IEC TR 63161

Edition 1.0 2022-07

TECHNICAL REPORT

colour inside

Assignment of safety integrity requirements – Basic rationale

IEC TR 63161:2022-07(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 It also gives information on projects, replaced and withdrawn publications.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 TR 63161

Edition 1.0 2022-07

TECHNICAL REPORT

colour inside

Assignment of safety integrity requirements – Basic rationale

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 13.110

ISBN 978-2-8322-3944-5

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

ASSIGNMENT OF SAFETY INTEGRITY REQUIREMENTS – BASIC RATIONALE

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

IEC TR 63161 has been prepared by IEC technical committee 44: Safety of machinery – Electrotechnical aspects. It is a Technical Report.

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

Draft	Report on voting
44/935A/DTR	44/954/RVDTR

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 Report 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 publication 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

This document describes an example basic logical rationale for assigning a safety integrity requirement to a safety related control function in a risk based approach. The parameters for the assignment are explained. It is described how these parameters can relate to the risk assessment according to ISO 12100 and to the safety integrity requirement.

ASSIGNMENT OF SAFETY INTEGRITY REQUIREMENTS – BASIC RATIONALE

1 Scope

This document can be used where a risk assessment according to ISO 12100 has been conducted for a machine or process plant and where a safety related control function has been selected for implementation as a protective measure against specified hazards. This document describes an example basic logical rationale to assign a safety integrity requirement to the selected function.

The description is generic and as far as reasonably possible independent from any specific tool or method that can be used for assignment of a safety integrity requirement. The requirement can be expressed as a safety integrity level (SIL), or performance level (PL).

An example basic rationale is described that is embodied by such methods and tools, as far as they follow a risk based quantitative approach.

Conversely, the logic described in this document can be used as a reference for assessing specific methods or tools for safety integrity assignment. This can clarify how far the respective tool/method is following a risk based quantitative approach, and where deviations from that approach are imposed by other considerations. In real applications, the quantitative risk based approach can be modified or overridden by other considerations in many cases and for good reasons. It is not within the scope of this document to discuss or evaluate such reasons. Usually the reasons for deviations from a given tool or method from a quantitative logic are provided, so that this can be discussed in the proper frame.

Examples for such analyses are provided for common assignment tools in the format of risk graphs and risk matrices.

This document can be used for safety related control functions in all modes of application: continuous mode, high demand mode and low demand mode of application.

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.

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

3 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
probability
real number in the interval 0 to 1 attached to a random event and expressing quantitatively how likely the occurrence of that event is

Note 1 to entry: See 5.2.2 for more information.

[SOURCE: IEC 60050-103:2009, 103-08-02, modified – Notes 1 and 2 to entry have been removed and replaced with a new Note 1 to entry.]

3.2
event rate
frequency with the dimension of time^{-1}, typically given in the units h^{-1} or year^{-1}, attached to a random event and expressing quantitatively how frequently this event is expected to occur

Note 1 to entry: See 5.2.3 for more information.

3.3
tolerable risk
level of risk that is accepted in a given context based on the current values of society

Note 1 to entry: For the purposes of ISO/IEC Guide 51:2014, the terms "acceptable risk" and "tolerable risk" are considered to be synonymous.

[SOURCE: ISO/IEC Guide 51:2014, 3.15]

3.4
tolerable risk limit
risk which is accepted in the context of a given hazard of machinery or process equipment and which is quantified as an event rate for the occurrence of harm with a specified level of severity as a consequence of the hazard

Note 1 to entry: See 5.9.5 for more information.

Note 2 to entry: The harm with the specified level of severity is a necessary attribute of a tolerable risk limit, however it is not expressed in the limit itself.

Note 3 to entry: This definition adds the element of quantification to the general definition of "tolerable risk", which is not necessarily implied in the term "tolerable risk" without the modifier "limit".

3.5
hazardous event
event that can cause harm

Note 1 to entry: See 4.3.2 for more information.

[SOURCE: ISO 12100:2010, 3.9, modified – The note to entry has been removed and replaced by a new one.]

3.6
hazardous situation
circumstance in which a person is exposed to at least one hazard

Note 1 to entry: According to ISO 12100:2010, 3.10.

Note 2 to entry: See 4.3.2 for more information.

[SOURCE: ISO 12100:2010, 3.10, modified – The note to entry has been removed and replaced by two new ones.]

3.7
demand
<to a safety control function> event that causes the safety control system to perform the safety control function

Note 1 to entry: See 5.9.2 for more information.

[SOURCE: IEC 62061:2021, 3.2.25, modified – The abbreviated term "SCS" has been replaced by the words "safety control system", and "a safety function" has been replaced with "the safety control function".]

3.8
initiating event
<for a safety control function> situation which, without the safety function, will result in damage or harm of any sort or severity

Note 1 to entry: See 5.9.3 for more information.

3.9
safety demand
<for a safety control function> situation where, unless prevented by the safety control function under assessment, an accident with a specified level of harm to people would occur

Note 1 to entry: See 5.9.4 for more information.

3.10
hazard rate
rate of accidents of a specific severity in conjunction with a specific hazard that occurs although a safety control function has been installed to prevent this type of accident

3.11
probability of avoiding or limiting harm
probability that potentially exposed persons do not suffer harm of the specified level of severity during a hazardous event

Note 1 to entry: See 5.8 for more information.

3.12
avoidability
probability that potentially exposed persons avoid exposure to the hazard during a hazardous event

Note 1 to entry: See 5.8 for more information.

3.13
vulnerability
probability that exposed persons in a hazardous situation do suffer harm of the specified level of severity

Note 1 to entry: See 5.8 for more information.

