPLES The following continuous mode detections of dangerous situations are possible:

- Position monitoring by controlling of actual position value compared with acceptable threshold
- Speed monitoring by controlling of actual speed value compared with acceptable threshold;
- Temperature monitoring by controlling of actual temperature value compared with acceptable threshold;
- Pressure monitoring by controlling of actual temperature value compared with acceptable threshold

- Case 2, event triggered

The initiation event is detected only with the demand of the safety function.

EXAMPLES The following event triggered detections of dangerous situation are possible:

- Guard door monitoring by position switch(es);
- Position control by over travelling sensor switching off by reaching dangerous position;
- Overtemperature control by digital temperature sensor switching off at dangerous temperature;
- Overpressure control by overpressure sensor switching off at dangerous pressure.

B.12.2.3 Initiation of reaction function (effect)

Two possible cases to react on a demand of a safety function exist:

- Case 1, continuous mode of operation

The initiation of the reaction function is realized in continuous mode of operation.

EXAMPLES The following continuous mode monitoring of the reaction function is possible:

- Stop of dangerous movements by STO of PDS;
- Temperature monitoring by automatic temperature control unit – thermostat;
- Pressure monitoring by automatic pressure control unit – pressure switch and control circuit.

- Case 2, event triggered

The initiation of the reaction function is performed only with the demand of the safety function.

EXAMPLES The following event triggered monitoring of the reaction function is possible:

- Switching off a contactor of a motor to stop dangerous movement;
- Stop of hydraulic or pneumatic movements by switching a valve into defined state;
- Activation of a break to hold a hydraulic axis in position.

B.12.2.4 Design possibilities

The design of rarely activated safety functions depends on either whether persons are to be protected or the integrity of the machine is to be guaranteed, see Table B.9.

Table B.9 – Cause and effects of rarely activated safety functions

Continuous mode of operation	Event triggered	Behaviour	Demand of safety function for protection of	
			Persons	Integrity of machine
Input (initiation event as cause)				
Dynamic changing signal value of sensor		Dynamical monitoring of physical parameters		Process itself
	Binary changing signal of sensor (ON/OFF, OFF/ON)	Static monitoring	Operator (human action)	Process itself
Output (initiation of reaction function as effect)				
Dynamic control of actuator		PDS	Operator (human action)	Process itself
	Actuator binary switching-off	De-energizing of power elements responsible for movements, pressure, temperature, vibration, …	Operator (human action)	Process itself

These design possibilities will be considered for test requirements, see Clause 6.

B.12.2.5 Architectures of rarely activated safety functions

Demand mode of operation of subsystems performing rarely activated safety functions can be different and leads to possible combinations as represented in Figure B.3.

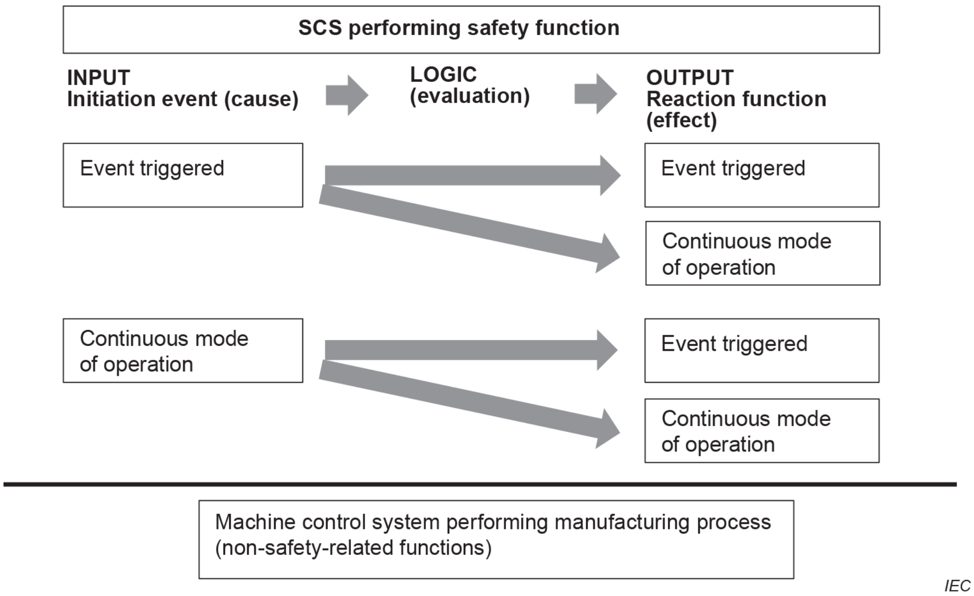


Figure B.3 – Rarely activated safety functions and mode of operation of subsystems

B.12.3 Fault consideration and fault exclusion

The limitations of fault consideration and fault exclusion are as follows: For some applications, it is not expected that all failures can be excluded with sufficient confidence for SIL 3.

B.12.4 Architectural constraints of a subsystem

The architectural constraints limit the claimed SIL of a subsystem independent of the PFH value of this subsystem (see 6.3).

As diagnostic coverage of subsystem element(s) is the basis for evaluation of SFF the effectiveness of diagnostic functions becomes important. The effectiveness of a diagnostic function can only be guaranteed when a fault reaction function is provided, see IEC 62061:2021, 7.4.3.

The diagnostic functions are considered as separate functions that can have a different structure than the safety function and can be performed by

– the same subsystem which requires diagnostics; or
– other subsystems of the SCS or SRP/CS; or
– subsystems of the SCS or SRP/CS not performing the safety function.

Table B.10 shows the worst-case requirements of architectural constraints and basic requirements. Subsystems designed according to IEC 62061 can be assigned to PL and categories of ISO 13849-1.

Table 7 of this document shows this assignment of maximum SIL and architecture constraints according to IEC 62061 to maximum PL and categories according to ISO 13849-1.

Table B.10 – Architectural constraints and basic requirements on a subsystem

Safe failure fraction SFF = DC_{avg}	**Hardware fault tolerance (HFT) [a]**		**Basic requirements (see [c])**	
	0	**1**		
	1 subsystem element (as single channel subsystem)	**2 subsystem elements (as dual channel subsystem)**		
< 60 %	SIL 1 well-tried components required no CCF requirements	SIL 1	Basic safety principles and well-tried safety principles	CCF
60 % to < 90 %	SIL 1	SIL 2		
90 % to < 99 %	SIL 2	SIL 3		
≥ 99 %	SIL 3 (see [b])	SIL 3		

[a] A hardware fault tolerance of N means that N+1 faults could cause a loss of the safety function.

[b] For HFT 0 and SFF ≥ 99 %, the following limitations can be relevant:

– It is highly recommended to limit the maximum of SIL 2 where fault exclusions have been applied to faults that could lead to a dangerous failure (see 7.3.3.3);

– SIL 3 can only be claimed when there is continuous monitoring of the correct functioning of the element. Typically, electronic technology will be required to achieve this.

[c] For basic requirements see also ISO 13849-2:2012, Annex A to Annex D. Examples are: For basic safety principles, this means the use of suitable materials; for well-tried safety principles, the use of deenergizing; and for well-tried components, the use of contactors or position switches.

For a single channel subsystem (HFT = 0):

$$SFF = DC_{avg} = \frac{\lambda_{DD1}}{\lambda_{D1}} = \frac{DC_1 \times \lambda_{D1}}{\lambda_{D1}} = DC_1$$

For a dual channel subsystem (HFT = 1):

$$\mathrm{SFF} \approx \mathrm{DC}_{\mathrm{avg}} = \frac{\lambda_{\mathrm{DD1}} + \lambda_{\mathrm{DD2}}}{\lambda_{\mathrm{D1}} + \lambda_{\mathrm{D2}}} = \frac{\mathrm{DC}_1 \times \lambda_{\mathrm{D1}} + \mathrm{DC}_2 \times \lambda_{\mathrm{D2}}}{\lambda_{\mathrm{D1}} + \lambda_{\mathrm{D2}}} = \frac{\frac{\mathrm{DC}_1}{\mathrm{MTTF}_{\mathrm{D1}}} + \frac{\mathrm{DC}_2}{\mathrm{MTTF}_{\mathrm{D2}}}}{\frac{1}{\mathrm{MTTF}_{\mathrm{D1}}} + \frac{1}{\mathrm{MTTF}_{\mathrm{D2}}}}$$

where

λ_{DD1}, λ_{DD2} is the rate of dangerous failure of subsystem element 1 and 2 which is detected by the diagnostic functions;

λ_{D1}, λ_{D2} is the rate of dangerous failure of subsystem element 1 and 2;

DC_1, DC_2 is the diagnostic coverage of subsystem element 1 and 2.

B.12.5 Subsystem design architectures

Based on the hardware failure tolerance and the architectural constraints typical basic subsystem architectures are proposed in IEC 62061:2021, 7.5.2 which are widely used in the context of the safety of machinery:

– Basic subsystem architecture A as single channel subsystem without a diagnostic function, or described as 1oo1
(special case of basic subsystem architecture C with DC = 0)
– Basic subsystem architecture B as dual channel subsystem without a diagnostic function, or described as 1oo2
(special case of basic subsystem architecture D with DC = 0 for both channels);
– Basic subsystem architecture C as single channel subsystem with a diagnostic function, or described as 1oo1D;
– Basic subsystem architecture D as dual channel subsystem with a diagnostic function, or described as 1oo2D;

Other architectures can be used instead to evaluate the PFH value and a claimed SIL but this document does not offer further information for evaluation as these architectures are not commonly used in practice.

B.12.6 PFH value of subsystems

To evaluate the PFH value of a subsystem, Annex H provides further information.

Relevant parameters to be considered are:

– selected basic subsystem architecture;
– evaluated DC values (0 %, 60 %, 90 % or 99 %, see also Annex D) and test intervals for each subsystem element;
– estimated CCF factor β (10 %, 5 %, 2 % or 1 %, see also Annex E);
– estimated or calculated λ_{D} (or $\mathrm{MTTF}_{\mathrm{D}}$) of each subsystem elements;
– useful lifetime T_1 which can be limited to T_{10}.

This document gives in Clause H.5 to Clause H.12 further relevant information of derivation of the PFH formulas in order to provide a better understanding of the PFH value evaluation and to prevent misuse of evaluated PFH values.

B.13 Validation

Initial verification corresponds to the validation process (see Clause 7 of this document). Table B.11 gives an overview of validation process.

Table B.11 – Overview of validation process with required information

	Validation process	Input information Source of requirement	Output information Where information can be found
Input information for validation process	**Validation plan with basic requirements**		
	– Specification documents identified? – Operational and environmental conditions during testing specified? – Analyses and tests to be applied, – Reference to test standards to be applied, – Persons or parties responsible for each step in the validation process – The required equipment		
	Fault lists		
	– Faults taken from the generic list(s) to be included, – Any other relevant faults to be included, – Faults taken from the generic list(s) which may be excluded – Exceptionally any other faults		
	Information necessary for validation		
	– Specification of the required characteristics of each safety function – Block diagram(s) – Circuit diagram(s) – Functional description – Time sequence diagram(s) for switching components – Relevant characteristics of components previously validated – Relevant characteristics of components not yet previously validated – Analysis of all relevant faults – Information for use, e.g. installation and operation manual/instruction handbook – Safety-related characteristics of designed subsystem(s)		

Table B.11 – Overview of validation process with required information (continued)

	Validation process	Input information Source of requirement	Output information Where information can be found
Activities during the validation process	**a) Analysis as part of validation**		
	Input information: – Safety function(s) and their characteristics – SCS or SRP/CS structure and subsystem architectures – Quantifiable aspects and qualitative aspects (systematics, software) Verification of safety requirements specification (SRS) regarding consistency, completeness and correctness: – Intended application and safety aspects considered? – All conditions and human behaviour considered?		
	b) Testing as part of validation		
	Test procedure by: – Test plan (test specifications, required test outcome, chronology) – Test records (persons, environmental conditions, test equipment, etc.) – Comparison of test records with test plan		
	c) Validation of the safety function		
	– Demonstrating that the SCS or SRP/CS provides the safety function(s) in accordance with their specified characteristics. – Use of analysis and testing (with fault injection)		
	d) Validation of the safety integrity of the SCS or SRP/CS		
	– Verification of all safety-related characteristics and validation of subsystems and combination of subsystems – Validation of all measures against systematic failures – Validation of safety-related software		

B.14 Documentation

Table B.12 gives an overview based on the SCS or SRP/CS design activities.

Table B.12 – Technical documentation based on the design process (Table 9 of IEC 62061:2021, modified)

Topics	Main items
Functional safety plan	
Safety requirements specification (SRS)	Functional requirements specification (for SCS or SRP/CS)
	Safety integrity requirements specification (for SCS or SRP/CS)
SCS design	Structured design process
	Structure of sub-functions
	SCS architecture
	Sub-function and subsystem safety requirements
Subsystem design and realization	Subsystem architecture
	Fault exclusions claimed when estimating fault tolerance/SFF
	Subsystem assembly
Software	Software safety requirements
	Software based parameterization
	Software configuration management items
	Suitability of software development tools
	Documentation of the application program
	Results of application software module testing
	Results of application software integration testing
Validation	Validation plan
	Validation principles
Documentation	Documentation of SCS or SRP/CS integration (testing)
	Documentation of well-tried components
	Documentation for installation, use and maintenance
	Documentation of SCS validation
	Documentation for SCS configuration management

Table B.13 gives an overview of all relevant information, especially in the context of information for use given either

– by the manufacturer of subsystems or
– by the SCS or SRP/CS integrator.

The manufacturer of a subsystem can be the machine manufacturer, the integrator of machinery or the component manufacturer.

NOTE The integrator can be for example a manufacturer, assembler, engineering company, or entity with the overall responsibility for the machine.

Documentation in terms of information for use will be made available to users of subsystem(s) or SCS designed according to IEC 62061 or SRP/CS designed according to ISO 13849-1.

Table B.13 – Overview of documentation

Overview of documentation	Input information Source of requirement	Output information Where information can be found
Specification of safety integrity		
– SIL 1, 2 or 3, – if relevant, architectural constraints of the subsystem(s).		
Technical documentation relevant to all safety-related parts		
– Documentation according to Table 9 of IEC 62061:2021 – Safety function(s) provided by the SCS according to Clause 5 or safety sub-function provided by the SCS subsystem – Subsystem when designed (according to Clause 7) (including test or analysis of fault behaviour) – Characteristics of each safety function – Environmental conditions – Measures against systematic failure – Well-tried components when used	IEC 62061:2021, Table 9	
Information for use given by the manufacturer of subsystems (for the safe installation, use and maintenance of the subsystem)		
– Description of the subsystem (general, function, installation, interface(s), configuration/settings/programming) – Information on operating limits (environmental limits, interfacing limits, other limits like operating frequency, etc.) – Fault exclusions – Necessary measures at the subsystem to prevent degradation of the intended SCS function – Provisions for the maintainability – Response time of the subsystem – Useful lifetime of the subsystem – Diagnostic functions – Inspection procedures – Safety-related parameters		
Information for use given by the SCS integrator (for the machine user to develop procedures to ensure that the required functional safety of the SCS is maintained during use and maintenance of the machine)		
– Operating limits of the SCS (including environmental conditions) – Clear descriptions and related instructions for the user interfaces with the SCS (e.g. operator panel, indications and alarms) – Description (including interconnection diagrams) – Marking if required, according to ISO 12100:2010, 6.4.4 – Useful lifetime and requirements for the SCS components – Any operating mode relevant to the safety function(s) – Tools necessary for maintenance and re-commissioning, and the procedures for maintaining the tools and equipment – Provisions for maintenance and all information for maintenance (procedures for fault diagnosis and repair, procedures for confirming correct operation subsequent to repairs and preventive maintenance and corrective maintenance		

Annex C
(informative)

Examples of $MTTF_D$ values for single components

This Annex C describes different methods to calculate or evaluate $MTTF_D$ values for single components. Table C.1 and Table C.2 summarize relevant information (for more information on Table C.1, see IEC 62061 or ISO 13849-1).

Table C.1 – $MTTF_D$ or B_{10D} values for components (derived from ISO 13849-1:2015)

Component	Typical $MTTF_D$ [*a*] or B_{10D} [*cycles*] values
Mechanical components	$MTTF_D$ = 150
Hydraulic components with $n_{op} \geq$ 1 000 000	$MTTF_D$ = 150
Hydraulic components with 1 000 000 > $n_{op} \geq$ 500 000	$MTTF_D$ = 300
Hydraulic components with 500 000 > $n_{op} \geq$ 250 000	$MTTF_D$ = 600
Hydraulic components with 250 000 > n_{op}	$MTTF_D$ = 1 200
Pneumatic components	B_{10D} = 20 000 000
Relays and contactor relays with small load (mechanical load)	B_{10D} = 20 000 000
Relays and contactor relays with maximum load	B_{10D} = 400 000
Proximity switches with small load (mechanical load)	B_{10D} = 20 000 000
Proximity switches with nominal load	B_{10D} = 400 000
Contactors with small load (mechanical load)	B_{10D} = 20 000 000
Contactors with nominal load	B_{10D} = 1 300 000 (see [a])
Position switches	B_{10D} = 20 000 000
Position switches (with separate actuator, guard-locking)	B_{10D} = 2 000 000
Emergency stop devices	B_{10D} = 100 000
Push buttons (e.g. enabling switches)	B_{10D} = 100 000

[a] B_{10D} is estimated as two times B_{10} (50 % dangerous failure) if no other information (e.g. product standard) is available.

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

Table C.2 – Relationship of λ_D, $MTTF_D$ and B_{10D}

Formulas	Units	Parameters
$\lambda_D \approx 0{,}1 \frac{C}{B_{10D}} = \frac{C}{10} \frac{\text{RDF}}{B_{10}}$	$\left[\frac{1}{h}\right]$	$C = \frac{cycles}{hour[h]}$
$\text{MTTF}_D = \frac{1}{\lambda_D \; 8\,760} \approx \frac{10}{n_{op}} \frac{B_{10}}{\text{RDF}}$	$[a]$	$n_{op} = \frac{cycles}{year[a]}$
$T_{10D} = \frac{B_{10D}}{n_{op}} \approx \frac{\text{MTTF}_D}{10}$	$[a]$	$B_{10D} = \frac{B_{10}\,[\text{cycles}]}{\text{RDF}}$ Ratio of dangerous failures (RDF)

Annex D
(informative)

Examples for diagnostic coverage (DC)

D.1 General

A diagnostic function represents a periodic testing function (see IEC 62061:2021, 6.9) performed by a subsystem of an SCS or SRP/CS.

Diagnostic functions are carried out:

– automatically (initiated automatically or manually) and

– frequently (related to the process safety time and demand rate).

Therefore, a diagnostic coverage DC can only be claimed (see IEC 62061:2021, 7.4.3 and 7.4.4) for a diagnostic function when:

– a fault reaction is implemented
  - to set the relevant parts of the machine in a safe state as a consequence of a detected fault and
  - to be performed before a hazard due to this fault can occur;

– the diagnostic test interval is adequate to reveal failures at least at the demand of a safety function (diagnostic test interval is greater or equal to the demand rate).

Consequently, an analysis of each subsystem element is performed to determine all relevant faults and their corresponding failure modes (see IEC 62061:2021, 7.3.3).

The DC of each subsystem element has a significant impact on the estimation of SFF (see IEC 62061:2021, 7.4.2). Using the worst-case approach $\lambda_s \approx 0$ and depending on HFT, SFF can be estimated with following equations:

For HFT=0

$$\text{SFF} = \text{DC}_{\text{avg}} = \frac{\lambda_{\text{DD1}}}{\lambda_{\text{D1}}} = \frac{\text{DC}_1 \times \lambda_{\text{D1}}}{\lambda_{\text{D1}}} = \text{DC}_1 \qquad \text{(D.1)}$$

For HFT=1

$$\text{SFF} \approx \text{DC}_{\text{avg}} = \frac{\lambda_{\text{DD1}} + \lambda_{\text{DD2}}}{\lambda_{\text{D1}} + \lambda_{\text{D2}}} = \frac{\text{DC}_1 \times \lambda_{\text{D1}} + \text{DC}_2 \times \lambda_{\text{D2}}}{\lambda_{\text{D1}} + \lambda_{\text{D2}}} = \frac{\frac{\text{DC}_1}{\text{MTTF}_{\text{D1}}} + \frac{\text{DC}_2}{\text{MTTF}_{\text{D2}}}}{\frac{1}{\text{MTTF}_{\text{D1}}} + \frac{1}{\text{MTTF}_{\text{D2}}}} \qquad \text{(D.2)}$$

where

λ_{DD1}, λ_{DD2} is the rate of dangerous failure of subsystem element 1 and 2 which is detected by the diagnostic functions;

λ_{D1}, λ_{D2} is the rate of dangerous failure of subsystem element 1 and 2;

DC_1, DC_2 is the diagnostic coverage of subsystem element 1 and 2.

D.2 Influence of cabling, wiring and interconnections

D.2.1 General

To ensure the systematic integrity of an SCS or SRP/CS measures to avoid systematic hardware failures are implemented on subsystem and SCS or SRP/CS level. Cabling, wiring and interconnections can have an impact on the capability of a diagnostic function and can therefore limit a possible DC for a subsystem element: Specific fault considerations and possible fault exclusions lead to potential impacts on the DC evaluation.

Basically, the measures in Table D.1 to prevent short circuit and impacts on maximum claimable DC can exist.

Table D.1 – Measures to prevent of short circuit

Fault	Measure	Examples
Short circuit Prevention of short circuit by applying – well-tried safety principles and fault exclusion, or – by cross-monitoring, direct or indirect monitoring	Basic safety principles (see also IEC 60204-1, ISO 13849-1):	
	– Use of de-energization	Use of high active signals (loss of power supply, wiring interruption or short circuit)
	Well-tried safety principles (see also IEC 60204-1, ISO 13849-1):	
	– Fault avoidance in cables	External to enclosure: Cable with shielding connected to the protective bonding circuit on each separate conductor
	– Separation distance	Sufficient distance between position terminals, components and wiring to avoid unintended connections
	Faults and fault exclusions (see also IEC 60204-1, ISO 13849-1)	

	Between any two conductors	– Permanently connected (fixed) and protected against external damage, e.g. by cable ducting, armouring, or
		– Within an electrical enclosure, or
		– External to enclosure:
		  – Individually shielded with earth connection or
		  – Separate multicore cables

	Between adjacent terminals	Terminals and connections in accordance with IEC 60947-7-1 or IEC 60947-7-2 and the requirements of IEC 60204-1
	Well-tried component (see also IEC 60204-1, ISO 13849-1)	
	Cable	Cabling external to enclosure protected against mechanical damage (including, e.g. vibration or bending)
	Diagnostic function	
	– Cross-monitoring – Direct or indirect monitoring	Evaluation of plausibility of status of signal(s)

NOTE 1 Measures to avoid short circuit are applied to single and dual channel subsystems.

NOTE 2 For dual channel subsystem DC = 99 % for each subsystem element achievable where fault(s) due to short circuit can be prevented.

D.2.2 "Serial wiring"

Undetected or masked faults are possible where a serial wiring of signals is used. Measures to prevent an accumulation of faults will be applied depending on the application and on the probability of occurrence of an accumulation. Where an accumulation of faults cannot be excluded, a DC of less than 90 % should be assumed.

EXAMPLE 1 Monitoring of three interlocked safeguards, where two position switches are used for each interlocked safeguard and the evaluation of these position switches is realized by a "serial wiring". When one operator is opening and closing only one safeguard at the same time due to the manufacturing process, then the probability of occurrence of masking faults by one of the other safeguards can be excluded. When one operator uses any of the safeguards to enter the same hazardous area, then the probability of occurrence of masking faults by one of the other safeguards can occur and a possible foreseeable misuse cannot be excluded. DC of 60 % reasonably can be assumed and each subsystem (safeguard) is limited to a maximum achievable SIL 2. See also ISO 14119:2013, 8.6 and ISO/TR 24119 for more information.

EXAMPLE 2 Emergency stop devices are wired in serial by using two electrical contact elements that are opened by a direct opening action with mechanical latching. The electrical contact elements are wired in serial. It can be excluded that an operator will push one emergency stop device and then a second one. The probability of occurrence of masking faults can be considered as very low, and therefore excluded. DC of 99 % can be assumed and each subsystem (emergency stop device) can claim SIL 3.

D.3 Use of manufacturing process information

D.3.1 General

The non-safety-related part of the machine control system is performing the manufacturing process and can provide, based on the expected behaviour of the manufacturing process, information which can be used for evaluation of diagnostics on subsystem element(s).

Depending on the manufacturing process diagnostics (test) rate DC measures of the SCS or SRP/CS can lead to a higher DC for subsystem element(s) than without considering this information.

The evaluation of manufacturing process information is realized by the safety-related logic.

Typical reasons for carrying out this procedure are where:

– direct monitoring of a subsystem element is not possible;
– process degradation or process quality problems allow the prediction of upcoming possible hazardous situations before a safety function will be demanded.

Evaluated DC for each subsystem element depending on the process diagnostic test rate (rt) and the demand rate (rd) of the safety function is limited to:

– DC ≤ 60 % when rt/rd > 1;
– DC ≤ 90 % when rt/rd ≥ 10;
– DC ≤ 99 % when rt/rd ≥ 100.

D.3.2 Use of expected timing or awaiting of signal status

Timing of signals due to the manufacturing process can be used for diagnostics, especially where physically a single channel signal is expected to have a specific behaviour.

EXAMPLE 1 An inductive or analogue monitoring device is used by an evaluation dynamic signal that is well-known. Where the behaviour of this dynamic signal deviates from an expected value or threshold a diagnostic function can detect this deviation and initiate a fault reaction function. This can be considered as a single channel subsystem with a DC value of 60 % to 90 % and a maximum achievable SIL 2.

EXAMPLE 2 Direct monitoring of well-tried components (e.g. contactors) by using feedback signals (mirror contacts) wired to non-safety-related hardware but evaluated by a safety-related subsystem (logic with cross-monitoring with dynamic signal change to detect static faults and short circuit).

D.4 Typical DC measures

Table D.2 gives an overview of DC values and examples of recommended measures. When applying a specific measure, the effectiveness of the diagnostics should be considered.

Table D.2 – DC values and recommended measures

DC	Measures	Examples
99 %	Cross monitoring of two channels with dynamic signal change to detect static faults and short circuit	
	Plausibility check of two channels	– Normally open and normally closed mechanically linked contacts
	Direct monitoring (for single or dual channel subsystem)	– Electrical position monitoring of control valves – Monitoring of electro-mechanical devices by mechanically linked contact elements
90 %	Cross monitoring of inputs without dynamic test	– Using manufacturing process (expectation of signal behaviour) – Without short-circuit prevention
	Cyclic test stimulus by dynamic change of the input signals	– Automatically changing an output to check whether the input connected with this output will change state
	Cross monitoring of output signals with dynamic test without detection of short circuits (for multiple I/O)	– Check if the two 3/2 exhaust valves have switched off by making use of a pressure switch and switching on the valves one by one to see if a difference in pressure occurs
	Indirect monitoring	– Monitoring by pressure switch, electrical position monitoring of actuators, monitoring a cylinder is in its end position and remains in this end position
60 %	Cross monitoring of inputs without dynamic test	– Using manufacturing process (expectation of signal behaviour)
	Monitoring some characteristics of the sensor	– Response time – Range of analogue signals, electrical resistance, capacitance

Annex E
(informative)

Measures for the achievement of functional safety with regards to electromagnetic phenomena

E.1 General

Electromagnetic interference can disturb or damage process monitoring, control and automation systems. Currents due to lightning, switching operations, short-circuits and other electromagnetic phenomena can cause overvoltage and electromagnetic interference.

These effects can occur for example:

– where large conductive loops exist,
– where different electrical wiring systems are installed in common routes, e.g. power supply, communication, control or signal cables.

Other electrical disturbances can be caused by electrostatic discharges due to persons coming into contact with the equipment, from the use of mobile phones nearby and operation of frequency converters.

For EMC purposes, electrical equipment for machinery is deemed to be either apparatus or fixed installations. Where electrical safety and electromagnetic compatibility result in different requirements, electrical safety (especially electrical shock) always has the higher priority, see also for example IEC 60204-1.

E.2 Measures

E.2.1 General

The recommendations in E.2.2 to E.2.3 provide guidance to fulfil EMI (electromagnetic interference immunity) for the items of equipment (devices and/or apparatus) and for their integration into the electrical equipment of the machine.

E.2.2 Recommendation for electrical/electronic items of equipment (devices or apparatus)

For the electrical/electronic items of equipment (devices or apparatus):

– When available, only electrical and/or electronic devices or apparatus which meet the requirements of the relevant product standard (with regard to immunity against electromagnetic phenomena) should be used; since a product family/product standard usually gives more specific requirements, it is generally considered that it takes precedence over the corresponding generic standard.
– Examples of product standards are IEC 61326-3-1, IEC 61800-5-2, IEC 61496-1, IEC 60947-5-3[1]. For their integration/installation into the machine electrical equipment, the information for use of the manufacturer will be applied.
– If no relevant dedicated product-family or product standard addressing electromagnetic influences on functional safety exists, the generic standard IEC 61000-6-7:2014 is applicable.

---

[1] Under consideration.

– For subsystems designed according to IEC 62061 or ISO 13849-1, the electromagnetic environment and its phenomena should be considered in the SRS, as required by IEC 61508. The immunity requirements should be based on the foreseeable electromagnetic threats in the real environment over the whole operational life of the equipment. The generic standard IEC 61000-6-7:2014 is applicable if for the subsystem under consideration no relevant dedicated product-family or product standard addressing electromagnetic influences on functional safety are available.

EXCEPTION: For SCS or SRP/CS designed according to PL a or PL b by using Category B of ISO 13849-1 follow the EMI requirements of IEC 61000-6-2:2014.

E.2.3 Recommendation for the integration of an SCS or SRP/CS into the electrical equipment of the machine

For the integration of an SCS or SRP/CS into the electrical equipment of the machine EMI measures according to Annex H of IEC 60204-1:2016 and of IEC 60204-1:2021 can be applied.

Table E.1 provides a list of recommendations to improve electromagnetic immunity of an SCS or SRP/CS and reduce emission of electromagnetic disturbances.

Table E.1 – Non-exhaustive list of recommendations regarding EMI measures for integration of devices or equipment into the electrical equipment of the machine

Examples of EMI measures	Use
Installed in a shielded and earthed cabinet or components in a shielded and earthed housing	Recommended, whenever possible to be installed
Shielded and grounded or twisted cables for sensors and safety related input/output-signals (cable shields are flat, grounded in low impedance close to the components)	
RF-filter, overvoltage and transient protection (e.g. filter, transient-voltage suppression diode, optocoupler, ferrites) for safety related input/output signals	
If applicable: shielded and earthed cables for motors or sine filter between motor and inverter or equivalent measures	
RC filter, fly-back diode or equivalent measures to achieve spark quenching on switching of inductive loads	
…	
Field experience with high reliability of the system	Highly recommended
Harness of low voltage DC to the components in twisted pair	
Suitable EMC filters for power mains (overvoltage and transient protection)	
Separation of EMC sources and sensitive components e.g. – separate routing and location of power lines and signal lines – separate metal cabinets for power electronics and low power electronics – distance > 20 cm between power components and sensitive components	
…	

Annex F
(informative)

Guidelines for software

F.1 General

Table F.1, Table F.2, Table F.3, Table F.4, Table F.5 and Table F.6 give an overview of necessary documents and basic activities.

NOTE Software can be designed according to IEC 62061 or ISO 13849-1.

Safety-related application software is running in a pre-designed platform (combination of hardware and software) according to IEC 61508, or other functional safety standards linked to IEC 61508 e.g. IEC 61131-6, where:

SW level 1 use limited variability language (LVL),

SW level 2 use of a language other than limited variability language (LVL).

F.2 Documentation

Table F.1, Table F.2, Table F.3, Table F.4, Table F.5 and Table F.6 summarize the relevant documents and information during the SW level 1 and SW level 2 design, implementation and integration.

Table F.1 – Documents for SW level 1 and SW level 2

Document	Comments
Coding guidelines	See Table F.2
Specification of the safety functions	See Clause 5, B.3 and Table B.2
Specification of the hardware design (see [a]) – Plant sketch(s) – Control system design – Wiring diagram(s) – I/O-list	See 4.4
Software design specification (see [b]) – Safety-related software specification and validation plan – Software system and module design specification – Architecture of safety-related program – Architecture of non-safety-related program – Module architecture of safety-related program – Program sketch (logical representation)	See overview of basic activities for SW level 1, Table F.3 and SW level 2, Table F.4 SW level 1 and SW level 2 SW level 2
Protocols – Software verification – Code review – Software validation	See Table F.3

[a] Hardware printout generated by CAD tools can be used.

[b] Software printout generated by pre-designed software-platform can be used.

Table F.2 – Coding guidelines

A Variables
Prefixes of boolean variables: "b".
Prefixes of binary inputs: "I_b" (non-safety-related input), **"IS_b"** (safety-related input).
Prefixes of binary outputs: "Q_b" (non-safety-related output) or **"QS_b"** (safety-related input).
Prefixes of instances: Timers: "T_", positive edge detections: **"R_"**, Flip-Flops: **"FF_"**
Prefixes of instances: Instances of SF_GUARD: GUARD_<*guard name*>, SF_ESTOP: ESTOP_<*number*>, SF_FDBACK: CONTACTORS_<*contactors*>
Prefixes of global variables: "G_" (non-safety-related), **"GS_"** (safety).
Prefixes of temporary variables: "#"
Variable names: The variable name after the prefix should be self-explanatory, e.g. should contain the device name under consideration. For example GD1 for guard door 1.
Variable declaration: Initialize with the safest condition. Include a comment in each declaration.
B Signal processing
Software architecture: Partition the software data flow in a pre-processing layer (inputs), a switch off logic (logic) and a post-processing layer (outputs).
Realize the pre-processing layer in consecutive networks. The output of each network should somehow contribute to the switch off logic.
For each binary output: Realize the corresponding switch off logic and the post-processing layer in one network (if possible).
Assignment: Use outputs and variables in only one program statement.
Comments: Each network has a comment.
Cyclic processing: Run each part of the safety-related software unconditionally as part of each cycle.
Monitoring of two channel inputs: Monitor on two channel inputs (e.g. push buttons) by the input cards with a discrepancy time of e.g. 100 ms.
Monitoring of contactors: Monitor of the mirror contacts of contactors with a feedback time of e.g. 1 s.
Monitoring of guard door: Monitor of the interlocking devices with a discrepancy time of e.g. 100 ms to 500 ms.
Automatic restart: Is only allowed for guard doors where the operator cannot stay in the hazard zone.
Errors in peripheral devices: Manual reset is necessary.
Triggering of safety functions: Trigger by FALSE.
Concept of acknowledge of detected failures: Selectivity of "reset/acknowledge" depending on the availability concept; human actions requirements
Response time (typical): Calculate or test and document the response time of the safety-related program.
C Library function blocks / functions (FBs/FCs)
Usage: Wherever applicable use pre-designed library FBs/FCs.
Guard door: SF_GUARD.
Emergency stop device: SF_ESTOP.
Contactor: SF_FDBACK.
Enabling device: SF_EV2DI
Automatic reset: Depending on the library functions (to be cited here)
Activation: Depending on the library functions (to be cited here)
Self-developed FBs/FCs: If applicable, capsule logical signal combinations which have multiple assignments within the project in a FB/FC. The life cycle complies with the V-model. These FBs/FCs will be password protected. A library management is necessary.

Table F.3 – Overview of protocols

Activities	Reference	Correct (y/n)
Verification of software system design specification		
1. Does the module architecture comply with the specification of the safety functions? 2. Does the software design specification comply with the specification of the safety functions?		
Software code review		
1. Does the software comply with the coding guidelines? 2. Does the control system design comply with the specification? 3. Is the interconnection of the I/O-signals in the software correct? Is the parameterization of the relevant FBs correct? 4. Does the hierarchy of the plc-safety program comply with the specification? 5. Does the architecture of safety-plc-program comply with the specification? 6. Does the plc-safety-program comply with the table specification? 7. Does the safety-related software specification comply with the specification of the safety functions?		
Software validation – to be checked		
1. Was the I/O-test carried out with a positive result? 2. Was the test of the safety functions and other test requirements carried out with a positive result? 3. Were all manufacturer specific tests of the parameterization of external safety devices (e.g. laser scanners, converters, etc.) carried out positively and documented?		
Software validation – necessary documentation		
4. Documents of the V-model 5. Final document of the safety relevant software including signatures 6. Final document of the control system hardware configuration with checksums and all adjustments 7. Archiving of the handbooks of all safety relevant system components 8. Final document of the configuration of all safety relevant peripheral devices 9. The relevant C standards		

Date:
Name:
Software signature:
Hardware signature:

F.3 Activities

The main difference between SW level 2 and SW level 1 is the higher degree of flexibility in programming due to higher freedom and complexity of the used program language.

Therefore, the following additional activities are necessary:

– software system design and

– module design.

Table F.4 – SW level 1 – Overview of basic activities

Requirements (input)	Result (output)
Developing of software safety requirements	
Specification of the safety function(s)	Input for **Software design specification**
Architecture of the SCS or SRP/CS	
Response time	
Operator interfaces and controls	
Relevant modes of operation of the machine	
Diagnostics (e.g. characteristics of sensors, final actuators)	
Coding guidelines	
Developing of software design specification	
Software design specification	Input for **Coding**
For each subsystem	
SIL and test cases	
For module design apply the same requirements based on (see 8.3.3) module description, interface, libraries used and specific coding rules	Logic
	Test cases fault insertion or injection(s)
	Diagnostic functions with fault reaction
	Achieving or maintaining a safe state
	Periodic testing or functional tests
	Preventing unauthorized modification
	Response time
	SW architecture; global data; libraries; pre-existing software modules; test cases and procedures
Coding	
Software design specification	To be tested **Program code**
Coding rules	
Coding guidelines	
For module coding apply the same requirements	Source code listing (e.g. ladder, function blocks, models)
	Structure as logical flow
	Code review report
	Sufficient comments
	Same names for parameters
	Names represent the function
	Predefined state
	Limited use of set/reset
	Outputs assigned once only

Table F.4 – SW level 1 – Overview of basic activities (continued)

Requirements (input)	Result (output)
Software testing	
Software design specification	Tested
Check of functionality	
Coding rules and guidelines	**Program code** (verification by tests)
For module testing apply the same requirements (see 8.3.3)	Test guidelines:
	Types of tests; test equipment; software versioning; corrective actions on failed test
	The manufacturer’s specification
	Functional testing
	Failure simulation
	Documentation

Table F.5 – SW level 2 – Overview of basic activities (1/2)

Requirements (input)	Result (output)
Developing of software safety requirements	
Specification of the safety function(s) Architecture of the SCS or SRP/CS Response time Operator interfaces and controls Relevant modes of operation of the machine Diagnostics (e.g. characteristics of sensors, final actuators) Coding guidelines	Input for **Software design specification**
Developing of software design specification	
Structured, reviewable, testable, understandable, maintainable and operable For each subsystem SIL and test cases	Input for **Software system design**
	Logic Test case fault insertion or injection(s) Diagnostic functions with fault reaction Achieving or maintaining a safe state Periodic testing or functional tests Preventing unauthorized modification Response time SW architecture; global data; libraries; pre-existing software modules; test cases and procedures

Table F.5 – SW level 2 – Overview of basic activities (1/2) (continued)

Requirements (input)	Result (output)
Developing of module design specification	
Software design specification Coding rules Coding guidelines	Input for **Module design specification**
	Description of the logic (i.e. the functionality) of each module Fully defined input and output interfaces of each module Format and value ranges of input and output data and their relation to modules Test cases which will include normal and outside normal operation Documentation of the interrupts
Module design	
Module design specification Module description Module interface Module libraries used Special coding rules	Input for **Module design**
Development of module(s)	Description of the logic (i.e. the functionality) of each module Fully defined input and output interfaces of each module Format and value ranges of input and output data and their relation to modules
	Test cases which will include normal and outside normal operation Documentation of the interrupts

Table F.6 – SW level 2 – Overview of basic activities (2/2)

Requirements (Input)	Result (Output)
Coding	
Software design specification Coding rules Coding guidelines	To be tested **Program code**
For module design apply the same requirements	Source code listing (e.g. ladder, function blocks, models) Structure as logical flow Code review report Sufficient comments Same names for parameters Names represent the function Predefined state Limited use of set/reset Outputs assigned once only
Module testing	
Module design specification Test cases Coding guidelines	Tested Module and integration testing (verification by tests)
	Documentation of test cases: Functional tests Black-Box, Grey-Box or White-Box testing Documentation of corrective actions: Integration test cases: software modules and software elements/subsystems interact correctly Program analysis
Software testing	
Software design specification Test cases Coding guidelines	Tested Program code (verification by tests)
	Test guidelines: Types of tests; test equipment; software versioning; corrective actions on failed test The manufacturer’s specification Functional testing Failure simulation Documentation

Annex G
(informative)

Examples of safety functions

G.1 General

Annex G of IEC 62061:2021 gives generic examples of typical safety functions.