3.14
hidden failure
hidden fault
failure or fault in hardware or software that does not announce itself and is not detected by dedicated methods when it occurs

Note 1 to entry: The term "hidden" in the given sense is complementary to the term "revealed" according to IEC 61511-1:2016, 3.2.13.

Note 2 to entry: A hardware or software failure or fault announces itself, e.g. by a disturbance of the equipment under control, its working process, or its surroundings.

Note 3 to entry: The "hidden status" of a hardware or software failure or fault is terminated when it is either detected by a dedicated check or method, or when it becomes overt by disturbing the equipment under control, its working process, or its surroundings. This may be related, e.g. to a change of the operation status or to a person approaching the equipment. Failures that stay "hidden" without termination are not relevant.

4 Risk based quantitative approach

4.1 General

In a risk based approach, a safety control function can be specified to keep a risk that is caused by a machine or process below a defined maximum level, the "tolerable risk limit".

The concept of "risk" is defined in ISO 12100:2010, 3.12 as "combination of the probability of occurrence of harm and the severity of that harm". Although both elements of the definition can be understood quantitatively, "risk" is not necessarily understood as a quantifiable parameter in the context of ISO 12100. That holds even more for the "tolerable risk", i.e. the risk which is accepted in a given context based on the values of society.

On the other hand, the efficiency of a safety control function for mitigating risk, often indicated as reliability of the control system, is described with the term "safety integrity". This expresses the degree of reliance that is put on a safety control function. "Safety integrity" has a quantitative aspect, which is clearly revealed by the complement of safety integrity, the unreliability of a safety control function. The unreliability is quantified as "target failure measure", i.e. either as average probability of the function to fail on demand PFD_{avg}, or as the rate of dangerous function failures per hour, PFH.

SIL assignment is the process of deriving a target figure for the failure measure of a safety control function from a risk assessment. As soon as a risk assessment is used as a basis for specifying a required level of safety integrity, it is implied that elements of this risk assessment are quantified. After all, a quantitative result is derived as output of the procedure and it is generally assumed that this is in a logical relation to the assumptions which were used as inputs.

Consequently, there is a basic logical rationale of functional safety assignment, which captures all relevant aspects of the application of a safety control function in quantified parameters and sets them in a logical relation to the tolerable risk limit and the target failure measure for the function.

NOTE Information on risk management can be found in ISO 31000:2018.

4.2 Sequence of steps in functional safety assignment

The following steps can be used to lead to a functional safety assignment in the context of a risk analysis for a machine or process. In this context, "SIL" is used as generic placeholder for any type of safety integrity indicator.

1) A hazard is identified by the analysis.
2) Accident scenarios with that hazard can be developed: It is stated which persons could suffer which type of harm, by which parts or functions of the machine, in which operation modes of the machine or process, etc. – see 4.3.2 for the elements of an accident scenario.
3) Mitigation measures can be devised conceptually. According to ISO 12100:2010, 6.1, the priority of measures decreases from inherently safe design measures (step 1) over safeguarding and/or complementary protective measures (step 2) to information for use (step 3). Safety functions are a form of "safeguarding and/or complementary protective measures".
4) The iteration of the overall design of the machine or process leads to the decision that an instrumented control function will be implemented. At the latest at this point, the functionalities of the control function are defined.

5) The safety related parts of the instrumented control function can be identified. With respect to the hazard in step 1 above, the function will be capable of preventing the given hazard from causing harm, if it works as devised.

NOTE 1 The required SIL is relevant for the functionality according to step 5. With this step 5, the preconditions for a SIL-assignment can be given. The following steps comprise the assignment in a strict sense. Typically, this can be done using a graphical tool, table or scoring system. The current description assumes that no such pre-designed tool is available, but the basic logic of the process can be followed in a "quantitative approach", meaning that the parameters are assigned numerical values and their relation to the "target failure measure" is expressed in explicit equations.

6) The severity class of the representative accident scenario can be determined – see 4.3.4.

7) The rate of initiating events for the accident scenarios can be determined – see 5.9.3.

8) From the risk analysis, the circumstances and conditions can be extracted, which could prevent an accident of the given severity or higher, once an initiating event is given, but without assuming the safety function as effective. These circumstances and conditions can be assigned to the factors P_r, F_r, or A_v and are estimated quantitatively (see 5.6, 5.7, and 5.8). Each of the given factors is a probability in the strict sense according to 5.2.2. Consequently, each of these parameters will be quantified as a real number, in the range of 0 to 1.

NOTE 2 In graphical tool and scoring methods, the numerical range is typically "discretized". This means only discrete values are used, each of which represents a certain range of the continuous range between 0 and 1.

9) The expected rate of accidents without safety function – the "safety demand rate" – can be determined according to Formula (4).

10) The expected rate of accidents with safety function – the "hazard rate" – can be determined according to Formula (6).

11) The allowable failure rate of the safety function PFH can be obtained from Formula (7). This implies that the expected rate of accidents is compared with a tolerable limit $L_{(S)}$ for the given severity class.

12) Demand mode assignment: Up to this point, the safety function has been treated as a function in high demand mode of application. Accordingly, the initiating event rate has so far not been used for determining the requirement. See Formula (7) in 6.2 and the explanation given there. Still, initiating event rate I_R and safety demand rate D_R can be determined:

- I_R and D_R are input for the decision between high demand mode of operation and low demand mode of operation.
- I_R is needed for specifying and/or evaluating the rates and reaction times of diagnostic measures.

With the information about initiating event rate I_R, safety demand rate D_R and other particulars of the application such as feasibility of regular proof tests, it can now be decided whether the function be treated as a function in a low demand mode of operation. See Clause 7.

NOTE 3 More information on demand rate and determination of the required SIL level can be found in IEC TR 63039:2016.

The flow chart in Figure 1 describes the steps above mentioned.