The definition of the safety function differs from that of ISO 12100 because this document addresses risk reduction performed by an SCS or SRP/CS.

NOTE Safety functions are designed according to IEC 62061 or ISO 13849-1.

Based on additional information in Clause 4 and Clause 5 of this document specific safety functions are listed in this Annex G.

G.2 Safety functions

G.2.1 Basic information

Table G.1 gives a non-exhaustive list of examples of safety functions according to ISO 12100. Some basic information is necessary to describe an implemented safety function.

Table G.1 – Examples of safety functions and associated safety-related devices

Safety functions to protect persons
Interlocking guard
Interlocking guard with guard locking
Interlocking guard with a start function (with manual reset function)
Sensitive protective equipment (SPE), muting
Pressure-sensitive protective devices
Device with reset (push button)
Hold-to-run control device
Two-hand control device
Enabling device
Other safety functions
Selecting of local control
Manual parameter selection device (and procedure)
Manual operating mode selection device (and procedure)
Emergency stop device
Energy control device (and procedure)
Safety functions for the protection of integrity of the machine
Limited operation – Other protective devices
Operation to remain within specified limits – Other protective devices

G.2.2 Detailed description of safety requirements

The development of a separate risk assessment is not necessary if the requirements for the safety function are already described in the corresponding type-C standard.

If there are no defined requirements, the safety function will be determined according to the specifications required by IEC 62061 or ISO 13849-1.

The safety requirements specification defines all requirements for the safety function with regard to the safety of people and the environment. It is derived from the risk assessment.

Table G.2 gives an overview of basic information related to the safety requirements specification.

Table G.2 – Basic information related to the safety requirements specification

Basic information of safety functions
Name of the SF
Summary description of functions
Triggering event
Safety-related reaction
Operating mode
Required safety integrity, PL_r / SIL
Frequency of request (request rate)
Overrun
Behaviour in the event of power failure
Priorities for combined request of individual
Supplementary safety function
Additional parameters
Fault detection measures
Fault reaction measures (function)
Intended use
Safe state
Criteria achieving the safe state of the machine
Limit values and triggering criteria of the safety function
Acknowledgement and restart after detected faults
Possibilities for bypassing the safety function
Requirements for the sensors
Requirements for the actuators
Logic requirements
Reaction time(s)
Intervention by the operator
Interfaces to non-safety-related functions

The following topics can be important:

- International Standards considered are:
  - IEC 60204-1 Electrical safety
  - ISO 14119 Interlocking guards
  - IEC 61496 Electro-sensitive protective equipment
  - ISO 13850 Emergency stop functions
  - ISO 13851 Two-hand control devices — Functional aspects and design principles
  - ISO 13857 Safety distances to prevent hazard zones being reached by upper and lower limbs
  - ISO 14118 Prevention of unexpected start-up
  - other
  - …

- The functional description of the safety function is:
  - "When the guard door is opened then the motor will stop immediately".
  - …

- Systematic integrity measures applying safety principles are:
  - Basic safety principles ✓: …
  - Well-tried safety principles ✓: …
  - Well-tried components ✓: …
  - …

- Systematic integrity suing other additional measures are:
  - Avoiding ✓: Selection of components
✓: …
  - Controlling ✓: Voltage
✓: EMC, EMI
✓: …
  - …

- Other additional requirements are:
  - Restart When the hazard zone is accessible then no automatic restart is allowed
  - Unexpected restart As long as the interlocking guard is opened
  - other
  - …

G.2.3 Example of interlocking guard

Safety-related parameters for a safety function with the required SIL 1 are shown in Table G.3 for example.

Table G.3 – Example of safety-related parameters for a safety function with required SIL 1

Input			Logic	Output		
Architecture constraints, max. SIL 1				**Architecture constraints, max SIL 1**		
	HFT =	0			HFT =	0
	Category =	1			Category =	1
	DC =	0			DC =	0
	Failure rates				Failure rates	
Position switch 1	B_{10D} [cycles] =	20 000 000		Contactor 1	B_{10D} [cycles] =	1 300 000
	C [1/h] =	1			C [1/h] =	1
	λ_D [1/h] =	5,0 E-09			λ_D [1/h] =	7,7 E-08
high	$MTTF_D$ [a] =	22 831		high	$MTTF_D$ [a] =	1 484
—	T_{10D} [a] =	2 283			T_{10D} [a] =	148
	SFF =	0			SFF =	0
PFH (< SIL 3)				**PFH (< SIL 3)**		
Basic subsystem architecture A				Basic subsystem architecture A		
	PFH =	5,0 E-09			PFH =	7,7 E-08
Achieved SIL 1				**Achieved SIL 1**		

Safety-related parameters for a safety function with the required SIL 3 are shown in Table G.4 for example.

Table G.4 – Example of safety-related parameters for a safety function with required SIL 3

Input			Logic	Output		
Architecture constraints, max. SIL 3				**Architecture constraints, max SIL 3**		
	HFT =	1			HFT =	1
	Category =	3			Category =	4
	DC =	0,90			DC =	0,99
	Failure rates				Failure rates	
Position switch 1 (with separate actuator)	B_{10D1} [cycles] =	2 000 000		Contactor 1	B_{10D1} [cycles] =	1 300 000
Position switch 2 (with separate actuator)	B_{10D2} [cycles] =	2 000 000		Contactor 2	B_{10D2} [cycles] =	1 300 000
	C [1/h] =	1			C [1/h] =	1
	λ_{D1} [1/h] =	5,0 E-08			λ_{D1} [1/h] =	7,7 E-08
	λ_{D2} [1/h] =	5,0 E-08			λ_{D2} [1/h] =	7,7 E-08
high	$MTTF_{D1}$ [a] =	2 283			$MTTF_{D1}$ [a] =	1 484
high	$MTTF_{D2}$ [a] =	2 283			$MTTF_{D2}$ [a] =	1 484
—	T_{10D1} [a] =	228			T_{10D1} [a] =	148
—	T_{10D2} [a] =	228			T_{10D2} [a] =	148
	SFF =	90 %			SFF =	99 %
PFH (< SIL 3)				**PFH (< SIL 3)**		
Basic subsystem architecture D				Basic subsystem architecture D		
	PFH =	1,0 E-09			PFH =	1,6 E-09
Achieved SIL 3				**Achieved SIL 3**		

Annex H
(informative)

Evaluation of PFH value of a subsystem

H.1 General

Approaches of evaluation of a PFH value of a subsystem are showed in this Annex H.

NOTE Evaluation of a PFH value of a subsystem is based on IEC 62061 or ISO 13849-1.

H.2 Table allocation approach (IEC 62061)

The following simplification can be applied for subsystems based on elements following Weibull distribution:

– $\lambda_D \approx 0{,}1 \frac{C}{B_{10D}}\left[\frac{1}{\text{h}}\right]$ or $\text{MTTF}_\text{D} = \frac{1}{8\,760\,\lambda_\text{D}}$ $[\text{years}]$

– $T_1 = T_{10D} \approx 0{,}1 \frac{1}{\lambda_\text{D}}[\text{h}]$ or $T_1 = 0{,}1 \frac{1}{8\,760\,\lambda_\text{D}} = 0{,}1\ \text{MTTF}_\text{D}\ [\text{years}]$

PFH values can be evaluated by using Table H.1 and Table H.2 of IEC 62061:2021 with the following restriction:

– T_1 is equal to 20 years;

– for dual channel subsystems (HFT = 1) the MTTF_D of each channel is equal;

– if the MTTF_D per channel is different, either the lowest MTTF_D of each channel of both channels can be used as a worst case approach, or the geometric average of MTTF_D of each channel of both channels $\text{MTTF}_\text{D} = \sqrt{\text{MTTF}_{\text{D1}}\ \text{MTTF}_{\text{D2}}}$.

H.3 Simplified formulas for the estimation of PFH value (IEC 62061)

In IEC 62061:2021, Clause H.2, a simplified approach is described for the estimation of PFH for a number of basic subsystem architectures and formulas that can be used for subsystems.

Further approaches are described in this document, in Clause H.4.

H.4 Approaches of IEC 61508, IEC 62061 and ISO 13849-1

H.4.1 General

The evaluation of PFH formulas can be performed by different approaches with respective boundary conditions. In this Clause H.4 the different approaches will be described.

A number of reliability techniques are more or less straightforwardly usable for the analysis of the unreliability of safety-related subsystems, among which are reliability block diagrams and Markov chains. IEC 62061 has traditionally used reliability block diagrams and it assumes subsystems as being non-repairable (except for the formulas in IEC 62061:2021, Clause H.4), while ISO 13849-1 has always used Markov modelling and it assumes subsystems as being repairable.

In the context of IEC 62061 the basic approach and the importance of T_{10} will be elaborated in Clause H.6. Clause H.7 gives an overview of PFH formulas derived in this Annex H.

H.4.2 Approach of IEC 61508

H.4.2.1 General

Reliability techniques are sorted according to the two following points of view:

– Static (Boolean) versus dynamic (states/transitions) models;

– Analytical versus Monte Carlo simulation calculations.

Boolean models encompass all models describing the static logical links between the elementary failures and the whole system failure. Reliability block diagrams (RBD) and fault trees (FT) belong to Boolean models.

States/transitions models encompass all models describing how the system behaves (jumps from state to state) according to arising events (failures, repairs, tests, etc.). Markovian, Petri nets and formal language models belong to states/transitions models.

NOTE For further information see Annex B of IEC 61508-6:2010.

The simplified approach first is based on RBD graphical representations.

When an E/E/PE safety-related system is used in continuous or high demand mode of operation, IEC 61508-6:2010 requires the calculation of its PFH. This is the average of the so-called unconditional failure intensity (also called failure frequency) $w(t)$ over the period of interest:

$$\mathrm{PFH}(T) = \frac{1}{T}\int_0^T w(t)\,dt$$

H.4.2.2 Boundary conditions of IEC 61508

The use of a reliability block diagram (RBD) approach assumes a constant failure rate. The calculations are based on the following assumptions:

– the resulting average probability of failure on demand for the system is less than 10^{-1}, or the resultant average frequency of dangerous failure for the system is less than 10^{-5} h^{-1};

– component failure rates are constant over the life of the system;

– the overall hardware failure rate of a channel of the subsystem is the sum of the dangerous failure rate and safe failure rate for that channel, which are assumed to be equal;

– the proof test interval is at least an order of magnitude greater than the MRT;

– for each subsystem there is a single proof test interval and MRT;

– the expected interval between demands is at least an order of magnitude greater than the proof test interval;

– for all subsystems operating in high demand or continuous mode of operation, the fraction of failures specified by the diagnostic coverage is both detected and repaired within the MTTR (mean time to restoration, typically assumed to be 8 h) used to determine hardware safety integrity requirements;

– for 1oo1 and 2oo2 voted groups operating in high demand or continuous mode of operation, the E/E/PE safety-related system always achieves a safe state after detecting a dangerous fault; to achieve this, the expected interval between demands is at least an order of magnitude greater than the diagnostic test intervals, or the sum of the diagnostic test intervals and the time to achieve a safe state is less than the process safety time;

– where the term "channel" is used, it is limited to only that part of the system under discussion, which is usually either the sensor, logic or final element subsystem.

H.4.3 Approach of IEC 62061

H.4.3.1 General

The simplified approach is based on RBD graphical representations where four basic architectures are used.

The PFH value of the safety function is given by the sum of the PFH values of all subsystems involved in performing the safety function.

H.4.3.2 Boundary conditions of IEC 62061

The simplified formulas used for the evaluation of PFH value are based on the following assumptions:

– modelling technique based on reliability block diagram (RBD);
– exponential failure model (component failure rates are constant over the component lifetime);
– systems are non-repairable;
– the unavailability $P(t) = 1 - e^{-\lambda t}$;
– failure density is $P'(t)$;
– the term (λ t) is assumed to be ≤ 0,1 to allow $P'(t) \approx \lambda$;
– supported range from 1 % to 10 % for the common cause factor β;
– regarding the lifetime of components that are subjected to ageing and wear, the failure mechanism is limited to T_{10D};
– the overall hardware failure rate of a channel of the subsystem is the sum of the dangerous failure rate and safe failure rate for that channel;
– for 1oo1 and 2oo2 voted groups operating in high demand or in continuous mode of operation, the SCS always achieves a safe state after detecting a dangerous fault; to achieve this, the expected interval between demands is at least an order of magnitude greater than the diagnostic test intervals, or the sum of the diagnostic test intervals and the time to achieve a safe state is less than the process safety time;
– where the term "channel" is used, it is limited to only that part of the system under discussion, which is usually either the sensor, logic or final element subsystem.

H.4.4 Approach of ISO 13849-1:2015, Annex K

H.4.4.1 General

Comparable with the SIL, ISO 13849-1 employs the performance level (PL) to express the safety-related capability of safety functions. "PL a" to "PL e" denote the level of performance in ascending order. As with SIL, each PL requires the PFH (in ISO 13849-1, PFH is called PFH_D) not to exceed a PL-specific quantitative limit.

ISO 13849-1 allows any calculation method for PFH that adequately takes account of the features listed in ISO 13849-1:2015, 4.5.1, i.e., failure rates, diagnostics, susceptibility to common cause failures and system architecture.

Nevertheless, 4.5.4 of ISO 13849-1:2015 provides a simplified procedure for estimating the quantifiable aspects of PL, i.e. for estimating the PFH. ISO 13849-1:2015, Annex K, consists of Table K.1 only. Within the frame of the simplified procedure and in connection with other annexes of ISO 13849-1:2015, Table K.1 is used to read out the PFH of a subsystem executing a safety function or a part of it.

For implementations of safety functions or subsystems implementing a part of a safety function, ISO 13849-1 defines five categories (B and 1 to 4) primarily by specifying the behaviour of the (sub)system in the presence of faults. Since this behaviour mainly depends on the architecture of the system, ISO 13849-1 suggests a so-called designated architecture for each category. Although the designated architectures are not mandatory for a specific category, they serve as a basis for the determination of the PFH.

The five designated architectures can be attributed to three basic architectures:

– category B and category 1: single-channel, untested (1oo1)
– category 2: single-channel with separate test equipment (1oo1D)
– category 3 and category 4: dual-channel, channels mutually tested (1oo2D).

NOTE 1 Despite category 4 requiring a fault tolerance of at least two, a conservative estimation of PFH is made on a basis of the dual-channel architecture in conjunction with a high diagnostic coverage of 99 %.

ISO 13849-1 allows for high demand of the safety function only, i.e., it premises at least one demand per year.

For this reason, the PFH may be equated with the hazard rate.

The technique applied by the simplified procedure to determine the PFH (in fact: the hazard rate) for the designated architectures assumes the presence of high demand up to continuous demand for the categories B, 1, 3 and 4.

The reason for this is that within this range of the demand rate the related designated architectures do not show a significant dependence of the PFH on the actual demand rate. By contrast, the designated architecture for category 2 exhibits such a dependence.

To cope with this characteristic, the simplified procedure assumes the desirable and beneficial case that any detectable failure of the only functional channel will always be detected in due time before a demand arises, or, at least that the test rate is much greater than the demand rate.

Furthermore, the simplified procedure assumes restoration of defective systems and new start-up within a negligible period of time, once the failure has been detected by diagnostics or has been revealed by an accident, in the latter case contributing to PFH.

Typical operation of subsystems applying the designated architectures in the field of machinery results in a very low influence of the restoration time on the PFH, and neglecting the restoration time implies an estimate on the safe side with respect to PFH.

ISO 13849-1:2015, Table K.1 provides pre-calculated PFH values for the five categories defined in ISO 13849-1. These values have been obtained by applying Markov modelling to the designated architectures. At this point, the possible combinations of functional block failures or channel failures constitute different system states. Failures, tests, demand of the safety function and repair lead on to transitions between the system states, thus forming a state transition model.

As restoration after an accident is also considered, there are no absorbing states, i.e., states without outlet. Some of the system states are dangerous, which means that the safety function cannot be executed. All of the state transition rates are assumed to be constant in time or are approximated as constant in time. Because of this, the state transition models become Markov models, which allow for an easy numerical evaluation of the temporal progress of the state probabilities and of the fluxes between the states. All fluxes outgoing from dangerous system states and due to demand of the safety function are taken as contributions to the PFH. The temporal average of their sum yields the PFH.

One of the input parameters used for numerical evaluation is the failure rate of a channel to the dangerous side.

Because of the presupposition of failure rates to be constant in time, the mean time to dangerous failure, $MTTF_D$, is given simply by the reciprocal of the dangerous failure rate λ_D. In order to deal with a convenient measure, ISO 13849-1 has chosen to use $MTTF_D$ in years instead of the dangerous failure rate. Thus, $MTTF_D$ is just to be interpreted as a synonym of $1/\lambda_D$ and is not be confused with a guaranteed lifetime.

The second essential input parameter is the mean diagnostic coverage of a functional channel, DC_{avg}, expressed as a percentage.

ISO 13849-1 requires architectures implying redundancy to limit common cause failures by design. A simple scoring procedure is used to provide evidence that sufficient effort has been taken in order to limit the common cause factor β to a maximum value of 2 % (ISO 13849-1:2015, Annex F). The simplified procedure of ISO 13849-1 assumes that this requirement is met. The simplified procedure of ISO 13849-1 is designed so as to deliver results with little expenditure of modelling, ideally without complex calculation. Therefore, the knowledge of the category, of the $MTTF_D$ of the functional channel(s) and of DC_{avg} is sufficient to read a PFH result for a (sub)system from ISO 13849-1:2015, Table K.1. The bar graph of ISO 13849-1:2015, Figure 5, presents a quick overview of the numerical content of Table K.1.

NOTE 2 ISO 13849-1:2015, Figure 5 does not cover PFH values for category 4 with $MTTF_D$ > 100 years while ISO 13849-1:2015, Table K.1 includes $MTTF_D$ values up to 2 500 years for category 4.

If a functional channel comprises several functional blocks or components, its $MTTF_D$ will be calculated from the block or component $MTTF_D$ values prior to using Table K.1. For this, Annex D of this document provides a simple Equation (D.1).

In the case of category 3 or 4 employing channels with unequal $MTTF_D$ an average $MTTF_D$ has to be used for ISO 13849-1:2015, Table K.1. This is calculated by equation (D.2) of Annex D of this document.

Accordingly, prior to applying ISO 13849-1:2015, Table K.1, a series of functional blocks or components with different DC values will be assigned a mean DC value, DC_{avg}. This value is obtained from equation (E.1) of Annex E of ISO 13849-1:2015. The same equation may be used in the case of category 3 or 4 if the DC values of the two channels are different.

H.4.4.2 Boundary conditions of ISO 13849-1:2015, Annex K

The simplified procedure of ISO 13849-1 supports designated architectures only.

If deviating architectures can be decomposed into a series arrangement of subsystems, each representing a designated architecture, the procedure may be applied to each subsystem individually. Then the PFH of the safety function is given by the sum of the PFH values of all subsystems involved in performing the safety function.

The simplified procedure of ISO 13849-1 may also be used if a different architecture can be mapped to one of the designated architectures with the help of simplifications on the safe side, i.e. by neglecting redundancy.

Like most quantification methods, the simplified procedure assumes failure rates that are constant over time. Therefore, the use of parts subject to wear requires limitation of the operational time to the T_{10D} value given by Equation (C.3).

Making use of the simplified procedure of ISO 13849-1 implies that a PFH value always has to be read from ISO 13849-1:2015, Table K.1, i.e. one single table of limited size. Therefore, concerning the input parameters, some boundaries are introduced.

The mission time of the safety system is fixed to 20 years.

The common cause factor β is fixed to 2 %, which means that a β of more than 2 % is not supported. In the event of β being smaller than 2 %, the procedure yields an estimate on the safe side.

In the case of the tested single-channel architecture of category 2 (1oo1D) only time-optimal testing is supported. This means that any detectable failure of the only functional channel always has to be detected in due time, or, at least, that the test rate has to be much greater than the demand rate.

Additionally, there are some numerical limitations of the simplified procedure in ISO 13849-1:2015, Table K.1. These limitations are due to the specifications of the categories of ISO 13849-1:2015, 6.2 and they are concerning the range of $MTTF_D$ and the values of DC_{avg} that are covered, or not covered, by ISO 13849-1:2015, Table K.1.