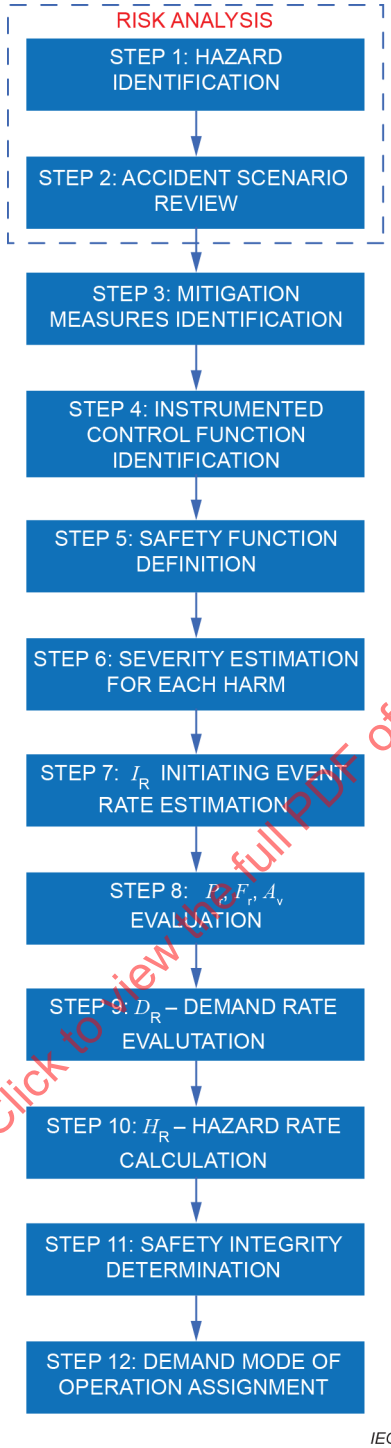


Figure 1 – Sequence of steps in functional safety assignment

NOTE 4 More information on techniques to be applied for the individual steps in Figure 1 can be found in ISO 31010:2019.

4.3 Reference information

4.3.1 General

The quantified parameters in a risk assessment are always related to reference information that is not in itself quantitative in nature. This information does not itself appear in the shape of parameters with a value in the risk assessment and SIL assignment. However, it provides the reference and justification for those parameters that can be quantified.

4.3.2 Accident scenario

A safety function can be defined as a safeguard against certain accidents. An "accident scenario" can be given as a short, generalized narrative that connects in a simple comprehensible story all the aspects that are common to the accidents under discussion. An accident scenario can identify:

- which type of machinery or equipment is involved in the accident;
- which aspect of the equipment or its operation is giving raise to the accident; what the "hazard" is; examples of how hazards can be described with their origin, consequences and situation sketches are given in ISO 12100:2010, Annex B;
- who can be affected, in which operation situation of the equipment;
- in which way people could be affected – which harm would they suffer, in which level of severity;
- which initial events can lead to the accident: failures of parts, human errors, and external influences?
- in which way would the event proceed from initial events to the final accidents; are there specific intermediate stages that could be identified as typical steps? Are there specific boundary conditions that influence the progress of events?

In the sequence of events of an accident scenario, two stages have specific definitions in ISO 12100. See also Table 1 in 5.10.

- Hazardous event: event that can cause harm (ISO 12100:2010, 3.9): This implies that the machinery does exert potentially dangerous effects to a "hazard zone", while the access of persons to that hazard zone is not prevented.
- Hazardous situation: circumstance in which a person is exposed to at least one hazard (ISO 12100:2010, 3.10): This is a "hazardous event" with the additional condition that a person is indeed situated entirely within the hazard zone or with body parts within the hazard zone.

4.3.3 Hazard zone

In the context of an accident scenario, the hazard zone can be given as the volume and/or ground in or around the machine where people could come into contact with the hazard caused by the machine. The hazard zone can be defined as reference for the "exposure parameter". See also ISO 12100:2010, 3.11.

4.3.4 Severity of harm

"Risk" is defined in ISO 12100:2010, 3.12 as a "combination of the probability of occurrence of harm and the severity of that harm". The "severity of harm" is generally expressed in "severity classes": S1, S2, and so on. These classes are defined each with an exemplary description of the harm, such as:

- Severity class S1: minor injury including scratches and minor bruises that require attention by first aid means without medical intervention;
- Severity class S2: reversible injury, including severe lacerations, stabbing, and severe bruises that requires attention from a medical practitioner;
- and so on.

It is generally avoided to express the "severity" quantitatively, with a number and a unit. Accordingly, it is not established practice to express risk in a specific unit either. Instead, the hazard and risk assessment identifies the applicable severity class as a qualitative descriptor of the risk. As such, the severity is a boundary condition of the quantitative assessment, however not explicitly included in it.

4.3.5 Safety control function

To assign a SIL, it would need to be known which types of accidents the function under assessment can prevent. The assignment of a SIL to a safety function is related to the risk that the safety function can mitigate. Therefore, a short functional description of the function would be used as a boundary condition for the assignment: for example, which signals at which levels or values trigger the function (process signals), what does it do (stop a certain movement, interrupt an electrical line, close a media line, bring something into a specific position, etc.).

5 Quantified parameters of a functional safety assignment

5.1 General

The parameters which are described in this Clause 5 describe either the frequency of certain events in time, or the likelihood of events under given initial conditions. These items can be quantified on a numerical scale.

5.2 Parameter types

5.2.1 General

Quantified parameters in risk estimation can be separated into two distinct types:

- as probability in a strict sense;
- as event rate.

For quantitative risk assessment and SIL assignment, this distinction can be seen as being essential.

5.2.2 Probability

A probability in a strict sense quantifies the expectancy that a given statement is true under given conditions. That can be expressed with a real number between 0 and 1, without unit.