In the case of category B, ISO 13849-1:2015, Table K.1 covers $MTTF_D$ values from 3 years to < 30 years. For category 1, $MTTF_D$ ranges from 30 years to 100 years, whereas for category 2 or 3 a range of 3 years to 100 years is covered. In the case of category 4, ISO 13849-1:2015, Table K.1 lists PFH values for an $MTTF_D$ ranging from 30 years to 2 500 years.

Regarding $MTTF_D$, all table entries are staggered according to the logarithmic E24 series resulting in 24 values per decade. Often the original $MTTF_D$ value does not exactly fit in with a table entry so that the next lower entry has to be chosen.

NOTE 1 The category-specific limitations of the $MTTF_D$ range in ISO 13849-1:2015, Table K.1 reflect one of the approaches in ISO 13849-1:2015 to prevent systems without redundancy or without sound diagnostics from reaching high performance levels solely because of their low failure rate or, respectively, because of their high $MTTF_D$. This is accomplished by a capping of $MTTF_D$ if it exceeds certain limits, thus deteriorating the PFH value determined.

A stronger limitation of ISO 13849-1:2015, Table K.1 consists in providing PFH values only for one or two values of the mean diagnostic coverage, depending on the category.

For category 2 or 3 ISO 13849-1:2015, Table K.1 supports a DC_{avg} of 60 % and of 90 %. For category 4 only, a DC_{avg} of 99 % is supported since ISO 13849-1 does not permit a lower diagnostic coverage in this category. In practice, with no additional resource at hand, in the case of category 2 or 3, a DC_{avg} between 60 % and 90 % has to be capped to 60 % and a DC_{avg} beyond 90 % has to be capped to 90 %. Vigorous capping will of course result in a significant increased PFH value, i.e., a conservative estimate.

NOTE 2 Again, capping of DC_{avg} to 90 % at category 2 or 3 is part of the approach of ISO 13849-1 to limit the attainable performance level. As a side effect, this results in a more conservative PFH value. A free available software implementation of the simplified procedure of ISO 13849-1 uses interpolation to avoid DC_{avg} capping between 60 % and 90 % hence allowing for the determination of more accurate PFH values.

H.5 Basic considerations regarding exponential and Weibull distributions

H.5.1 Exponential distribution

The unavailability (unreliability) of an element with a constant failure rate of λ can be expressed as a cumulative distribution function (CDF) based on the exponential distribution by the following term

$$P(t) = 1 - e^{-\lambda t} \tag{H.1}$$

where

t represents time.

If (λ t) << 1 then a simplified approach to evaluate $P(t)$ can be assumed by

$$P(t) \approx \lambda t \tag{H.2}$$

The assumption $e^{-\lambda t} \approx 1 - \lambda\, t$ is based on the real exponential function commonly defined by the following power series

$$e^{x} = \sum_{n=0}^{\infty} \frac{x^{n}}{n!} = 1 + x + \frac{x^{2}}{2} + \frac{x^{3}}{6} + \frac{x^{4}}{24} + \ldots .$$

NOTE $P(t)$ can be written as $P(t) \approx -x - \frac{x^{2}}{2} + \frac{x^{3}}{6} + \frac{x^{4}}{24} - \ldots$ where $x = -\lambda\, t$.

Within an accuracy of 1 %, $\frac{x^{2}}{2} + \frac{x^{3}}{6} + \frac{x^{4}}{24} + \ldots \leq \frac{-x}{100}$ leads to $-x \leq \frac{1}{50}; -x \leq \frac{1}{10}$ applies respectively within an accuracy of ≤ 5 % and $-x \leq \frac{1}{5}$ within an accuracy of ≤ 10 %.

In good engineering practice an accuracy of 5 % is acceptable and $(\lambda t) \ll 1$ can be written as $(\lambda t) \leq \frac{1}{10}$.

Based on Formula (H.1) the probability density function $P'(t)$ can be written as

$$P'(t) = \frac{\mathrm{d}}{\mathrm{d}t} P(t) = \lambda \ e^{-\lambda t} \tag{H.3}$$

where

t represents the time;

λ is the constant failure rate.

H.5.2 Weibull distribution

Non-electronic components are typically characterized by Weibull distribution.

According to IEC 61649 the Weibull cumulative distribution function $F(t)$ (as unavailability of an element) is defined as

$$F(t) = 1 - e^{-\left(\frac{t}{\eta}\right)^{\beta}} \tag{H.4}$$

where

t represents the time;

η represents the characteristic life or scale parameter;

β represents the shape parameter.

Three ranges of values of the shape parameter β are salient:

– For $\beta = 1$, the Weibull distribution is identical to the exponential distribution;

– $\beta > 1$ is the case of increasing instantaneous failure rate; and

– $\beta < 1$ is the case of decreasing instantaneous failure rate.

$F(t) = P(t)$ when $\eta = \frac{1}{\lambda}$ and $\beta = 1$.

If $\left(\frac{t}{n}\right)^{\beta} \ll 1$ then a simplified approach to evaluate $F(t)$ can be assumed by

$$F(t) \approx \left(\frac{t}{\eta}\right)^{\beta} \tag{H.5}$$

By assuming $n = \frac{1}{\lambda}$ Formula (H.5) can be written as

$$F(t) \approx (\lambda\, t)^{\beta} \tag{H.6}$$

According to IEC 61649 the Weibull probability density function is defined as

$$f(t) = \frac{d}{dt} F(t) \approx \beta \, \frac{t^{\beta-1}}{\eta^{\beta}} e^{-(\frac{t}{\eta})^{\beta}} \tag{H.7}$$

where

t represents the time;

η represents the characteristic life or scale parameter;

β represents the shape parameter.

The instantaneous failure rate $\lambda(t)$ is defined by

$$\lambda(t) = \beta \frac{t^{\beta-1}}{\eta^{\beta}} \quad \text{(H.8)}$$

H.6 T_{10} and B_{10}

H.6.1 General

For electromechanical control switches and for pneumatic valves that are characterised by two states (open or closed), failures are mainly due to the length of time they have been in use (which depends on the number of cycles). For these components the nominal lifetime is usually measured in B_{10} cycles (number of cycles until 10 % of components have failed in a life test).

The value $B_{10\text{D}}$ is the number of cycles until 10 % of components fail dangerously can be evaluated with $B_{10\text{D}} = \frac{B_{10}}{\text{RDF}}$ where RDF is the ratio of dangerous failures (comparable to $\text{MTTF}_D = \frac{\text{MTTF}}{\text{RDF}}$).

If the RDF is not known or not available, $B_{10\text{D}}$ can be determined as $B_{10\text{D}}$ = 2 × B_{10}. The $B_{10\text{D}}$ information is converted as a function of time with the relationship: $T_{10\text{D}} = \frac{B_{10\text{D}}}{n_{\text{op}}}$

The conversion factor being the average number of actuations per year (n_{op}).

$T_{10\text{D}}$ stands for the elapsed time at which 10 % of the components tested have failed dangerously.

Owing to the practical test procedure (e.g. by component manufacturer), RDF can only be evaluated at T_{10}. For the considered time T_{10} no practical values of RDF exist because the test procedures end at T_{10}. The limitation should be T_{10} and not $T_{10\text{D}}$. Owing to the provisions of ISO 13849-1, $T_{10\text{D}}$ has been established and Formula (H.12) represents a compromise by limiting $T_{10\text{D}}$ when the deviation between T_{10} and $T_{10\text{D}}$ becomes too high (i.e. RDF ≤ 50 %).

By assuming as a first approximation that failures follow an exponential distribution instead of a Weibull distribution, the evaluation of the reliability (MTTF) based on the life time T_{10} of such components can be computed based on the T_{10} lifetime.

H.6.2 T_{10} with exponential distribution

The unavailability at T_{10} of the exponential distribution is written as

$$P(T_{10}) = 1 - e^{-\lambda T_{10}} = 0{,}1 \quad \text{(H.9)}$$

and leads to, based on generic formula $y = e^{x}$ and $x = \ln y$

$$T_{10}\ \frac{-\ln(0{,}9)}{\lambda} \approx 0{,}1\frac{1}{\lambda} = 0{,}1\ \text{MTTF} \qquad \text{(H.10)}$$

With B_{10}, B_{10D} and n_{op}, the mean number of annual operations, the following relationship can be written as

$$T_{10} = \frac{B_{10}}{n_{op}} \approx 0{,}1\ \text{MTTF or } T_{10D} = \frac{B_{10D}}{n_{op}} = \frac{B_{10}}{\text{RDF}\ n_{op}} \approx 0{,}1\ \text{MTTF}_D \qquad \text{(H.11)}$$

Based on Formula (H.16) MTTF and MTTF_D for components can be calculated as

$$\text{MTTF} \approx \frac{B_{10}}{0{,}1 \times n_{op}}\ \text{ or }\ \text{MTTFD} \approx \frac{B_{10D}}{0{,}1 \times n_{op}} = \frac{B_{10}}{\text{RDF}\ 0{,}1 \times n_{op}}$$

If RDF ≤ 50 % than T_{10D} will be limited to

$$T_{10D} = \frac{B_{10}}{\text{RDF}\ n_{op}} = \frac{B_{10}}{0{,}5\ n_{op}} \approx 0{,}1\ \text{MTTF}_D \qquad \text{(H.12)}$$

By reaching T_{10} the Weibull cumulative distribution function is increasing dramatically and the ratio of dangerous failure (RDF) of the component will change. T_{10} represents therefore the maximum proof-test or the useful lifetime. Beyond T_{10} non-electronic components will be exchanged.

H.6.3 T_{10} with Weibull distribution

The unavailability at T_{10} of the Weibull distribution, for example with a shape parameter of 2 can be written as

$$F(T_{10}) = 1 - e^{-(\lambda_W T_{10})^2} \qquad \text{(H.13)}$$

and leads to

$$T_{10} = \frac{\sqrt{-\ln(0{,}9)}}{\lambda_W} \approx 0{,}325\ \frac{1}{\lambda} \qquad \text{(H.14)}$$

The relationship between the failure rates of this Weibull distribution and the exponential distribution based on Formula (H.10) and Formula (H.14) at T_{10} becomes:

$$T_{10} = \frac{\sqrt{-\ln(0{,}9)}}{\lambda} = \frac{\sqrt{-\ln(0{,}9)}}{\lambda_W} \qquad \text{(H.15)}$$

or $$\lambda_W = \frac{\lambda}{\sqrt{-\ln(0,9)}} = \frac{\lambda}{\sqrt{\ln(\frac{1}{0,9})}} = \ln\left(\frac{1}{0,9}\right)^{-\frac{1}{2}} \lambda \approx 3,08\ \lambda \qquad \text{(H.16)}$$

The following example shows the relevance of T_{10}:

– with B_{10} = 1 000 000 cycles and

– duty cycle of C = 1/h or n_{op} = 8 760 cycles per year

– MTTF becomes MTTF ≈ 1 141 years and T_{10} ≈ 114 years.

At the considered time T_1 = 20 years, the number of cycles is $8\,760\left[\frac{\text{cycles}}{a}\right]20[a]$ or 175 200 [cycles] which corresponds only to 17,52 % of the B_{10} value.

Figure H.1 shows the distribution functions and a factor of nearly 6 of difference between the availability of the distribution functions.

The exponential distribution will have a worst-case value of the unavailability compared to Weibull distribution.

When T_{10} > 20 years or T_{10} < T_1 the Weibull distribution and the exponential distribution will have significant differences. T_{10} is therefore an important limitation for evaluation of PFH values.

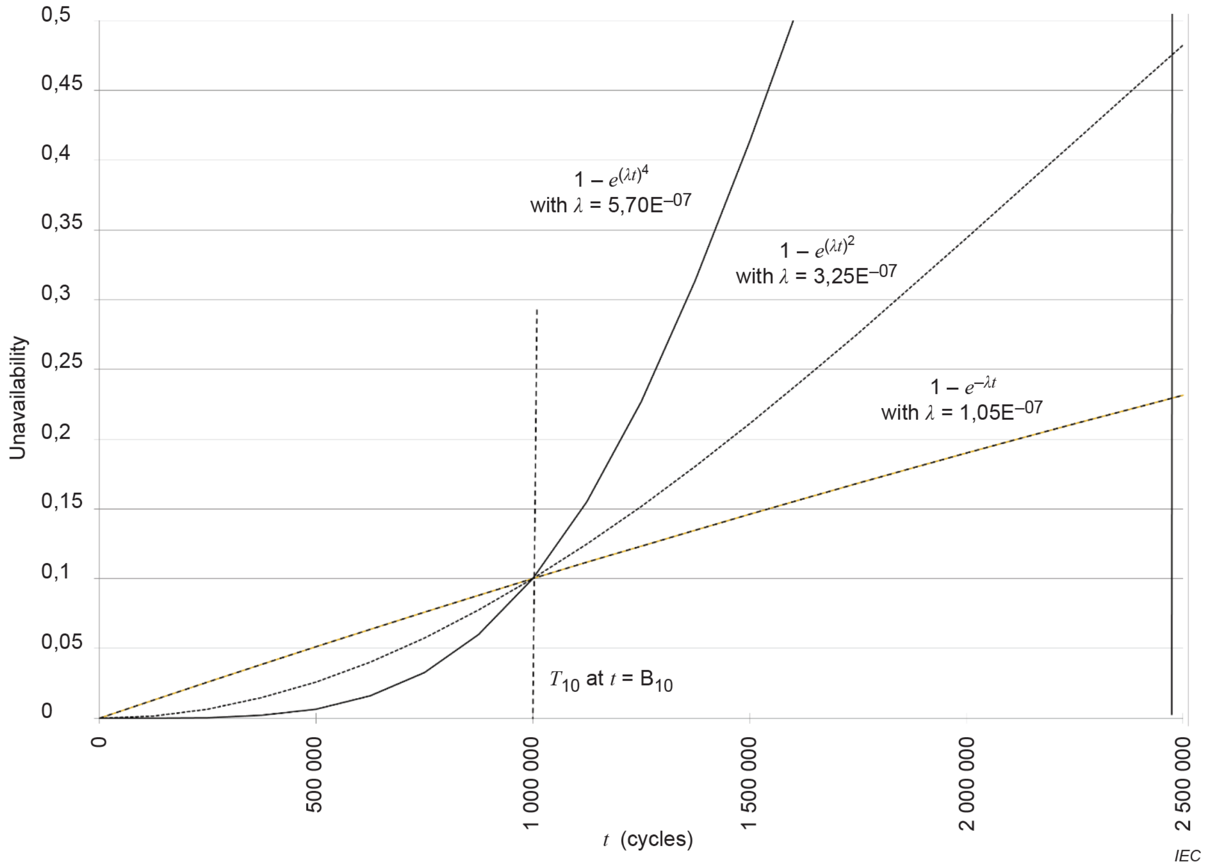


Figure H.1 – Cumulative distribution functions (CDF)

The value of λ can be considered to be constant under the assumption that the value for the considered time period *t* is:

– equal to the useful lifetime for electronic components, and

– equal to the smallest one of the useful lifetime or T_{10D} for non-electronic components.

H.7 Overview of PFH formulas

H.7.1 Definitions

The basic definition of PFH (average frequency of failure) over the period [0, *T*] is

$$\mathrm{PFH} = \frac{1}{T}\int_0^T \left(\frac{\mathrm{d}}{\mathrm{d}t} P(t)\right) \mathrm{d}t = \frac{1}{T}\int_0^T P'(t)\,\mathrm{d}t \qquad \text{(H.17)}$$

where

t represents the time;

$P'(t)$ represents the probability density function (PDF) for non-reparable subsystems.

T represents the mission time and will be less than or at most equal to the useful lifetime of a subsystem. The examples provided are based on a mission time equal to 20 years.

H.7.2 Formulas

The PFH formulas listed in Table H.1 to Table H.6 can be used. The detailed derivation of those formulas is developed in Clause H.8 to Clause H.12.

NOTE The formulas in Table H.1 to Table H.6 are based on reliability block diagram and are similar by using the Markov modelling of ISO 13849-1 and applying a simplified approach where ($\lambda\, t$) << 1, see H.5.1.

Table H.1 – Formulas for basic subsystem architecture A (1oo1)

PFH formula	Exponential distribution	Comments
λ_D	$\frac{1}{T}(1 - e^{-\lambda_D T})$	Generic formula
NOTE For non-electronic components, a worst-case $\lambda_D = \lambda_{DU} = 1\,000$ FIT with 1 FIT = 1E-09/h can be assumed where the expected demand rate is less than one time per year.		
Definition of terms: – λ_D, dangerous failure rate of the channel [1/h] – T, useful lifetime or mission time [h]		

Table H.2 – Formulas for basic subsystem architecture C (1oo1D)

PFH formulas	Comments
$(1 - DC)\,\lambda_D$	Generic formula (fault reaction performed by another subsystem)
$(1-DC)\,\lambda_D^{CC} + DC\,\lambda_D^{CC}\,\lambda_{react}^{CC}\,\frac{(T_1+T_2)}{2} + \lambda_{CC}$	Generic formula
$(1-\beta)(1-DC)\lambda_D + (1-\beta)^2\,DC\,\lambda_D^2\,\frac{(T_1+T_2)}{2} + \beta\,\lambda_D$	Worst case consideration in context of machinery, where $\lambda_{react} \le \lambda_D$ and β Min (λ_D, λ_{react}) = $\beta\,\lambda_D$
NOTE 1 For non-electronic components a worst-case $\lambda_D = \lambda_{DU} = 1\,000$ FIT with 1 FIT = 1E-09/h can be assumed where the expected demand rate is less than one time per year.	
Definition of terms: – β common cause factor (0,01; 0,02; 0,05 or 0,1) between main channel and fault reaction channel [%] – λ_D dangerous failure rate of main channel [1/h] – λ_{react} failure rate of fault reaction channel [1/h] – DC Diagnostic coverage (0; 0,6; 0,9 or 0,99) of the main channel [%] – $\lambda_{CC} = \beta$ Min(λ_D, λ_{react}) failure rate due to common cause failures [1/h] – $\lambda_D^{CC} = \lambda_D - \lambda_{CC}$ [1/h] – $\lambda_{react}^{CC} = \lambda_{react} - \lambda_{CC}$ [1/h] – T_1, useful lifetime [h] – T_2, diagnostic test interval [h] NOTE 2 Other functional safety standards are using for T_1 the mission time T_M.	

Table H.3 – Formulas for basic subsystem architecture B (1oo2)

PFH formulas	Comments
$\lambda_{D1}^{CC}\,\lambda_{D2}^{CC}\,T_1 + \lambda_{CC}$	Generic formula
$(1-\beta)^2\,\lambda_D{}^2\,T_1 + \beta\,\lambda_D$	Generic formula, where $\lambda_D = \lambda_{D1} = \lambda_{D2}$
NOTE 1 For non-electronic components a worst-case $\lambda_D = \lambda_{DU} = 1\,000$ FIT with 1 FIT = 1E-09/h can be assumed where the expected demand rate is less than one time per year.	
Definition of terms: – β common cause factor (0,01; 0,02; 0,05 or 0,1) between channel 1 and channel 2 [%] – λ_{D1}, dangerous failure rate of channel 1 [1/h] – λ_{D2}, dangerous failure rate of channel 2 [1/h] – DC_1, Diagnostic coverage (0; 0,6; 0,9 or 0,99) of the channel 1 [%] – DC_2, Diagnostic coverage (0; 0,6; 0,9 or 0,99) of the channel 2 [%] – $\lambda_{CC} = \beta$ Min(λ_{D1}, λ_{D2}), failure rate due to common cause failures [1/h] – $\lambda_{D1}^{CC} = \lambda_{D1} - \lambda_{CC}$ [1/h] – $\lambda_{D2}^{CC} = \lambda_{D2} - \lambda_{CC}$ [1/h] – T_1, useful lifetime [h] NOTE 2 Other functional safety standards are using for T_1 the mission time T_M.	

Table H.4 – Formulas for basic subsystem architecture D (1oo2D)

PFH formulas	Comments
$\lambda_{D1}^{CC}\ \lambda_{D2}^{CC}\left((1-DC_1)\frac{T_{1o1}}{2}+(1-DC_2)\frac{T_{1o2}}{2}\right)+\lambda_{D1}^{CC}\ \lambda_{D2}^{CC}\ (DC_1+DC_2)\frac{T_2}{2}+\lambda_{CC}$	Generic formula
$\lambda_{D1}^{CC}\ \lambda_{D2}^{CC}\ (2-DC_1-DC_2)\frac{T_1}{2}+\lambda_{D1}^{CC}\ \lambda_{D2}^{CC}(DC_1+DC_2)\frac{T_2}{2}+\lambda_{cc}$	Generic formula, where $T_1 = T_{1o1} = T_{1o2}$
$(1-\beta)^2\ \lambda_D{}^2\ \left((1-DC)\ T_1+DC\ T_2\right)+\beta\ \lambda_D$	Generic formula, where $\lambda_D = \lambda_{D1} = \lambda_{D2}$ DC = $DC_1 = DC_2$

NOTE 1 For non-electronic components a worst-case $\lambda_D = \lambda_{DU} = 1\,000$ FIT with 1 FIT = 1E-09/h can be assumed where the expected demand rate is less than 1 time per year.