EXAMPLE

How likely is it that a person will suffer at least a severe injury if it occurs inside a building when this building collapses?

Statement: A person will suffer at least a severe injury.

Precondition: The person is inside a building when it collapses.

The answer would be given in terms of a probability value:

0 would indicate that the collapse of the building would never inflict severe injuries or worse to the person inside the building;

1 would indicate that the collapse would inflict with certainty at least a severe injury.

In this example, the available information would not be sufficient to decide on a probability value with any confidence. The answer would depend critically, e.g. on the specifics of the building and the situation of the person inside it.

5.2.3 Event rate

An event rate can be used to quantify the expectancy of how frequently a given event will occur at a given time and a given reference frame. This is expressed as a ratio of the expected number of events to the length of the time. The dimension of an event rate is (time^{-1}), typically in the units 1/h or 1/year.

A failure rate, for example, is an event rate that quantifies for a specified equipment unit the expected number of failures in relation to the use time of that unit. The "reference frame" in that case is "one unit of the specified equipment". For an equipment failure rate, the reference frame is self-evident – "one unit of the equipment under investigation". Event rates in risk assessment are related to accident events. These may involve various persons and various pieces of equipment. Event rates can be quantified and are meaningful only if in these cases the "reference frame" is described sufficiently exactly.

5.3 Probability of occurrence of harm

The "probability of occurrence of harm" is generally expressed in the format "number of events connected with the given severity, per unit of time". This can be applied to a given scope of machinery or process. The given format can take the characteristics of an "event rate" as defined in 5.2.3. The "probability of occurrence of harm" is accordingly not a probability in a strict sense, it is rather an event rate. As such, the probability of the occurrence of harm is a function of other parameters. See Clause 8 for the relations.

5.4 Quantification of risk

With the understanding of severity of harm and probability of occurrence of harm as described in 4.3.4 and 5.3, the definition of risk in ISO 12100 can be expressed in a quantitative framework as follows:

$$R = S \times E_{\mathrm{R}} \tag{1}$$

where

R is the risk;

S is the severity;

E_{R} is the rate for the events under consideration with harm of the given severity.

With the severity as boundary condition, the "risk" is accordingly quantified as event rate.

Different levels of risk can be defined for a single risk assessment, depending on the risk mitigating measures and factors which are assumed. Where such assumptions are not related to different levels of severity, they can be quantitatively expressed in different event rates. Accordingly, different types of risk can be given as follows – each in relation to the relevant event rate:

- risk before mitigation by any factors: initiating event rate I_{R} (see 5.10);
- risk without safety function: safety demand rate D_{R} (see 5.9.4);
- risk "after" safety function: hazard rate H_{R} (see 3.10);
- tolerable risk: tolerable risk limit $L_{(\mathrm{S})}$ (see 5.10).

See also Figure 2.

5.5 Target failure measure

The "target failure measure" for a safety function can be given as the quantitative measure for the unreliability that is conceded to the function.

NOTE 1 The following definition of "target failure measure" is given in IEC 61508-4:2010, 3.5.17: target probability of dangerous mode failures to be achieved in respect of the safety integrity requirements.

Depending on the mode of application, continuous, high demand or low demand, the target failure measure can be defined either as event rate, or as probability in a strict sense as follows:

– High demand or continuous mode of operation: Failure rate of the safety function – PFH.

  PFH is the rate of dangerous failures of the safety function, which are not recognized and mitigated by diagnostics before an accident can occur.

– Low demand of operation: Average probability of failure on demand – PFD_{avg}.

  PFD_{avg} is the probability of finding the function dangerously failed as an average over time. The probability of a failure (PFD) is a function of time and fluctuates in the period of diagnostics tests and proof tests. Where mean periods between safety demands are sufficiently long in comparison with this rhythm, PFD can be represented by its average value over time, i.e. by PFD_{avg}.

A SIL or PL represents an interval on the scale of the target failure measure in discrete levels: SIL1, SIL2, SIL3 or PLa, PLb, and so on. Graphical methods for functional safety assignment do typically yield the required SIL or PL only, which is then understood as representing the limiting value of the respective interval, i.e. the allowable maximum.

For low demand, high demand, or continuous mode of operation, the target failure measure for the safety function can be quantified under consideration of risk reducing measures or circumstances, other than the safety function itself. Such "other" measures or circumstances can be represented in the factors P_r, F_r, or A_v, or can be already accounted for in the initiating event rate I_R, see 5.6, 5.7 and 5.8.

NOTE 2 More information on demand rates can be found in IEC TR 63039:2016 – Probabilistic risk analysis of technological systems – Estimation of final event rate at a given initial state.

5.6 Probability of occurrence of a hazardous event – P_r

A "hazardous event" is an "event that can cause harm" (see 3.5). As long as the safety function is functional, the hazardous situation can be prevented. As a necessary precondition for the hazardous situation, the safety function would need to have dangerously failed. However, not every failure of a safety function necessarily leads to a hazardous event. If, for example, a mechanical work piece fixation in a tooling machine is analysed as a safety function, a failure of this function can in many cases lead to the ejection of parts only within the space of guards. In these cases, there is no "dangerous effect" projected into a "hazard zone" that could be occupied by people.

Change "the hazardous event cannot occur" to "the hazardous situation will be prevented".

Example of assessment question: Assuming that the safety function has failed, how likely is it that a hazardous event occurs?

Example of assessment answer: "Probability of occurrence of a hazardous event" – parameter Pr. This is expressed as a probability, with a real number between 0 and 1:

0 means that the hazardous event will never occur as a consequence of a failure of the safety function.

1 means that the hazardous event will occur with certainty after each dangerous failure of the safety function.

A failure of the safety function may be detected before a hazardous situation occurs. It can be assumed that the dangerous operation of the machine will then be terminated, and this operation will not take up again before the safety function is restored. In this case, the failure of the safety function does not lead to a hazardous situation. The probability of that outcome is $(1 - P_r)$, i.e. the complement to P_r.

The parameter P_r includes the "diagnosis by the process" of the failure of the safety function. This means that a failure of the safety function can be detected by a disturbance of the process and the machine is put in a safe state before a hazardous event occurs. Typically, this applies to safety functions which also serve functions in the normal working process. If a safety function can fail without overt indications, the failure is "hidden". For "hidden failures", the parameter P_r is typically 1.

5.7 Exposure parameter – F_r

A "hazardous event" does not yet imply that a person is actually exposed to the hazard. Only in a "hazardous situation" is a person actually exposed to the potentially dangerous effects, i.e. to the hazard. This additional condition can be quantified with the exposure parameter F_r.

Example of assessment question: Assuming that the hazardous event is projected into a hazard zone, how likely is it that there is at least one person in the hazard zone at the same time?

Example of assessment answer: "Exposure parameter" F_r, expressed as a probability, with a real number between 0 and 1:

0 means there is never a person in the hazard zone at the same time as the hazardous event.

1 means whenever the hazardous event occurs there will be a person in the hazard zone, sooner or later, but in any case, with an overlap in time.

For quantifying the parameter F_r the work situation can be assessed considering factors such as:

- need for access to the hazard zone associated with the mode of operation (setting/automatic/manual/special mode);
- nature of access (feeding of materials, correction of malfunction, maintenance or repair);
- time spent in the hazard zone: t_F [h];
- frequency of access to the hazard zone: f_F [h^{-1}].

If the hazardous event is expected to occur in a single moment in time, such as for example, an explosion, the parameter Fr is equivalent to the likelihood that the danger zone is occupied in that moment. In this case, the parameter F_r can be defined by frequency of presence of people in the danger zone and by the average duration of presence:

$$F_r = f_F \times t_F \quad (2)$$

For hazardous events that last for an extended period of time, the exposure parameter will not be equal to the "time fraction of occupancy in the hazard zone". In a typical example, the hazard can be the contact between human and moving parts of the machinery during normal operation of the machine. Such hazards can be protected with light curtains, safety doors or analogous devices. Should a safety function of this type fail in a dangerous mode and undetected (no diagnostics), the machine can continue to operate normally. The failure of the safety function does not affect the operational functions of the machine. The failure is "hidden" – see 5.6. The "hazardous event" can escalate to a "hazardous situation" as soon as a person enters the danger zone, without being protected by the safety function. In these and analogous cases, the exposure parameter F_r can be set to 1, independently of frequency of access f_F and time spent in the hazard zone t_F.

In other words, if a hazardous event can last for extended periods of times in a zone that persons access regularly, the next person accessing after failure of the safety function will be exposed to the hazard. Under these boundary conditions, the absence of persons at the moment of failure of the safety function does not reduce the risk. (There may still be a chance that the failure will be detected and the engine will be stopped before a person enters the danger zone. This can be accounted for in the parameter P_r, probability of occurrence of a hazardous event.)

5.8 Probability of avoiding or limiting harm – A_v

5.8.1 General

A "hazardous situation" implies that a person is actually exposed to the hazard. However, it does not yet imply that the person actually suffers harm. The exposed person could recognize the situation and avoid harm by his/her own dedicated actions. The exposed persons could also escape from harm by sheer luck. These additional conditions can be quantified with the probability of avoiding or limiting harm – parameter A_v.

Example of assessment question: Assuming that a person is exposed to the hazardous event in the hazard zone, how likely is it that the person will actually suffer the harm?

Example of assessment answer: "Probability of avoiding or limiting harm" – parameter A_v, expressed as a probability, with a real number between 0 and 1:

1 means that the exposed person will always avoid the dangerous effect and never suffer the harm.

0 means that the exposed person will suffer the harm in each case.

Note that in relation to the risk, the polarity of the parameter A_v can be inverted with respect to the polarity of the parameters P_r and F_r. While for P_r and F_r, the value 1 indicates the "high risk end" of the scale, for the parameter A_v it would be the other way round. Accordingly, in the final evaluation, the complement of A_v can be used: $1 - A_v$.

The parameter A_v according to 5.8 combines two aspects of avoidance:

- avoidance of harm by dedicated actions of the person who is exposed to a hazard;
- avoidance of harm by favourable circumstances or sheer luck.

These two aspects can be expressed separately. The first aspect can be assigned to a parameter "avoidability" (A) and the second aspect can be assigned to a parameter "vulnerability" (V).

If the vulnerability is used as a separate parameter in a SIL assignment, the parameter A_v according to 5.7 would be substituted by A and V as follows:

$$(1 - A_v) = (1 - A) \times V \tag{3}$$

5.8.2 Vulnerability (V)

The vulnerability can be given as the probability that exposed persons in a hazardous situation suffer harm of the specified level of severity.

Vulnerability parameter V can represent the avoidance of harm by favourable circumstances or by sheer luck.

For the following aspects of a hazardous situation, it can be suitable to use the "vulnerability" as a specific parameter:

- toxicity and/or concentration of a release of harmful substances, for example, smoke gases in a fire scenario or general chemical substances in a chemical industry accident scenario.
- chances of being hit by projectiles in scenarios that involve the mechanical disintegration of fast-moving machinery.

Example of assessment question: If a person is exposed to the hazardous event in the hazard zone and does not do anything to avert or mitigate the exposure, how likely is it that the person will actually suffer the harm?

Example of assessment answer: "Vulnerability" – parameter V, expressed as a probability, with a real number between 0 and 1:

0 means that the exposed person will never suffer the harm in the specified severity, even if exposed to the hazard;

1 means that the exposed person will suffer the harm in the specified severity in each case of exposure to the hazard.