Definition of terms:

- β, common cause factor (0,01; 0,02; 0,05 or 0,1) between channel 1 and channel 2 [%]
- λ_{D1}, dangerous failure rate of channel 1 [1/h]
- λ_{D2}, dangerous failure rate of channel 2 [1/h]
- DC_1, Diagnostic coverage (0; 0,6; 0,9 or 0,99) of the channel 1 [%]
- DC_2, Diagnostic coverage (0; 0,6; 0,9 or 0,99) of the channel 2 [%]
- $\lambda_{CC} = \beta$ Min(λ_{D1}, λ_{D2})
- $\lambda_{D1}^{CC} = \lambda_{D1} - \lambda_{CC}$
- $\lambda_{D2}^{CC} = \lambda_{D2} - \lambda_{CC}$
- T_1 useful lifetime [h]
- T_{1o1} useful lifetime [h] of channel 1
- T_{1o2} useful lifetime [h] of channel 2
- T_2 diagnostic test interval [h]

NOTE 2 Other functional safety standards are using for T_1 the mission time T_M.

H.7.3 Examples

In practice the PFH value based on B_{10D} and duty cycles is not limiting the reachable SIL:

- with a duty cycle of one time per hour or one time per day the PFH value ≪ max. PFH value of required SIL;
- architectural constraints are the limiting factor of reachable SIL.

When the duty cycle is higher than one time per hour T_{10D} becomes important.

Table H.5 shows the typical values using a worst case B_{10D} = 1 000 000 (e.g. contactor or position switch).

Table H.5 – Examples of PFH values based on B_{10D}

Single channel subsystem (HFT = 0)				DC = 0 %	DC = 60 %	DC = 90 %	
B_{10D}	**Cycles**	**λ_D**	**$MTTF_D$**	PFH = λ_D	PFH < λ_D 0,5	PFH < λ_D 0,2	
1 000 000	1 time per minute	6,00 E-06	19	6,00 E-06	2,65 E-06	9,69 E-07	SIL 1 < 1,00 E-05
	1 time per hour	1,00 E-07	1 142	1,00 E-07	4,17 E-08	1,26 E-08	SIL 3 < 1,00 E-07
	1 time per day	4,17 E-09	27 397	≪ 1,00 E-08			
	1 time per week	5,96 E-10	191 781				
	1 time per month	1,49 E-10	767 123				
				SIL 1	**SIL 1**	**SIL 2**	
				Architectural constraints			

Single channel subsystem (HFT = 1)				DC = 60%	DC = 90%	DC = 99%	
B_{10D}	**Cycles**	λ_D	$MTTF_D$	PFH < λ_D 0,06	PFH < λ_D 0,03	PFH < λ_D 0,021	
1 000 000	1 time per minute	6,00 E-06	19	3,51 E-07	1,78 E-07	1,26 E-07	SIL 2 < 1,00 E-06
	1 time per hour	1,00 E-07	1 142	≪ 1,00 E-08			SIL 3 < 1,00 E-07
	1 time per day	4,17 E-09	27 397				
	1 time per week	5,96 E-10	191 781				
	1 time per month	1,49 E-10	767 123				
				SIL 2	**SIL 3**	**SIL 3**	
				Architectural constraints			

By assuming an SCS with four subsystems the PFH value limits and therefore the $MTTF_D$ and T_{10D} limits based on B_{10D} = 1 000 000 for each subsystem can be calculated as represented in the following Table H.6.

Table H.6 – Examples of PFH values based on T_{10D} and B_{10D}

SIL limits with 4 subsystems		DC = 0 % PFH = λ_D	DC = 60 % PFH < λ_D 0,5	DC = 90 % PFH < λ_D 0,2
HFT = 0	SIL 1, min. $MTTF_D$ [a]	$MTTF_D > 48$	$MTTF_D > 24$	
	$T_1 = T_{10D}$ [a]	**4,8**	**2,4**	
	Max. number of cycles per hour	24	48	
	SIL 2, min. $MTTF_D$ [a]			$MTTF_D > 92$
	$T_1 = T_{10D}$ [a]			**9,2**
	Max. number of cycles per hour			12,5

SIL limits with 4 subsystems		DC = 60 % PFH < λ_D 0,06	DC = 90 % PFH < λ_D 0,03	DC = 99 % PFH < λ_D 0,021
HFT = 1	SIL 2, min. $MTTF_D$ [a]	$MTTF_D > 28$	$MTTF_D > 12$	
	$T_1 = T_{10D}$ [a]	**2,8**	**1,2**	
	Max. number of cycles per hour	41	95	
	SIL 3, min. $MTTF_D$ [a]		$MTTF_D > 136$	$MTTF_D > 92$
	$T_1 = T_{10D}$ [a]		**13,6**	**9,2**
	Max. number of cycles per hour		8,5	12,5

H.8 Methodology for the estimation of CCF

In the case of redundant structures (architectures 1oo1D, 1oo2, 1oo2D), it is assumed that the two channels fit together in a non-reactive way. Therefore, the individual failure rates of the channels will not be increased just by combining them. The dangerous failure rate of the first channel is $\lambda_{D1} = \lambda_{DD1} + \lambda_{DU1}$ and that of the second channel, $\lambda_{D2} = \lambda_{DD2} + \lambda_{DU2}$.

However, the channels are not fully independent because a single occurrence or condition can cause a critical malfunction simultaneously on both channels.

By definition, a common cause failure is characterized by the failure of each channel due to the same ("common") cause: if only one channel fails then it cannot be a common cause failure.

That is why a common cause failure always depends on the channel with the lower failure rate.

– The maximum common cause failure rate λ_{CC} occurs with $\beta = 1$ (100 %).
– When the failure rate of the second channel is higher than that of the first one, the second channel has additional failures even with $\beta = 1$. These additional failures cannot be common cause failures and λ_{CC} will be lower than the higher failure rate of the two channels.
– The maximum number of common cause failures occurs if each failure of the channel with the lower failure rate is a common cause failure. Hence, the lowest failure rate of the two channels will limit λ_{CC}.

This approach is expressed by $\lambda_{CC} \approx \beta\ \mathrm{Min}(\lambda_{D1}, \lambda_{D2})$, see Figure H.2.

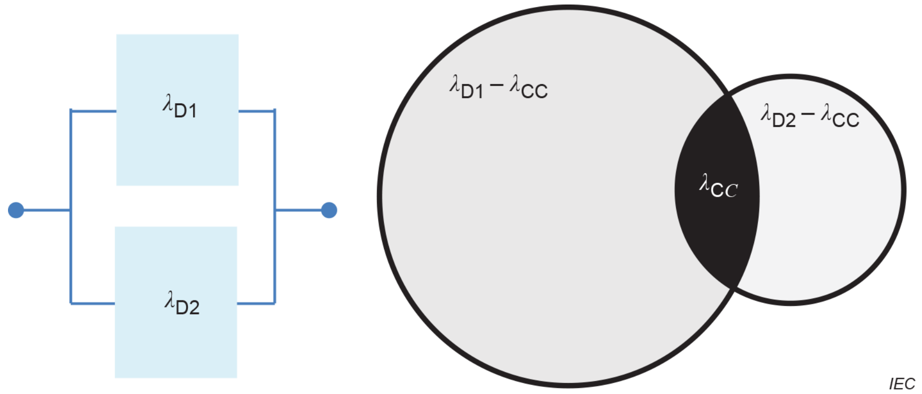


Figure H.2 – Common cause failure

This equation ensures that even with strong asymmetry of the failure rates the common cause failure rate cannot exceed the lower failure rate.

If no diagnostics (with additional hardware) for the detection of common cause failures is implemented, λ_{CC} yields a direct contribution to PFH which can be expressed by β Min(λ_{D1}, λ_{D2}).

H.9 Basic subsystem architecture A (1oo1)

H.9.1 General

This architecture consists of a single channel where any dangerous failure leads to a failure of the safety function when a demand arises. Figure H.3 shows the reliability block diagram at the instant t.

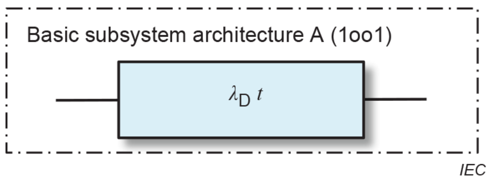


Figure H.3 – Basic subsystem architecture A (1oo1) reliability block diagram

The dangerous failure rate for the channel is given by λ_D. The unavailability is $P_D(t)$ is represented in Figure H.4.

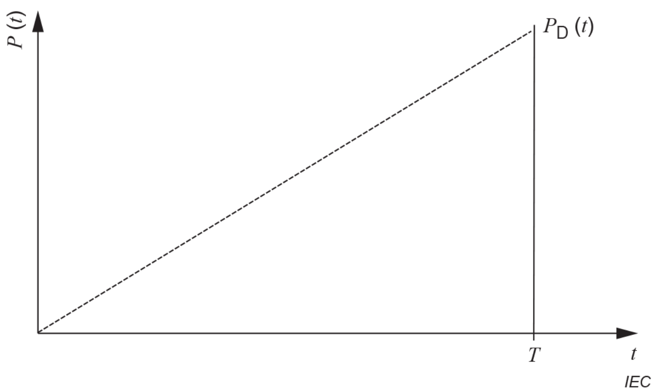


Figure H.4 – Unavailability function of basic subsystem architecture A (1oo1)

H.9.2 PFH

With the assumption ($\lambda\ t$) is << 1, the following simplified formula can be used, during the period [0, T], $P(t) = \lambda_D\, t$ (see H.5.1).

For a simplified approach $\text{PFH} = \frac{1}{T}\int_0^T P'_D(t)\ \text{dt}$ with $P'_D(t) \approx \lambda_D$ becomes

$$\text{PFH} = \frac{1}{T}\int_0^T \lambda_D\ \text{dt} = \frac{1}{T}\lambda_D\,[t]_0^T = \lambda_D \tag{H.18}$$

For the approach $\text{PFH} = \frac{1}{T}\int_0^T P'_D(t)\ \text{dt}$ with $P'_D(t) = \lambda_D\, e^{-\lambda_D\, t}$ becomes

$$\text{PFH} = \frac{1}{T}\int_0^T \lambda_D\ e^{-\lambda_D\ t}\ \text{dt} = \frac{1}{T}\left[e^{-\lambda_D\ t}\right]_0^T = \frac{1}{T}\left(1 - e^{-\lambda_D\ T}\right) \tag{H.19}$$

Formula (H.19) shows that the PFH (average frequency of failure) value can mathematically decrease the longer the considered time period *T* becomes, but for any hardware (electronic or non-electronic) component the used PFH value cannot change, i.e. it cannot decrease only because the considered time period is changing, i.e. increasing.

H.9.3 Simplified Weibull approach

This architecture consists of a single channel where any dangerous failure leads to a failure of the safety function when a demand arises. Figure H.5 shows the reliability block diagram at the instant *t* by assuming for example a shape factor of 2.

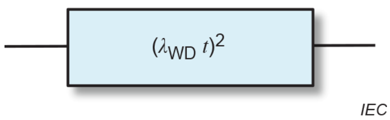


Figure H.5 – 1oo1 reliability block diagram, simplified Weibull approach

λ_{WD} represents the failure rate of the Weibull distribution (see also Formula (H.16)) and can be written as

$$\lambda_{WD} \approx 3{,}08\ \lambda_D \tag{H.20}$$

With the assumption that ($\lambda\ t$) is << 1, the following simplified formula can be used, during the period [0, T], $P_{WD}\ (t) \approx (\lambda_D t)^2$

$\text{PFH} = \frac{1}{T}\int_0^T P'_{WD}(t)\ \text{dt}$ with $P'_{WD}(t) \approx 2\,\lambda_{WD}{}^2\, t$ becomes

$$PFH = \frac{1}{T}\int_0^T 2\,\lambda_D^2\; t\; dt = \frac{1}{T}\;\lambda_{WD}^2\left[t^2\right]_0^T = \lambda_{WD}^2\,T \approx\; 9{,}49\,\lambda_D^2\; T \qquad (H.21)$$

H.10 Basic subsystem architecture C (1oo1D)

H.10.1 General

Two cases of performing of the fault reaction function will be distinguished:

1) Case 1: Another subsystem is performing the fault reaction function;
2) Case 2: A separate channel of the subsystem is performing the fault reaction function.

H.10.2 Fault reaction performed by another subsystem

This architecture consists of a single channel where any undetected dangerous failure leads to a failure of the safety function when a demand arises. The detection of any dangerous failure will lead to a safe state of the safety function.

EXAMPLE: A Type 2 photocell is connected to a safety-related logic solver. Dangerous failures of the photocell (λ_D) are cyclically monitored by the logic solver. Upon actuation of the photocell sensing field or upon detection of a dangerous failure the logic solver stops all dangerous movements by means of its safety-related output.

The logical view is represented in Figure H.6.

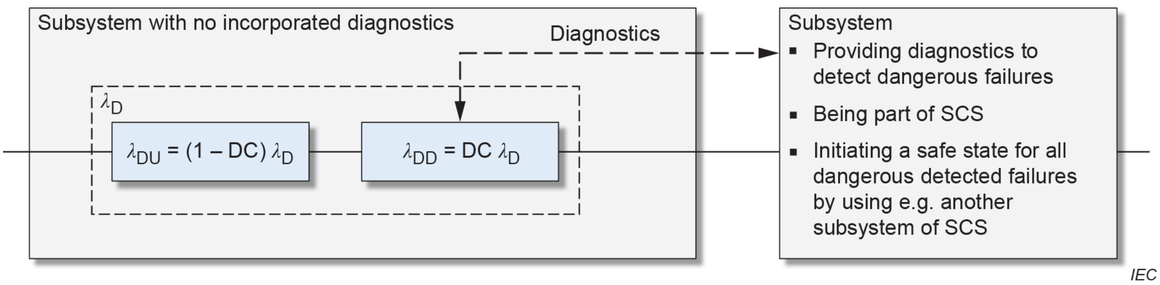


Figure H.6 – Basic subsystem architecture C (1oo1D) logical view with safe state initiation using another subsystem

Figure H.7 shows the reliability block diagram at the instant t.

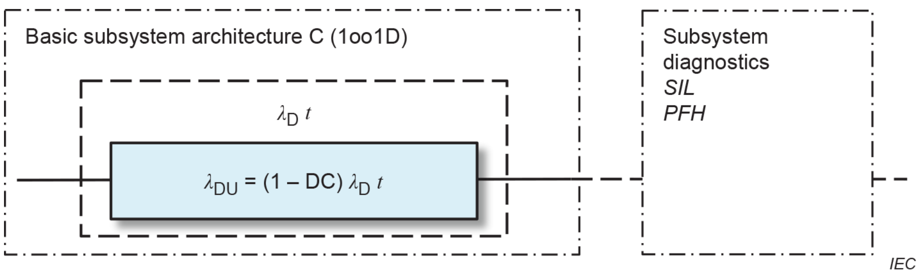


Figure H.7 – Basic subsystem architecture C (1oo1D) reliability block diagram with safe state initiation using another subsystem

The dangerous failure rate for the channel is given by $\lambda_D = \lambda_{DU}$ because the detection of any dangerous failure will lead to a safe state of the safety function.

The unavailability is $P_D(t) = P_{DU}(t)$. $P_{DU}(t)$ is represented in Figure H.8.

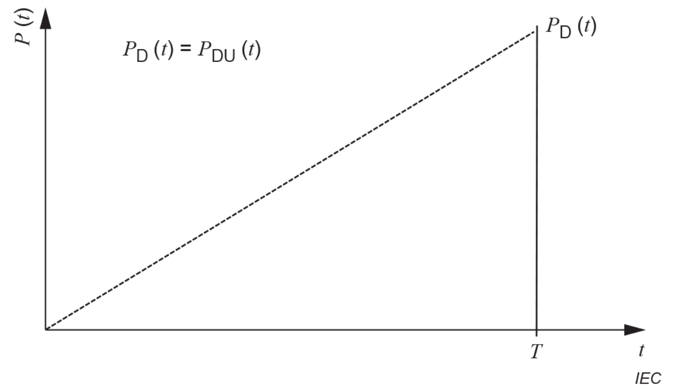


Figure H.8 – Unavailability functions of basic subsystem architecture C (1oo1D)

Based on the Formula (H.2) PFH becomes

$$\mathrm{PFH} = \frac{1}{T}\int_0^T \lambda_{\mathrm{DU}}\,\mathrm{dt} = \frac{1}{T}\lambda_{\mathrm{DU}}\left[t\right]_0^T = \lambda_{\mathrm{DU}} = \left(1-\mathrm{DC}\right)\lambda_{\mathrm{D}} \qquad \text{(H.22)}$$

H.10.3 Fault reaction to be considered in the subsystem

This architecture consists of a single channel, where any undetected dangerous failure leads to a failure of the safety function when a demand arises, and where detected dangerous failures lead to a fault reaction trying to initiate a safe state of the safety function.

The initiation of a safe state of the safety function depends therefore on detected dangerous failures (λ_{DD}) by the diagnostics and the fault reaction as a fault reaction channel (λ_{react}).

EXAMPLE A contactor λ_{D} is switched off to stop a dangerous movement. By monitoring the mirror contacts of this contactor another actuator (λ_{react}) (e.g. circuit breaker) can be switched off in case of a dangerous detected failure of the contactor.

The logical view is represented in Figure H.9.

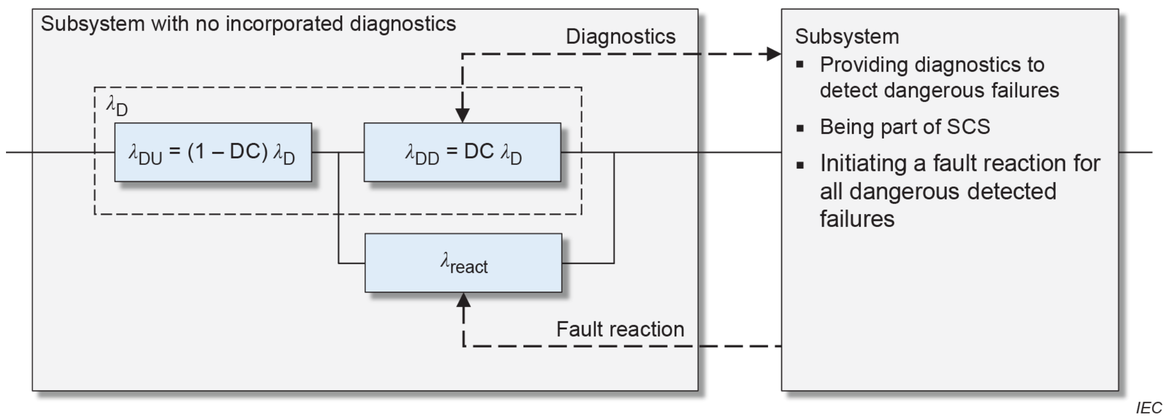


Figure H.9 – Basic subsystem architecture C (1oo1D) logical view with fault reaction

Figure H.10 shows the reliability block diagram at the instant t.

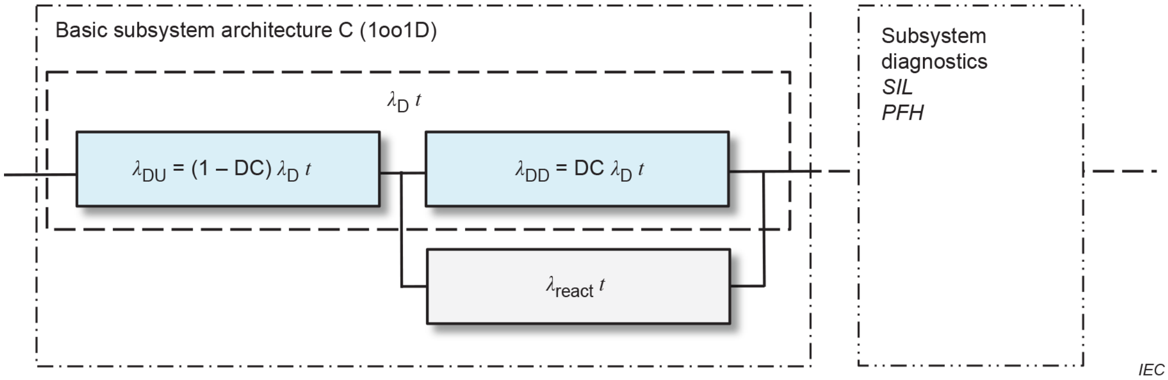


Figure H.10 – Basic subsystem architecture C (1oo1D) reliability block diagram with fault reaction

The unavailability can be written as $P_{\text{D}}(t)$ = $P_{\text{DU}}(t)$ + $P_{\text{Diag}}(t)$ = $P_{\text{DU}}(t)$ + $P_{\text{DD}}(t)$ $P_{\text{react}}(t)$

where the unavailability P_{Diag} is represented by two channels connected in parallel, the part of the functional channel (λ_{DD}) and the fault reaction channel (λ_{react}).

$P_{\text{DU}}(t)$, $P_{\text{DD}}(t)$ and $P_{\text{react}}(t)$ are represented in Figure H.11.

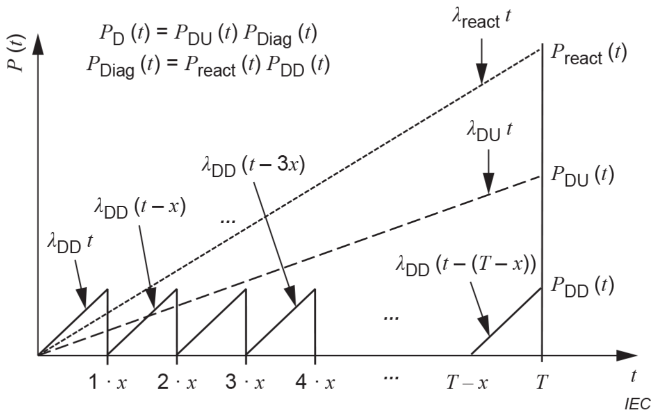


Figure H.11 – Unavailability functions of basic subsystem architecture C (1oo1D)

The quantity "x" represents the test interval (or diagnostic test interval, T_2) being << T (or useful lifetime, T_1) and being assumed to be $T = n\, x$.

The result of PFH_{DU} is equal to Formula (H.22): $\text{PFH}_{\text{DU}} = \lambda_{\text{DU}} = (1 - \text{DC})\, \lambda_{\text{D}}$

The following decomposition of PFH_{Diag} is possible:

$$\text{PFH}_{\text{Diag}} = \frac{1}{T}\int_0^T P'_{\text{Diag}}(t)\ \text{d}t$$

$$\text{PFH}_{\text{Diag}} = \frac{1}{T}\left(\int_0^x P'_{\text{Diag}}(t)\ \text{d}t + \int_x^{2x} P'_{\text{Diag}}(t)\ \text{d}t + \int_{2x}^{3x} P'_{\text{Diag}}(t)\ \text{d}t + \ldots + \int_{\text{T-}x}^{T} P'_{\text{Diag}}(t)\ \text{d}t\right) \qquad \text{(H.23)}$$

$$\mathrm{PFH_{Diag}} = \frac{1}{T} \sum_{K=1}^{n} \int_{(K-1)x}^{Kx} P'_{\mathrm{Diag}}(t)\ \mathrm{dt}$$

where $P_{\mathrm{Diag}}(t) = P_{\mathrm{react}}(t)\ P_{\mathrm{DD}}(t)$ and $P'_{\mathrm{Diag}}(t)$ over a generic period Δt = K-1,K becomes $P'_{\mathrm{Diag}}(t) = \lambda_{\mathrm{DD}}\ \lambda_{\mathrm{react}}\left[2\ t - (\mathrm{K}-1)x\right]$.

With the assumption ($\lambda\ t$) is << 1, the following simplified formulas can be used:

– $P_{\mathrm{react}}(t) \approx (\lambda_{\mathrm{react}}\ t)$, over the period [0, T];
– $P_{\mathrm{DD}}(t) \approx (\lambda_{\mathrm{DD}}\ t)$, over the period $\Delta t = x$ ([0,x], [x,2x], [2x,3x], …[T-x, T]).

NOTE For Δt periods becoming closer to T the assumption $\lambda\ t$ will provide higher results than the $(1 - e^{-\lambda\ t})$.

EXAMPLE: For Δt = 10 h [10 000, 10 010] and λ = 3,81 E-06 (30 years), $\lambda\ t$ = 3,81 E-05, but $(1 - e^{-\lambda\ 10\ 010}) - (1 - e^{-\lambda\ 10\ 000})$ = 3,66 E-05. In this case $\lambda\ t$ has higher 4 % results than with the detailed approach of $(1 - e^{-\lambda\ t})$, with λ = 1,14 E-05 (10 years), $\lambda\ t$ is 12 % higher.

Formula (H.23) becomes

$$\mathrm{PFH_{Diag}} = \lambda_{\mathrm{DD}}\ \lambda_{\mathrm{react}} \frac{(T_1 + T_2)}{2} \quad \text{(H.24)}$$

H.10.4 PFH

The summation of the terms in Formulas (H.22) and (H.24) can be written as

$$\mathrm{PFH} = (1\text{-}\mathrm{DC})\lambda_{\mathrm{D}} + \lambda_{\mathrm{DD}}\ \lambda_{\mathrm{react}} \frac{(T_1 + T_2)}{2} \quad \text{(H.25)}$$

H.10.5 Influence of CCF

The term in Formula (H.25) becomes

$$\mathrm{PFH} = (1\text{-}\mathrm{DC})\ \lambda_{\mathrm{D}}^{\mathrm{cc}} + \ \mathrm{DC}\ \lambda_{\mathrm{D}}^{\mathrm{cc}}\ \lambda_{\mathrm{react}}^{\mathrm{cc}} \frac{(T_1 + T_2)}{2} + \lambda_{\mathrm{cc}} \quad \text{(H.26)}$$

where $\lambda_{\mathrm{CC}} = \beta\ \mathrm{Min}(\lambda_{\mathrm{D}}, \lambda_{\mathrm{react}})$, $\lambda_{\mathrm{D}}^{\mathrm{cc}} = \lambda_{\mathrm{D}} - \lambda_{\mathrm{cc}}$, $\lambda_{\mathrm{react}}^{\mathrm{cc}} = \lambda_{\mathrm{react}} - \lambda_{\mathrm{cc}}$, T_1 represents the useful lifetime, λ_{D} the failure rate of the channel, λ_{react} the failure rate of the fault reaction function and DC the diagnostic coverage of the channel and T_2 the diagnostic test interval with $T_2 \ll T_1$.

The worst case should be considered with $\beta\ \mathrm{Min}(\lambda_{\mathrm{D}}, \lambda_{\mathrm{react}}) = \beta\ \lambda_{\mathrm{D}}$ as the value of λ_{react} will be in practice lower than λ_{D}.

$$\text{PFH} = (1-\beta)(1-\text{DC})\,\lambda_D + (1-\beta)\,\text{DC}\,\lambda_D\,(\lambda_{\text{react}} - \beta\,\lambda_D)\frac{(T_1+T_2)}{2} + \beta\,\lambda_D \quad \text{(H.27)}$$

When the value of λ_{react} will be in practice lower than or equal to λ_D the Formula (H.27) becomes with $\lambda_{\text{react}} = \lambda_D$

$$\text{PFH} = (1-\beta)(1\text{-}\,\text{DC})\,\lambda_D + (1-\beta)^2\ \ \text{DC}\,\lambda_D{}^2\,\frac{(T_1+T_2)}{2} + \beta\,\lambda_D \quad \text{(H.28)}$$

H.11 Basic subsystem architecture B (1oo2)

H.11.1 General

This architecture consists of two channels connected in parallel, such that either channel can perform the safety function. A single failure of a channel will not cause the loss of the safety function. There are no diagnostics to detect any dangerous failure in both channels. When there is a dangerous failure in both channels the safety function will fail when a demand arises. Figure H.12 shows the reliability block diagram at the instant t.

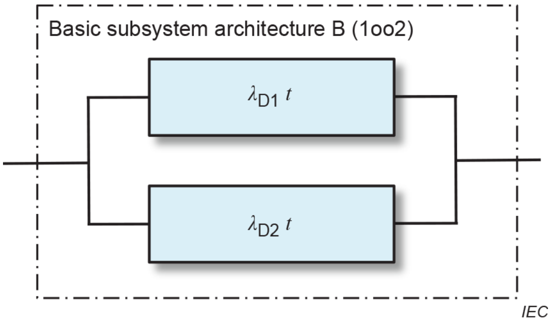


Figure H.12 – Basic subsystem architecture B (1oo2) reliability block diagram

The dangerous failure rates are given by λ_{D1} and λ_{D2}.

The unavailability is $P_D(t) = P_{D1}(t)\,P_{D2}(t)$.

$P_{D1}(t)$ and $P_{D2}(t)$ are represented in Figure H.13.

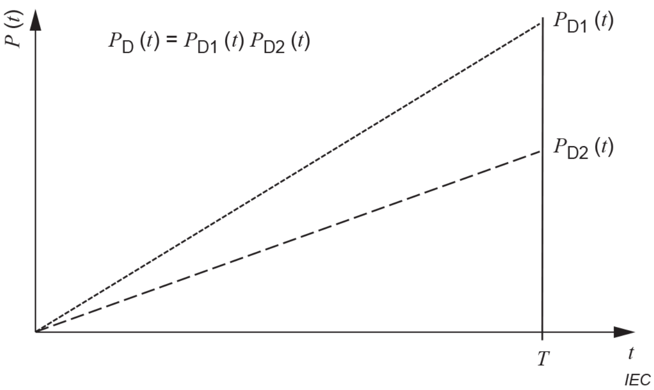


Figure H.13 – Unavailability functions of basic subsystem architecture B (1oo2)

H.11.2 PFH

With the assumption ($\lambda\, t$) is << 1, the following simplified formulas can be used, during the period [0, T], $P_{D1}(t) \approx \lambda_{D1}\, t$ and $P_{D2}(t) \approx \lambda_{D2}\, t$ and $P_D(t) \approx \lambda_{D1}\, \lambda_{D2}\, t^2$.

$\text{PFH} = \frac{1}{T}\int_0^T P'_D(t)\,\text{dt}$ with $P'_D(t) \approx 2\, \lambda_{D1}\, \lambda_{D1}\, t$ becomes

$$\text{PFH} = \frac{1}{T}\lambda_{D1}\lambda_{D2}\left[t^2\right]_0^T = \frac{1}{T}\lambda_{D1}\lambda_{D2}T^2 = \lambda_{D1}\lambda_{D2}T \tag{H.29}$$

Furthermore, the Formula (H.29) can be written as

$$\text{PFH} = \text{PFH}_{D1}\ \text{PFH}_{D2}\ T \tag{H.30}$$

where $\text{PFH}_{D1} = \lambda_{D1}$ and $\text{PFH}_{D2} = \lambda_{D2}$.

H.11.3 Influence of CCF

The term in Formula (H.29) becomes

$$\text{PFH} = \lambda_{D1}^{cc}\ \lambda_{D2}^{cc} T_1 + \beta\,\lambda_{cc} \tag{H.31}$$

where $\lambda_{cc} = \beta\ \text{Min}(\lambda_{D1}, \lambda_{D2})$, $\lambda_{D1}^{cc} = \lambda_{D1} - \lambda_{cc}$, $\lambda_{D2}^{cc} = \lambda_{D2} - \lambda_{cc}$, T_1 represents the useful lifetime, λ_{D1}, and λ_{D2} the failure rate of the channel 1 and 2.

When $\lambda_D = \lambda_{D1} = \lambda_{D2}$ the Formula (H.31) becomes

$$\text{PFH} = (1-\beta)^2\ \lambda_D^{\ 2}\ T_1 +\ \beta\,\lambda_D \tag{H.32}$$

H.12 Basic subsystem architecture D (1oo2D)

H.12.1 General

This architecture consists of two channels connected in parallel, such that either channel can perform the safety function. A single failure of a channel will not cause the loss of the safety function. There are diagnostics to detect dangerous failure in both channels. The detection of a dangerous failure in any channel will initiate the safe state of the safety function. Figure H.14 shows the reliability block diagram at the instant *t*.

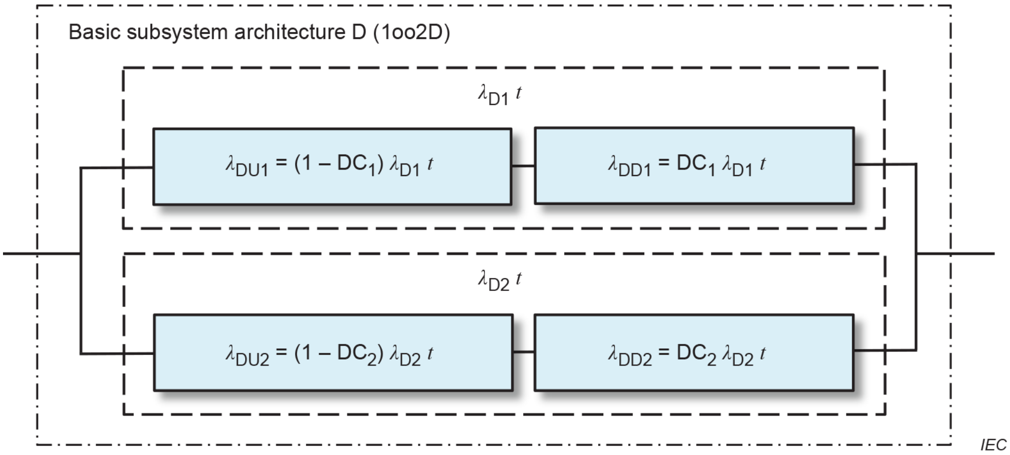


Figure H.14 – Basic subsystem architecture D (1oo2D) reliability block diagram

The dangerous failure rates are given by $\lambda_{D1} = \lambda_{DU1} + \lambda_{DD1}$ and $\lambda_{D1} = \lambda_{DU1} + \lambda_{DD1}$.

The unavailability is $P_D(t) = P_{D1}(t)\ P_{D2}(t) = (P_{DU1}(t) + P_{DD1}(t))\ (P_{DU2}(t) + P_{DD2}(t))$.

$P_{DU1}(t)$, $P_{DD1}(t)$, $P_{DU2}(t)$ and $P_{DD2}(t)$ are represented in Figure H.15.

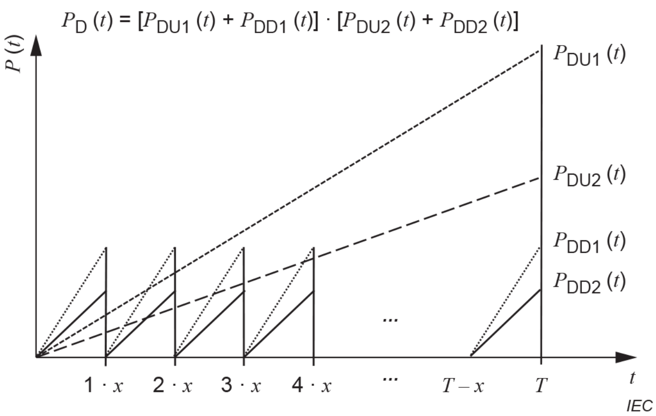


Figure H.15 – Unavailability functions of basic subsystem architecture D (1oo2D)

The quantity "x" represents the test interval (or diagnostic test interval, T_2) being << T (or useful lifetime, T_2) and being assumed to be $T = n\ x$ and

$$\text{PFH} = \frac{1}{T}\int_0^T P'_D(t)\,\text{dt} = \frac{1}{T}\left(\int_0^x P'_D(t)\,\text{dt} + \int_x^{2x} P'_D(t)\,\text{dt} + \int_{2x}^{3x} P'_D(t)\,\text{dt} + \ldots + \int_{\text{T-}x}^{T} P'_D(t)\,\text{dt}\right)$$

With the assumption ($\lambda\ t$) is << 1, the following simplified formulas can be used:

- $P_{DU1}(t) \approx \lambda_{DU1}\ t$, $P_{DU2}(t) \approx \lambda_{DU2}\ t$ over the period [0, T];
- $P_{DD1}(t) \approx \lambda_{DD1}\ t$, $P_{DD2}(t) \approx \lambda_{DD2}\ t$ over the period $\Delta t = x$ ([0,x], [x,2x], [2x,3x], …[T-x, T]).

$$P_D(t) = \underbrace{P_{DD1}(t)P_{DD2}(t)}_{\text{Term A}} + \underbrace{P_{DU1}(t)P_{DU2}(t)}_{\text{Term B}} + \underbrace{P_{DU1}(t)P_{DD2}(t)}_{\text{Term C}} + \underbrace{P_{DD1}(t)P_{DU2}(t)}_{\text{Term D}}$$

H.12.2 PFH evaluation of Term A

In general, PFH is defined by

$$\mathrm{PFH} = \frac{1}{T}\int_0^T P_D'(t)\,\mathrm{dt} = \frac{1}{T}\left(\int_0^x P_D'(t)\,\mathrm{dt} + \int_x^{2x} P_D'(t)\,\mathrm{dt} + \int_{2x}^{3x} P_D'(t)\,\mathrm{dt} + \ldots + \int_{T\text{-}x}^{T} P_D'(t)\,\mathrm{dt}\right)$$

The number of periods Δt is equal to $\left(\frac{T}{x}\right)$.

For each period $\Delta t = x$ ([0,x], [x,2x], [2x,3x], …[T-x, T]) the product of $P_{DD1}(t)\ P_{DD2}(t)$ will be the same and therefore PFH can be written as follows

$$\mathrm{PFH} = \frac{1}{T}\int_0^T P'(t)\,\mathrm{dt} = \frac{1}{x}\int_0^x P'(t)\,\mathrm{dt} = \frac{1}{x}\lambda_{DD1}\ \lambda_{DD2}\ x^2 = \lambda_{DD1}\ \lambda_{DD2}\ x \qquad \text{(H.33)}$$

or

$$\mathrm{PFH} = \lambda_{DD1}\ \lambda_{DD2}\ T_2 \qquad \text{(H.34)}$$

where $P(t) = P_{DD1}(t)\ P_{DD2}(t) = \lambda_{DD1}\ \lambda_{DD2}\ t^2$ and $P'(t) = 2\ \lambda_{DD1}\ \lambda_{DD2}\ t$.

H.12.3 PFH evaluation of Term B

During the period [0, T], $P_{DU1}(t) \approx \lambda_{DU1}\ t$, $P_{DU2}(t) \approx \lambda_{DU2}\ t$, $P'_{DU1}(t)\ P'_{DU2}(t) \approx 2\lambda_{DU1}\ \lambda_{DU2}\ t$ and the PFH formula can be written as

$$\mathrm{PFH} = \frac{1}{T}\int_0^T 2\ \lambda_{DU1}\ \lambda_{DU2}\ \mathrm{t}\ dt \approx \lambda_{DU1}\lambda_{DU2}\ T \qquad \text{(H.35)}$$

or

$$\mathrm{PFH} \approx \left(1 - \mathrm{DC}_1\right)\lambda_{D1}\left(1 - \mathrm{DC}_2\right)\lambda_{D2}\ T_1 \qquad \text{(H.36)}$$

H.12.4 PFH evaluation of Term C and Term D

The PFH formula can be written as follows (based on Formula (H.24)):

$$\mathrm{PFH} = \lambda_{DU1}\ \lambda_{DD2}\ \left(\frac{T + x}{2}\right) + \lambda_{DU2}\ \lambda_{DD1}\ \left(\frac{T + x}{2}\right) \qquad \text{(H.37)}$$

or

$$\mathrm{PFH} = \left[(1 - \mathrm{DC}_1)\, \lambda_{\mathrm{D1}}\, \mathrm{DC}_2\, \lambda_{\mathrm{D2}} + (1 - \mathrm{DC}_2)\, \lambda_{\mathrm{D2}}\, \mathrm{DC}_1\, \lambda_{\mathrm{D1}} \right] \left(\frac{T_1 + T_2}{2} \right) \quad (\mathrm{H.38})$$

H.12.5 PFH

The summation of the terms in Formula (H.34), Formula (H.36) and Formula (H.38) can be written as

$$\mathrm{PFH} = \frac{\lambda_{\mathrm{D1}}\, \lambda_{\mathrm{D2}}}{2} \left[T_1 (2 - \mathrm{DC}_1 - \mathrm{DC}_2) + T_2 (\mathrm{DC}_1 + \mathrm{DC}_2) \right] \quad (\mathrm{H.39})$$

H.12.6 Influence of CCF

The term in Formula (H.39) becomes

$$\mathrm{PFH} = \lambda_{\mathrm{D1}}^{\mathrm{cc}}\, \lambda_{\mathrm{D2}}^{\mathrm{cc}}\, (2 - \mathrm{DC}_1 - \mathrm{DC}_2) \frac{T_1}{2} + \lambda_{\mathrm{D1}}^{\mathrm{cc}}\, \lambda_{\mathrm{D2}}^{\mathrm{cc}} (\mathrm{DC}_1 + \mathrm{DC}_2) \frac{T_2}{2} + \lambda_{\mathrm{cc}} \quad (\mathrm{H.40})$$

Where $\lambda_{\mathrm{cc}} = \beta\ \mathrm{Min}(\lambda_{\mathrm{D1}}, \lambda_{\mathrm{D2}})$, $\lambda_{\mathrm{D1}}^{\mathrm{cc}} = \lambda_{\mathrm{D1}} - \lambda_{\mathrm{cc}}$, $\lambda_{\mathrm{D2}}^{\mathrm{cc}} = \lambda_{\mathrm{D2}} - \lambda_{\mathrm{cc}}$, T_1 represents the useful lifetime, λ_{D1} and λ_{D2} the failure rate of the channel 1 and 2, DC_1 and DC_2 the diagnostic coverage of the channel 1 and 2 and T_2 the diagnostic test interval with T_2 « T_1.