5.8.3 Avoidability (A)

The avoidability (A) can be defined as the probability that potentially exposed persons avoid exposure to the hazard during a hazardous event.

Example of assessment answer: "Avoidability"– parameter A, expressed as a probability, with a real number between 0 and 1:

1 means that the exposed person will always avoid the dangerous situation.

0 means that the exposed person will never avoid the dangerous situation.

For the case of "hidden failures", the value that can be assumed for the parameter A is subject to an analogous boundary condition as applies to P_r and F_r: the avoidance of harm can be accounted for as risk reduction only under the assumption that the failure of the safety function is recognized and the situation is restored to safety as a consequence of the exposure. If the assessment leads to the result that the harm could be avoided by "sheer luck" without even being noticed, the respective likelihood cannot be claimed for the parameter A. These occurrences would again only delay the proceeding of events, but not prevent the harm.

The fact that a failure is hidden would not automatically mean that the value of the parameter A were equal to 0 if a subsequent hazardous event could help to reveal it.

EXAMPLE: In the case of overspeed, prevention is not possible, as the event involving harm happens so quickly that typically neither the event itself nor its effects can be averted by human actions. The probability of avoiding the hazardous event would therefore be 0.

5.9 Demand types and related event rates

5.9.1 Event classes

The term "demand to a safety function" can describe different classes of events. Event descriptions could be, for example:

1) The predetermined conditions for triggering the safety function can be given. In the example of a light curtain that is protecting against contact with the moving parts of cutting machinery, this event description would apply to an intrusion of an object or body part in the plane of the curtain, sufficient in width and in time duration to trigger the function.

2) The predetermined conditions for triggering the safety function can be given in a situation, where the safety function is needed to prevent damage or harm of any nature. In the given example, that would apply if an object or body part penetrates the plane of the curtain so deeply that it will actually come into contact with the moving parts of the machinery. With respect to the above item 1, this excludes in first instance the safety margins.

3) The predetermined conditions for triggering the safety function can be given in a situation where the safety function is needed to prevent harm to people, and the harm would be at least at the severity which is assumed for the SIL assignment. In the given example, that would apply to a situation where a human hand is extended to the moving parts so that the hand or parts of it would be severed if the machine is not stopped in time.

The event descriptions above increase in specificity from item 1 to item 3. Each class of events in the given sequence can be included as a subset in the preceding class of events. Accordingly, in general the event rates decrease for the event types in the sequence from 1 to 3. For each of the related events, a specific definition is given by way of example in this document:

– "demand" according to 3.7 and 5.9.2;

– "initiating event" according to 3.8 and 5.9.3;

– "safety demand" according to 3.9 and 5.9.4.

5.9.2 Demand and demand rate

"Demand" and "demand rate" can apply to any situation which triggers the safety function in a given application. The demand rate in this sense is not a direct measure of the actual risk of accidents in that application. The triggering rate of the safety control function can also be determined by restrictions of the instrumentation and by safety margins that can be applied to the trigger limits. Therefore, the rate of "demands" according to 3.7 would not generally be suitable as input for the SIL assignment.

5.9.3 Initiating events and rate of initiating events I_R

An initiating event can be given as a situation that will result in damage or harm of any sort if it is not prevented by the safety function. This would include all cases of potential damage to equipment and production and all minor harm that would need to be prevented by the safety function without being specifically addressed in the SIL assignment.

Initiating events can be related to the following causes:

- disturbances or failures: mechanical failures of the equipment, failures of actuators such as motors or pneumatic/hydraulic actuators, external influences (e.g. power supply fluctuations), human errors in controlling the equipment;
- the nature of the working process of the machine itself: movement of cutting or pressing parts, direct interaction of machine parts with humans in the working sequence of the machine, direct interactions of machine parts with humans during charging/discharging, setting operation or maintenance;
- failure of a continuous control function that is required to prevent the machine from immediately creating a hazard.

The above-mentioned initiating event causes are typical for low demand applications, high demand applications and continuous demand in the sequence of the bullets. The frequency of occurrence can be described by an event rate, the "rate of initiating events", denoted as I_R.

A safety function is generally designed to recognize initiating events and to react on them. It is assumed that each initiating event will trigger the reaction of the safety function, as long as the function works.

Where the consequences of initiating failures are mitigated by factors that are regarded as inherent to the machine and/or its working process, these factors can also be accounted for in the initiating event rate. For example, where the exposed person is not the operator of the machine (typical in process industries), the actions of the operator that prevent hazardous events can be typically factored in the initiating event rate $I_{R,}$ rather than in the avoidability factor A_v.

Where a safety function is designed to prevent humans from coming into contact with the moving machinery, the initiating event can be defined by either the hazardous movements of the machine or the hazardous movements of the exposed human – whichever would be assumed to trigger the safety function.

5.9.4 Safety demands and safety demand rate D_R

A safety demand can be defined as a situation where an accident with a specified level of harm to people would occur unless prevented by the safety control function under assessment. Accordingly, the related event rate D_R can be defined as the rate of accidents of the specified type, with the specified level of harm to people that would occur if the safety function were not present.

Safety demand and safety demand rate can be given a specific meaning in the context of a risk assessment, which is used as a basis for a SIL assignment and which assumes a specified level of harm to people as an element of the accident scenario. In this context, the function is "demanded" with the same frequency, as it actually has to prevent the specified accident.