Where $\lambda = \lambda_{\mathrm{D1}} = \lambda_{\mathrm{D1}}$ and $\mathrm{DC} = \mathrm{DC}_1 = \mathrm{DC}_2$ the Formula (H.40) becomes

$$\mathrm{PFH} = (1 - \beta)^2\, \lambda_{\mathrm{D}}^2\, (1 - \mathrm{DC}) T_1 + (1 - \beta)^2\, \lambda_{\mathrm{D}}^2\, \mathrm{DC}\, T_2 + \beta\, \lambda_{\mathrm{D}} \quad (\mathrm{H.41})$$

H.13 Basic subsystem architecture D (1oo2D) with two periods of time consideration

H.13.1 General

For a non-electronic component, the useful lifetime is given by $T_{10\mathrm{D}}$, the mean time until 10 % of components fail dangerously. Depending on the mean number of annual operations of the component, the computed value $T_{10\mathrm{D}}$ could turn out to be less than the useful time T_1 specified for the subsystem, therefore useful lifetime will be limited to $T_{10\mathrm{D}}$. It may happen that in an architecture 1oo2D, depending on the particular application, the components in the two channels have different $T_{10\mathrm{D}}$ values and, consequently, the two channels will have two different values of useful lifetime (named below $T_{1\mathrm{o}1}$ and $T_{1\mathrm{o}2}$).

EXAMPLE: One channel consists of a main contactor that is switched off for normal machine function and when the safety function will be demanded. The second channel consist of a main contactor which is only switched off when the safety function will be demanded.

The reliability block diagram is the same as in H.12.1.

The unavailability is $P_{\mathrm{D}}(t) = P_{\mathrm{D1}}(t)\, P_{\mathrm{D2}}(t) = (P_{\mathrm{DU1}}(t) + P_{\mathrm{DD1}}(t))\, (P_{\mathrm{DU2}}(t) + P_{\mathrm{DD2}}(t))$ and

$$\mathrm{PFH} = \frac{1}{T}\int_0^T P'_{\mathrm{D}}(t)\,\mathrm{dt} = \frac{1}{T}\left(\int_0^x P'_{\mathrm{D}}(t)\,\mathrm{dt} + \int_x^{2x} P'_{\mathrm{D}}(t)\,\mathrm{dt} + \int_{2x}^{3x} P'_{\mathrm{D}}(t)\,\mathrm{dt} + \ldots + \int_{T\text{-}x}^{T} P'_{\mathrm{D}}(t)\,\mathrm{dt}\right)$$

With the assumption ($\lambda\ t$) is << 1, the following simplified formulas can be used:

– $P_{\mathrm{DU1}}(t) \approx \lambda_{\mathrm{DU1}}\ t$ over the period [0, $T_{1\mathrm{o}1}$], $P_{\mathrm{DU2}}(t) \approx \lambda_{\mathrm{DU2}}\ t$ over the period [0, $T_{1\mathrm{o}2}$];

– $P_{\mathrm{DD1}}(t) \approx \lambda_{\mathrm{DD1}}\ t$, $P_{\mathrm{DD2}}(t) \approx \lambda_{\mathrm{DD2}}\ t$ over the period $\Delta t = x$ ([0,x], [x,2x], [2x,3x], …[T-x, T]).

$$P_{\mathrm{D}}(t) = \underbrace{P_{\mathrm{DD1}}(t)P_{\mathrm{DD2}}(t)}_{\text{Term A}} + \underbrace{P_{\mathrm{DU1}}(t)P_{\mathrm{DU2}}(t)}_{\text{Term B}} + \underbrace{P_{\mathrm{DU1}}(t)P_{\mathrm{DD2}}(t)}_{\text{Term C}} + \underbrace{P_{\mathrm{DD1}}(t)P_{\mathrm{DU2}}(t)}_{\text{Term D}} \quad \text{(H.42)}$$

The periods of time consideration are $T_{1\mathrm{o}1}$ for channel 1 and $T_{1\mathrm{o}2}$ for channel 2.

H.13.2 PFH evaluation of Term A

In general, PFH is defined by

$$\mathrm{PFH} = \frac{1}{T}\int_0^T P'_{\mathrm{D}}(t)\,\mathrm{dt} = \frac{1}{T}\left(\int_0^x P'_{\mathrm{D}}(t)\,\mathrm{dt} + \int_x^{2x} P'_{\mathrm{D}}(t)\,\mathrm{dt} + \int_{2x}^{3x} P'_{\mathrm{D}}(t)\,\mathrm{dt} + \ldots + \int_{T\text{-}x}^{T} P'_{\mathrm{D}}(t)\,\mathrm{dt}\right)$$

The number of periods Δt respectively are equal to $\left(\frac{T_{1\mathrm{o}1}}{x}\right)$ and $\left(\frac{T_{1\mathrm{o}2}}{x}\right)$ and PFH becomes

$$\mathrm{PFH} = \frac{1}{x}\lambda_{\mathrm{DD1}}\ \lambda_{\mathrm{DD2}}\ x^2 = \mathrm{DC}_1\ \lambda_{\mathrm{D1}}\ \mathrm{DC}_2\ \lambda_{\mathrm{D2}}\ x \quad \text{(H.43)}$$

or

$$\mathrm{PFH} = \lambda_{\mathrm{DD1}}\ \lambda_{\mathrm{DD2}}\ T_2 \quad \text{(H.44)}$$

where $P(t) = P_{\mathrm{DD1}}(t)\ P_{\mathrm{DD2}}(t) = \lambda_{\mathrm{DD1}}\ \lambda_{\mathrm{DD2}}\ t^2$ and $P'(t) = 2\ \lambda_{\mathrm{DD1}}\ \lambda_{\mathrm{DD2}}\ t$.

H.13.3 PFH evaluation of Term B

During the period [0, T], $P_{\mathrm{DU1}}(t) \approx \lambda_{\mathrm{DU1}}\ t$, $P_{\mathrm{DU2}}(t) \approx \lambda_{\mathrm{DU2}}\ t$, the PFH formula can be written as

$$\mathrm{PFH} = (1-\mathrm{DC}_1)\ \lambda_{\mathrm{D1}}(1-\mathrm{DC}_2)\ \lambda_{\mathrm{D2}}\ \left(\frac{T_{1\mathrm{o}1}+T_{1\mathrm{o}2}}{2}\right) \quad \text{(H.45)}$$

H.13.4 PFH evaluation of Term C and Term D

The PFH formula can be written as

$$\text{PFH} = \lambda_{\text{DU1}}\ \lambda_{\text{DD2}}\ \left(\frac{T_{1\text{o}1}+x}{2}\right)+\lambda_{\text{DU2}}\ \lambda_{\text{DD1}}\ \left(\frac{T_{1\text{o}2}+x}{2}\right) \tag{H.46}$$

or

$$\text{PFH} = \lambda_{\text{D1}}\lambda_{\text{D2}}\left[(1-\text{DC}_1)\text{DC}_2\left(\frac{T_{1\text{o}1}+T_2}{2}\right)+(1-\text{DC}_2)\ \text{DC}_1\left(\frac{T_{1\text{o}2}+T_2}{2}\right)\right] \tag{H.47}$$

H.13.5 PFH

The summation of the terms in Formula (H.44), Formula (H.45) and Formula (H.47) can be written as

$$\text{PFH} = \frac{\lambda_{\text{D1}}\ \lambda_{\text{D2}}}{2}\left[\ T_{1\text{o}1}(1-\text{DC}_1)+T_{1\text{o}2}(1-\text{DC}_2)+T_2(\text{DC}_1+\text{DC}_2)\right]. \tag{H.48}$$

H.13.6 Influence of CCF

The term in Formula (H.45) becomes

$$\text{PFH} = \lambda_{\text{D1}}^{\text{cc}}\ \lambda_{\text{D2}}^{\text{cc}}\ (1-\text{DC}_1)\frac{T_{1\text{o}1}}{2}+\lambda_{\text{D1}}^{\text{cc}}\ \lambda_{\text{D2}}^{\text{cc}}\ (1-\text{DC}_2)\frac{T_{1\text{o}2}}{2}+\lambda_{\text{D1}}^{\text{cc}}\ \lambda_{\text{D2}}^{\text{cc}}\ (\text{DC}_1+\text{DC}_2)\ \frac{T_2}{2}+\lambda_{\text{cc}}\ . \tag{H.49}$$

Where $\lambda_{\text{cc}} = \beta\ \text{Min}(\lambda_{\text{D1}},\ \lambda_{\text{D2}})$, $\lambda_{\text{D1}}^{\text{cc}} = \lambda_{\text{D1}} - \lambda_{\text{cc}}$, $\lambda_{\text{D2}}^{\text{cc}} = \lambda_{\text{D2}} - \lambda_{\text{cc}}$, $T_{1\text{o}1}$ and $T_{1\text{o}2}$ represent the useful lifetime of channel 1 and 2, λ_{D1} and λ_{D1} the failure rate of the channel 1 and 2, DC_1 and DC_2 the diagnostic coverage of the channel 1 and 2 and T_2 the diagnostic test interval.

Annex I
(informative)

Commented examples of current regulations

I.1 General

Safety requirements for machinery exist worldwide. The regulatory method or legislative acts depend on local regulations. IEC and ISO International Standards in whole or in part can be incorporated by reference in such local regulations. Principle approaches are listed in this Annex I for illustration purposes only. The following examples are given for information purposes and do not constitute an exhaustive list. Any commentary thereof is merely for the purposes of informative contextualization and will not be relied upon as authoritative.

I.2 European Union

I.2.1 General European legislation

NOTE See link for more information: https://ec.europa.eu/growth/sectors/mechanical-engineering/machinery/

The use of a machine is covered by the requirements of Directive 2009/104/EC of the European Parliament and of the Council of 16 September 2009 concerning the minimum safety and health requirements for the use of work equipment by workers at work (second individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) that replaces 89/655/CEE Directive.

For the new machines sector, the applicable official text is the Machinery Directive:

– Directive 2006/42/EC of the European Parliament and of the Council of 17 May 2006 on machinery, and amending Directive 95/16/EC (recast) that replaces Machinery Directive 98/37/EC
– Machinery Directive 98/37/EC of the European Parliament and of the Council of 22 June 1998 that came into force December 29, 2009 and replaced Machinery Directive 89/392/EEC
– Council Directive 89/392/EEC of 14 June 1989

I.2.2 New proposed machinery regulation (under preparation)

A new machinery regulation is in progress to replace the actual Machinery Directive.

This revision was based on the fact that if the text of the directive was generally "relevant, effective, efficient and coherent", it was highlighted the need for improvements, simplifications and the need to fill a number of gaps.

The objective of this regulation[2] is to improve deficiencies and to contribute to both the digital transition and the strengthening of the single market. Additionally, the new machinery regulation will respond to the market needs by bringing greater legal clarity to the current provisions, simplifying the administrative burden and costs for companies by allowing digital formats for documentation and adapting conformity assessment fees for SMEs, while ensuring coherence with the EU legislative framework for products.

---

[2] The new Machinery Regulation is intended to ensure that the new generation of machinery guarantees the safety of users and consumers, and encourages innovation. While the AI Regulation is intended to address the safety risks of AI systems, the new Machinery Regulation is intended to ensure the safe integration of the AI system into the overall machinery. Businesses will need to perform only one single conformity assessment. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1682

The general objectives of the Machinery Directive are to ensure not only the free movement of machinery within the internal market but also a high level of protection for users and other exposed persons.

The available documents are present on the Europa website[3] and several documents are available:

– Proposal for a Regulation of the European Parliament and of the Council on machinery products;
– ANNEX – Annex to the Proposal for a Regulation of the European Parliament and of the Council on machinery products;
– Impact assessment;
– Executive summary of the impact assessment.

I.2.3 Relevant legislation

One of the main pieces of legislation governing the harmonization of essential health and safety requirements for machinery at EU level is the Machinery Directive 2006/42/EC.

The Machinery Directive

– promotes the free movement of machinery within the single market
– guarantees a high level of protection for EU workers and citizens.

As it is a 'new approach' directive, it promotes harmonization through a combination of mandatory health and safety requirements and voluntary harmonized standards. The Machinery Directive only applies to products that are to be placed on the EU market for the first time.

The Machinery Directive 2006/42/EC was published on 9 June 2006 and became applicable on 29 December 2009. It was amended by Directive 2009/127/EC of the European Parliament and of the Council of 21 October 2009, with regard to machinery for pesticide application, and by Regulation (EU) No 167/2013 of the European Parliament and of the Council of 5 February 2013 on the approval and market surveillance of agricultural and forestry vehicles, among others.

NOTE EU legislation that can apply to machinery, in addition to the Machinery Directive, for hazards they cover more specifically than the Machinery Directive, are for example

– Directive 2014/34/EU49 on equipment and protective systems intended for use in potentially explosive atmospheres (ATEX Directive);
– Directive 2014/68/EU59 on pressure equipment (PED);
– Directive 2014/53/EU65 on radio equipment (RED);
– Directive 2000/14/EC67 as amended by Directive 2005/88/EC68 on the noise emission in the environment by equipment for use outdoors (OND;
– Directive 2014/30/EU73 on electromagnetic compatibility (EMCD).

I.2.4 Duties of the manufacturer of the machine

According to the Machinery Directive the manufacturer’s tasks are as follows:

– carry out a risk assessment to identify which health and safety requirements apply to their machinery;
– keep the risk assessment in mind when designing and building their machinery;
– determine what limits there are on using the machinery;
– identify any possible hazards;

[3] https://ec.europa.eu/docsroom/documents/45508.

– assess the risk of their machinery causing severe injury or damage and take action to make their machinery safer;
– make sure that their machinery complies with the essential health and safety requirements listed in Annex I to the Machinery Directive;
– provide a technical document confirming that the machinery meets the Machinery Directive's requirements;
– make sure that they are applying conformity assessment procedures and that they are making all necessary information available, including instructions for assembly and use;
– check that they have filled in the EC declaration of conformity and that the CE conformity marking has been put on the machinery so that it can be used anywhere in the EU.

I.3 North America – USA

NOTE Relevant internet links:

https://standards.gov/sibr/query/index.cfm?fuseaction=home.main
https://ibr.ansi.org/
https://www.ansi.org/standards_activities/nss/media_usss?menuid
https://www.nist.gov/standardsgov/what-we-do/federal-policy-standards/key-federal-directives
https://www.cpsc.gov/Regulations-Laws--Standards

Examples of relevant legislation and standards can be found in:

– Safety of Machinery: Code of Federal Regulation (CFR) Title 29; Part 1910 (Subpart O – Machinery and Machine Guarding);
– Electrical Safety: Code of Federal Regulation (CFR) Title 29; Part 1910 (Subpart S-Electrical);
– NFPA 79, the electrical standard for industrial machinery is aligned with IEC 60204-1;
– UL 508A, electrical standard for industrial control panels;
– ANSI B11.0 (safety of machinery), ANSI B11.19 (performance requirements for risk reduction measures: Safeguarding and other means of reducing risk) and ANSI B11.26 (performance requirements for risk reduction measures: safeguarding and other means of reducing risk).

I.4 North America – Canada

NOTE Relevant internet links:

http://www.canlii.org/
http://www.justice.gc.ca/eng/index.html

Examples of relevant legislation and standards can be found in:

– Canada Consumer Product Safety Act
– Product Safety, O Reg 438/07
– C22.1-18: Canadian Electrical Code, Part I
– CSA C22.2 No 0 – General Requirements, Canadian Electrical Code, Part II and CSA C22.2 No 301 Industrial Electrical Machinery; SU 2011 Factory Automation Equipment and NFPA 79 Industrial Machinery.

I.5 South America – Brazil

Example of relevant legislation can be found in:

Regulation on Equipment and Machinery, no. 12 (Segurança no Trabalho em Máquinas e Equipamentos).

I.6 China

Example of relevant standards is as follows:

– IEC 62061:2005 was converted into China's national security standard GB 28526-2012 and promulgated and implemented in 2012.

I.7 Japan

Examples of relevant legislation are as follows:

The Industrial Safety and Health Act covers the employer's role in investigating the danger or harm, etc., due to buildings, facilities (machines, electric facilities), raw materials, gases, vapours, dust, etc., and those arising from work actions and other duties, and measures to prevent dangers or health impairment to workers.

Internet link: http://www.japaneselawtranslation.go.jp/law/detail/?id=1926&vm&re

Internet link: http://www.japaneselawtranslation.go.jp/law/detail/?id=1984&vm=04&re=01

The Electric Business Act defines "electric facilities".

NOTE "Electric facilities" are categorized as "for business use", "for general use", "for private", etc.

Internet link: http://www.japaneselawtranslation.go.jp/law/detail/?id=3355&vm=&re

Annex J
(informative)

Combination of modes of operation

J.1 General

The control system of processing equipment can be used to ensure the safety of persons, property and environment.

This control system is part of the so-called safety instrumented functions (SIF) according to IEC 61511 where safety requirements and protective measures will be considered. The demand rate of a safety instrumented function (SIF) is often considered in the context of a low demand mode of operation (less than or equal to 1 time per year).

NOTE See IEC 61511-1 for safety instrumented functions (SIF).

Nevertheless, machines with safety functions designed for high demand or continuous mode of operation can be used in this kind of application.

Clause J.2 shows a basic approach of the high demand mode of operation (see IEC 61508 and IEC 62061) and low demand mode of operation (see IEC 61508 and IEC 61511).

Clause J.3 gives guidance on how to design safety instrumented functions (SIF) by combining subsystems designed for low demand mode of operation and subsystems designed for high demand mode of operation.

J.2 Basic approaches with different modes of operation

J.2.1 General

Principally the approaches of high demand or continuous mode of operation and low demand mode of operation are similar based on decomposition of a safety function or a safety instrumented function (SIF) into subsystems where the failure of a subsystem leads to the loss of the respective function, see Figure J.1 and Figure J.2.

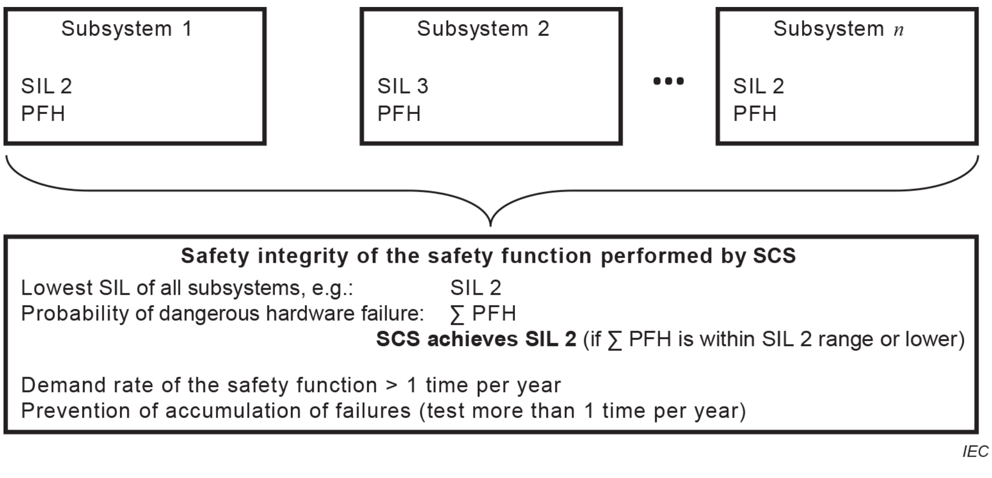


Figure J.1 – Basic approach in high demand or continuous mode of operation based on IEC 61508 (and IEC 62061)

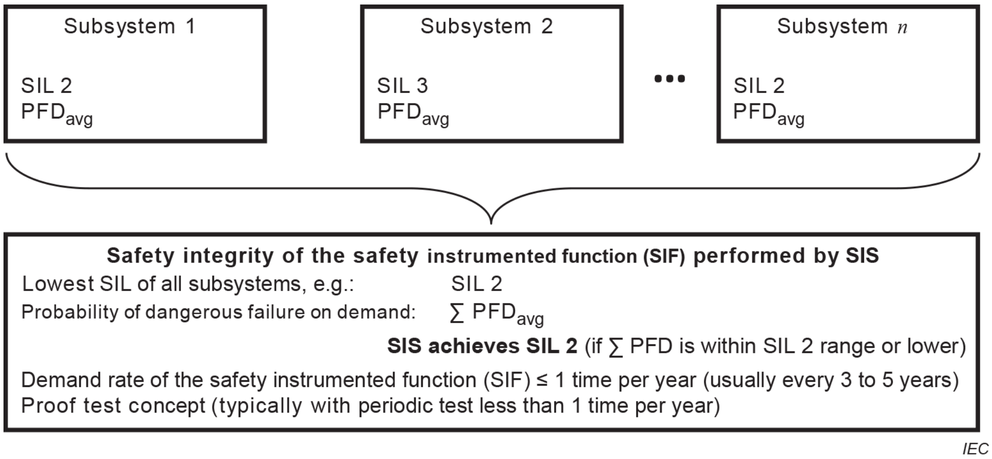


Figure J.2 – Basic approach in low demand mode of operation based on IEC 61508 (and IEC 61511)

J.2.2 Risk reduction measures on low demand mode of operation

In the context of safety instrumented functions (SIF) according to IEC 61511 (see also 5.3) and low demand mode of operation the following main aspects are relevant:

– Safety instrumented functions (SIF) implemented are mainly intended to protect the process and then the persons;

– Operators have detailed information of the design of the safety instrumented functions (SIF) and of the control system and the process control itself;

– The layers of protection approach can be used and, in this case, it takes into consideration the use and evaluation of the basic process control system (BPCS) performing the process control;

NOTE 1 While in low demand mode of operation the layer of protection can be used, for design and evaluation of safety functions in high demand mode of operation, no layers of protection are considered. The required SIL will not be affected by the machine control system or by the qualification of the operator.

– Demand rate of a safety instrumented function (SIF) can be low and is expected to be in an interval in terms of more than one or several years;

– Reaction time of safety instrumented function (SIF) is typically much higher than for safety functions in high demand mode of operation.

The concept used in the context of the process industry allows specific actions when a dangerous fault in a safety instrumented system (SIS according to IEC 61511) has been detected (by diagnostic tests, proof tests or by any other means) then compensating measures will be taken to maintain safe operation.

NOTE 2 The compensating measures required for continued safe operations can depend on safety integrity requirements, the tolerable risk associated with the hazardous event, the hardware fault tolerance of the SIS, the anticipated MRT ("mean repair time") and the availability of any other layers of protection. In some cases, it can be adequate to ensure action is taken to ensure repair of the dangerous failure within the assumed MPRT ("maximum permitted repair time") in the calculation of the PFD_{avg} but in other cases it can be judged necessary to provide other measures to compensate for the reduced risk reduction until the SIS is fully restored.

The fault handling approach used in the context of the safety of machinery for high demand mode of operation does not consider compensating measures: any dangerous fault detected in a subsystem designed with a hardware fault tolerance of 1 leads to a safe state. Only after reparation of faulty subsystem(s) can the machine operation be resumed again.

J.3 Use of subsystems in different modes of operation

J.3.1 General

Sometimes there is a need for incorporating a safety instrumented function (SIF) in low demand mode of operation in a safety-related control system that performs safety functions in high demand mode of operation implemented within the framework of ISO 12100.

The following information give guidance on how to design a safety instrumented function (SIF) by combining subsystems designed for low demand mode of operation with subsystems designed for high demand mode of operation.

The design of the subsystems is not within the scope of this Annex J and all information related to the integration of the subsystems (including the safety-related parameters) are assumed to be available.

J.3.2 Example with different modes of operation

The following examples according to ISO 13577-4:2022, Figure E.14 ("high temperature monitoring") and Figure E.17 ("low pressure monitoring") represent functional safety examples in context of industrial furnaces.

The following safety functions are considered:

– Safety function for "low pressure monitoring" in high demand mode of operation where two low pressure switches ("subsystem Input, pressure switches"), installed on a gas train trigger the closure of two on/off gas valves ("subsystem Output, valves"), installed on the same gas train;
– Safety instrumented function (SIF) for "high temperature monitoring" in low demand mode of operation where two thermocouples detecting a critical temperature value ("subsystem Input, thermocouples and TLC" designed in low demand mode of operation) trigger the two on/off gas valves ("subsystem Output, valves").

The required SIL for the safety instrumented function (SIF) in low demand mode of operation and the safety function in high demand mode of operation is supposed to be SIL 2.

NOTE 1 Annex A of IEC 62061:2021 provides a possible method to define a required SIL for safety functions.

The functional view is shown in Figure J.3, the logical view in Figure J.4 and the decomposition view in Figure J.5.

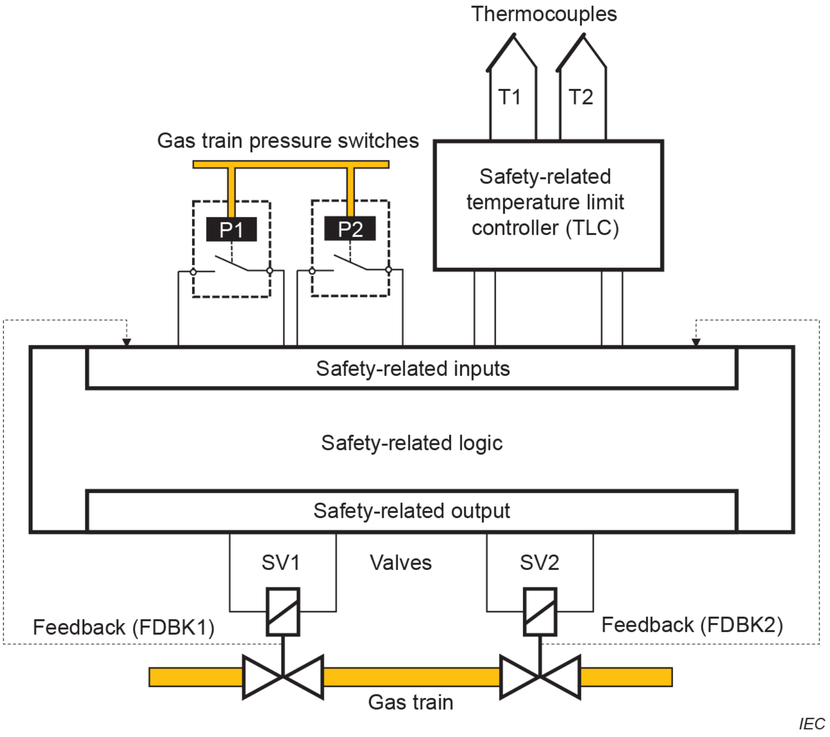


Figure J.3 – Functional view

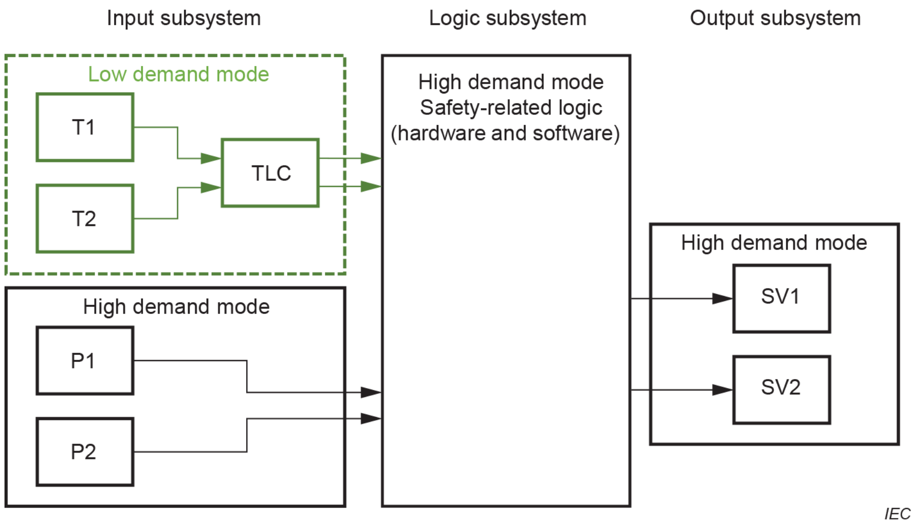


Figure J.4 – Logical view

NOTE The safety-related software design for low demand mode control system realized in the subsystem “Logic” will be different from the safety-related software of the subsystems used in high demand mode of operation. Both safety-related software parts will control the subsystem “Output”.

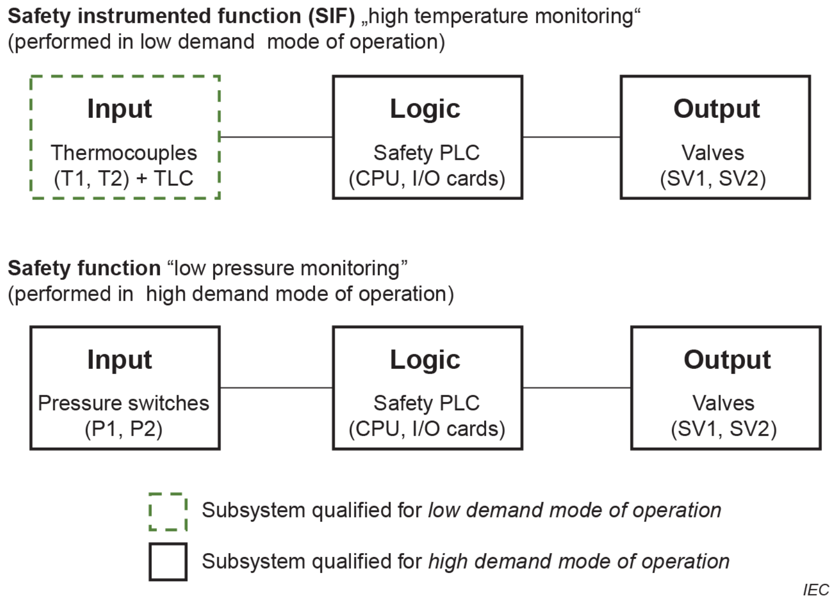


Figure J.5 – Decomposition view

J.3.3 Subsystem(s) used for different modes of operation

J.3.3.1 General

Figure J.5 shows the subsystem "Logic" and subsystem "Output" that will be used for both modes of operation.

A simple joint consideration of the entire safety-related control system would lead to problems because of the basic approach of low demand mode of operation and high demand or continuous mode of operation (e.g. PFH versus PFD_{avg}).

For the evaluation of the safety instrumented function (SIF) "temperature limitation" the following aspects will be taken into account:

– Hardware, software and systematic aspects will be considered separately for both modes of operation;

– The subsystem “Input” in low demand mode of operation will be evaluated by considering the basic safety principles, well-tried safety principles and, where applicable, well-tried components (see also ISO 13849-2:2012, Annexes A to D);

– The quantitative evaluation for the subsystem “Input” will be considered as described in J.3.3.2;

– For the subsystems "Logic" and "Output" there will be at least more than one demand per year to detect fault accumulation and undetected faults (see IEC 62061:2021, 7.3.3.4);

  NOTE 1 In the above example this is ensured since the subsystems "Logic" and "Output" are also used in the safety function "pressure limitation". In case of doubt, technical or organisational measures will be taken to ensure at least more than one triggering of the safety function per year.

– Subsystems used for high demand or continuous mode of operation will be not evaluated in the context of low demand mode of operation: safety functions and safety instrumented functions (SIF) are not designed and validated together but the overall software integration will be considered;

  NOTE 2 The subsystem "Input" will be evaluated as a subsystem of a safety instrumented function (SIF) in low demand mode of operation. The subsystems "Logic" and "Output" will be evaluated as subsystems of a safety function in high demand mode of operation. After the separate design and validation of both parts on subsystem level, the integration of all three subsystems is validated taking into account the interconnection and compatibility of the interfaces.

NOTE 3 The overall functional safety approach starting with the safety requirements specification, designing the safety-related control systems and validating the final solution will be applied for both modes of operations. The subsystems "Logic" and "Output" will be shared for both modes of operation and further investigations are necessary, e.g. regarding proof test, diagnostic functions and software implementation (see also type-C standard).

– The subsystems used for both modes of operation will achieve at least the same SIL in low demand mode and high demand or continuous mode of operation.

As there is no combination of different modes of operation, the safety function "pressure limitation" is completely evaluated in high demand mode of operation as required in IEC 62061.

In this example, since the "high temperature monitoring" (subsystem "Input") is operating in low demand mode of operation, it is evaluated as required in IEC 61511 or in IEC 61508.

J.3.3.2 Quantitative SIL evaluation (low versus high demand mode of operation)

The evaluation of the SCS based on the subsystems can be done as follows:

– For each subsystem, a quantitative "ratio of probability of failures" (RPF, expressed in percent) is determined with respect to the target SIL;

– The target SIL can be reached when the summation of these ratios of probability of failures is < 100 %.

Figure J.6 illustrates this approach.

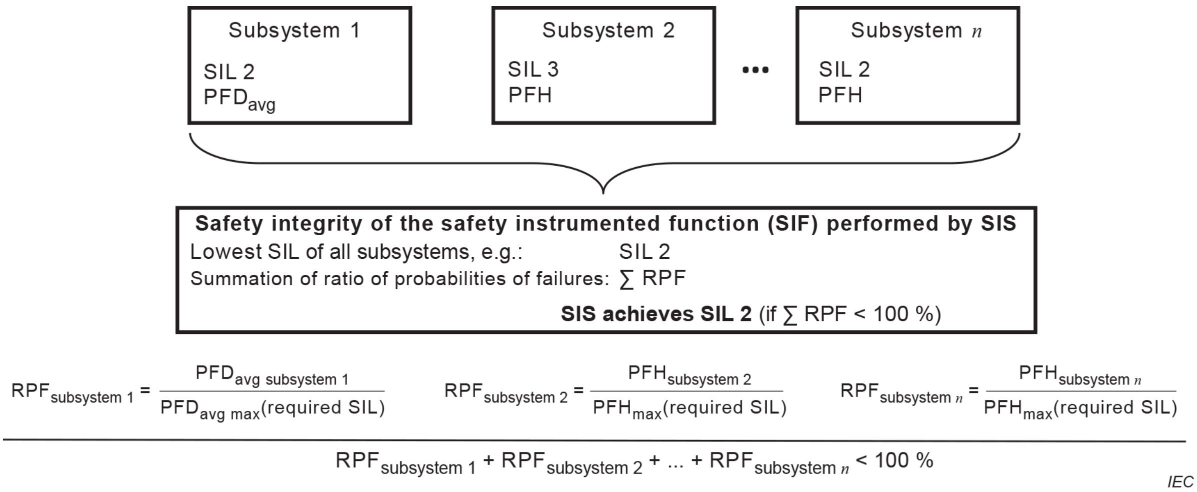
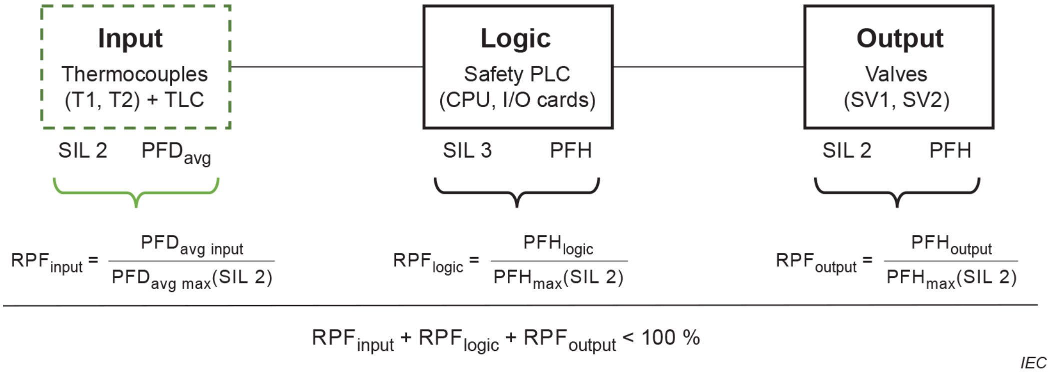


Figure J.6 – Quantitative SIL evaluation using the approach of ratio of probability of failures of each subsystem

J.3.3.3 Example of quantitative SIL evaluation (low versus high demand mode of operation)

Figure J.7 illustrates this approach for example with a target SIL 2 of the safety instrumented function (SIF).



NOTE The $PFD_{avg\ max}$ and PFH_{max} is SIL 2 in this example. Nevertheless, the PFH or PFD_{avg} of a subsystem can reach SIL 3.

Figure J.7 – Example of quantitative SIL evaluation using the approach of ratio of probability of failures of each subsystem

Table J.1 shows the maximum values for PFD_{avg} and PFH for respective target SIL.

Table J.1 – $PFD_{avg\ max}$ and PFH_{max} for respective target SIL

SIL	$PFD_{avg\ max}$	PFH_{max} [h^{-1}]
1	10^{-1}	10^{-5}
2	10^{-2}	10^{-6}
3	10^{-3}	10^{-7}

Bibliography

IEC 60204-1:2016, *Safety of machinery - Electrical equipment of machines - Part 1: General requirements*

IEC 60947-5-3:2013, *Low-voltage switchgear and controlgear - Part 5-3: Control circuit devices and switching elements - Requirements for proximity devices with defined behaviour under fault conditions (PDDB)*

IEC 60947-5-8:2020, *Low-voltage switchgear and controlgear - Part 5-8: Control circuit devices and switching elements - Three-position enabling switches*

IEC 60947-7-1, *Low-voltage switchgear and controlgear - Part 7-1: Ancillary equipment - Terminal blocks for copper conductors*

IEC 60947-7-2, *Low-voltage switchgear and controlgear - Part 7-2: Ancillary equipment - Protective conductor terminal blocks for copper conductors*

IEC 61000-6-7, *Electromagnetic compatibility (EMC) - Part 6-7: Generic standards - Immunity requirements for equipment intended to perform functions in a safety-related system (functional safety) in industrial locations*

IEC 61025:2006, *Fault tree analysis (FTA)*

IEC 61496-1, *Safety of machinery - Electro-sensitive protective equipment - Part 1: General requirements and tests*

IEC 61508-1:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General requirements (see* http://www.iec.ch/functionalsafety *Functional Safety and IEC 61508)*

IEC 61508-4:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations (see* http://www.iec.ch/functionalsafety *Functional Safety and IEC 61508)*

IEC 61508-5:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels (see* http://www.iec.ch/functionalsafety *Functional Safety and IEC 61508)*

IEC 61508-6:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3 (see* http://www.iec.ch/functionalsafety *Functional Safety and IEC 61508)*

IEC 61508-7:2010, *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures (see* http://www.iec.ch/functionalsafety *Functional Safety and IEC 61508)*

IEC 61800-5-2:2016, *Adjustable speed electrical power drive systems - Part 5-2: Safety requirements - Functional*

IEC 61511 (all parts), *Functional safety - Safety instrumented systems for the process industry sector*

IEC 61649:2008, *Weibull analysis*

IEC TS 62998-1:2019, *Safety of machinery - Safety-related sensors used for the protection of persons*

ISO 11161:2007, *Safety of machinery – Integrated manufacturing systems – Basic requirements*

ISO 13855:2010, *Safety of machinery – Positioning of safeguards with respect to the approach speeds of parts of the human body*

ISO 13856:2013, *Safety of machinery – Pressure-sensitive protective devices – Part 1: General principles for the design and testing of pressure-sensitive mats and pressure-sensitive floors*

____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
info@iec.ch
www.iec.ch