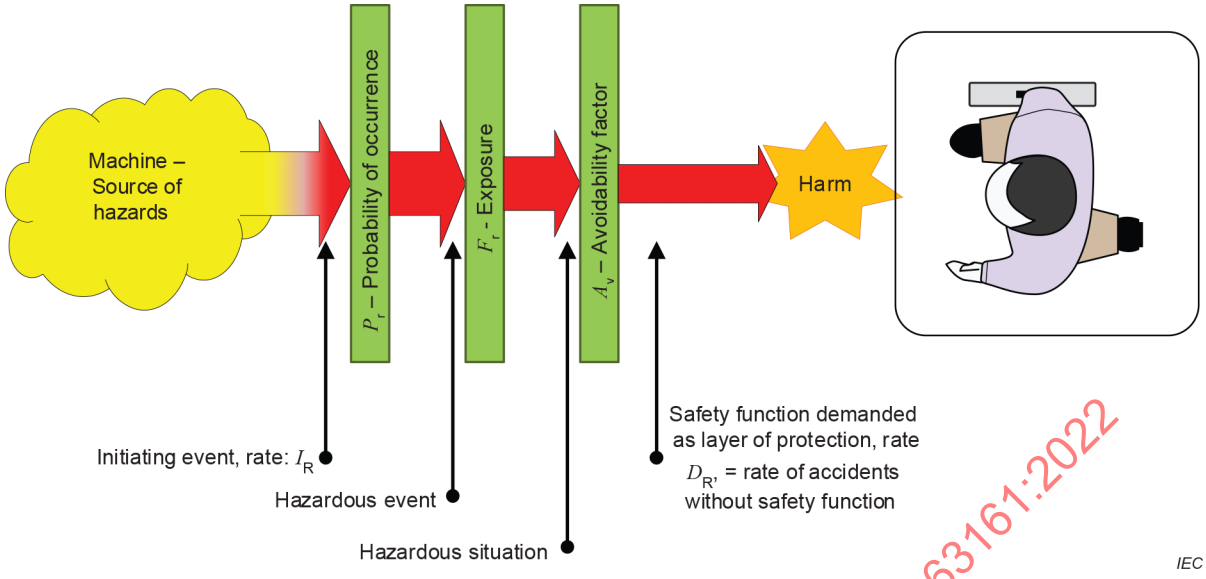
The safety demand rate D_R can be derived from the rate of initiating causes, by applying any risk reduction that may be claimed for the factors P_r, F_r, or $(1 - A_v)$. In order words, the safety demand rate D_R to a safety function would be the rate of initiating events I_R reduced by the overall probability that the specified harm to people is avoided and that the machine is put in a safe state, without assuming the intervention of the safety function. This can be written as a formula:

$$D_R = I_R \times P_r \times F_r \times (1 - A_v) \quad (4)$$

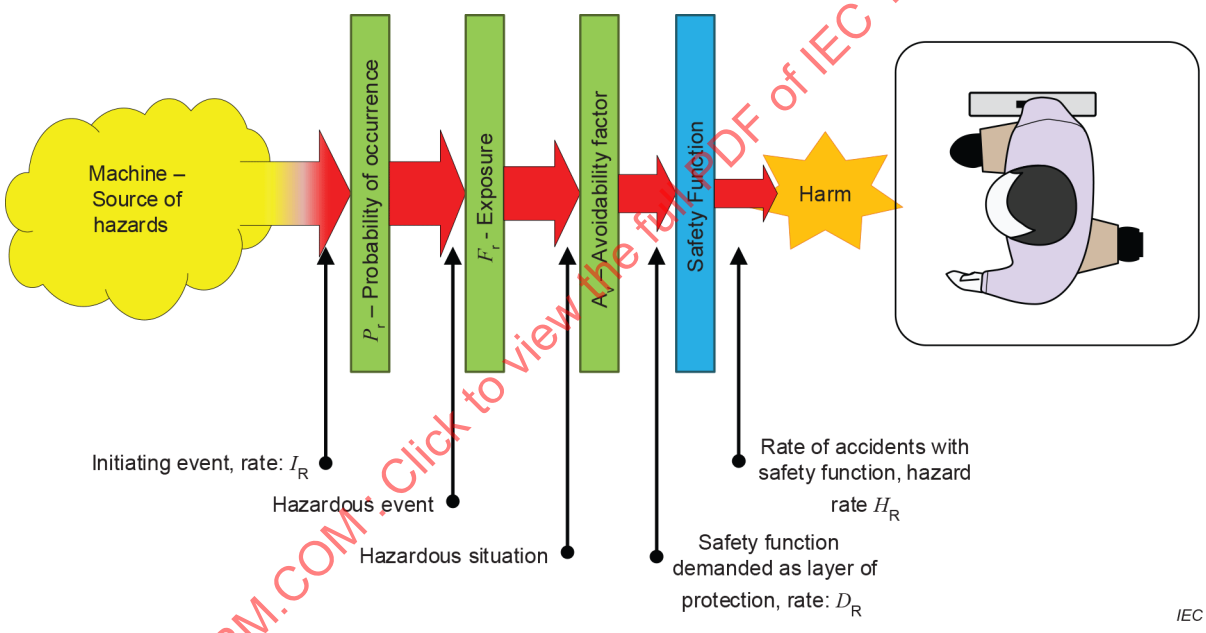
In Formula (4), I_R is the rate of initiating events. In the event of an initiating event, the accident could be prevented by factors expressed in $P_r \times F_r \times (1 - A_v)$. If the accident is not prevented by these other factors, it would be prevented by the safety function.

The risk which is remaining with D_R as event rate is the risk that would be mitigated by the safety function.

See Figure 2 for a representation of initiating events and demands with the related event rates in a "risk model".



a) Situation without safety function



b) Situation with safety function

Figure 2 – Protection layers, event rates and their relation

The single protection layers are shown from left to right in the sequence, in which they are regarded in a SIL assignment. In a real sequence of events, the safety function would take the first position on the left side, immediately reacting on initiating events. See 3.10 for I_R, 4.3.2 for "hazardous event" and "hazardous situation", and 5.10 for H_R, the "hazard rate".

5.9.5 Tolerable risk limit – Parameter $L_{(S)}$

For accidents of a given severity, there is a maximum event rate that would be allowed in the frame of a risk assessment. This corresponds to a maximum tolerable risk:

$$L_{(S)} = S \times E_{RMAX} \quad (5)$$

where

$L_{(S)}$ is the tolerable risk limit for the given severity;

S is the severity;

E_{RMAX} is the maximum allowable event rate for the given severity.

For each level of severity of an accident event, a "tolerable risk limit" is needed. It can be defined by Formula (5). $L_{(S)}$ can be given as an event rate, with the dimension of events per time (time^{-1}), typically in the unit 1/year.

The higher the severity class of an accident, the lower the numerical value of the corresponding risk limit $L_{(S)}$ can be. Typically, the values $L_{(S)}$ for a series of severity classes are placed in equal steps on a decadal logarithmic scale, for example 10 per year for severity S1, 10^{-1} per year for severity S2 and so on. Less severe accidents are tolerated more frequently than accidents with higher severity.

The tolerable risk limit is typically not explicitly indicated on graphical tools for SIL-assignment, although it can frequently be derived from such graphs. It is logically not possible to derive a requirement for risk reduction from risk estimation, without implying a tolerable risk limit.

5.10 Additional parameters

The following additional parameter definitions can be useful to express the logic of a SIL assignment in the form of equations, i.e., in a logically exact manner:

H_R Rate of accidents that occur, even though the function is installed. This is frequently called "hazard rate" in the pertinent literature;

T_R Proof test rate of a safety function;

T_I Proof test interval of a safety function, inverse to the proof test rate T_R = 1/ T_I;

D_I Average time between safety demands to the safety function;

PFD_{avg} Probability of a safety function failing on demand;

RRF Risk reduction factor: Ratio of the rate of accidents that would occur without the safety function to those that would occur with the safety function. RRF can also be defined as a requirement RRF_{req}. In this case, the denominator can be given by the tolerable risk limit: $RRF_{req} = D_R/L_{(S)}$.

Where a safety function is in a low demand mode of application, so that it can be assigned a PFD_{avg} (average probability of failing on demand), the risk reduction factor can also be expressed as the inverse of PFD_{avg}: RRF = 1 / PFD_{avg}.

These definitions are included here for the sake of completeness; however they are not further used in this document.

Table 1 – Parameters overview

Symbol	Parameter	Meaning	Dimension
PFH	Probability of dangerous failure per hour	Rate of failures of the safety function in high demand or continuous mode that results in an increase of the risk under assessment (see 5.5).	Event rate n / time
PFD_{avg}	Average probability of failing on demand	Applicable to a safety function in low demand mode of operation only: Probability of finding the safety function in a failed state, as an average over time (see 5.5).	No dimension, real number between 0 and 1
P_r	Probability of occurrence of a hazardous event	Probability that a hazardous event occurs as a consequence of the failure of the safety function (see 5.6).	No dimension, real number between 0 and 1
F_r	Exposure	Probability that at the time of the hazardous event a person is in the danger zone (see 5.7).	No dimension, real number between 0 and 1
A_v	Probability of avoiding or limiting harm	Probability that potentially exposed persons do not suffer harm of the specified level of severity during a hazardous event (see 5.8).	No dimension, real number between 0 and 1
A	Avoidability	Probability that potentially exposed persons avoid exposure to the hazard during a hazardous event (see 5.8.3).	No dimension, real number between 0 and 1
V	Vulnerability	Probability that exposed persons in a hazardous situation do actually suffer harm of the specified level of severity (see 5.9).	No dimension, real number between 0 and 1
I_R	Initiating event rate	Rate of events which triggers the safety function because the status of the machine by itself or the positions of persons in relation to the machine bear the potential for harm (see 5.9.3).	Event rate n / time
D_R	Safety demand rate	Rate of events where harm would occur without intervention of the safety function (see 5.9.4).	Event rate n / time
D_I	Safety demand interval	Average period between two safety demands to the safety function	time
S	Severity class	S is an indicator for the magnitude of harm that is inflicted by a single typical accident with the hazard in question (see 4.3.4).	No unit – qualitative description only
$L_{(S)}$	Tolerable risk limit	Maximum allowable average frequency for an event of the severity S due to the hazard in question (see 5.9.5).	Event rate n / time
H_R	Hazard rate	Rate of actual accidents inflicting the expected harm (see 3.10).	Event rate n / time
T_I	Test interval	Proof test interval of a safety function – only relevant in a low demand mode (see 5.10).	time
T_R	Test rate	Proof test rate of a safety function – only relevant in a low demand mode (see 5.10).	Event rate n / time
RRF	Risk reduction factor	Ratio of the rate accidents that would occur without safety function, to those that occur with safety function – only relevant in a low demand mode (see 5.10).	No dimension – positive real number > 1

6 General principle of functional safety assignment

6.1 Basics

6.1.1 Applicability to complete functions

A functional safety assignment that is derived from a risk assessment applies always to an entire safety function. Only the entire function including all subsystems is capable of mitigating risk. To assign a SIL to a subsystem of the entire safety system, the maximum allowable unreliability for the entire system would need to be considered and divided into portions for each subsystem.

6.1.2 Risk relation

The higher the risk that can be assigned as "mitigation target" to the safety function, the more stringent the safety integrity requirement to the function. The proportionality between risk to be covered and required safety integrity can be defined by the tolerable risk limit $L_{(S)}$.

The safety integrity requirement to a safety function becomes more stringent with increasing probability of the hazardous event P_r, and with increasing exposure parameter F_r. It becomes less stringent with increasing value of the probability of avoiding or limiting harm A_v and with increasing value of the tolerable risk limit $L_{(S)}$. ($L_{(S)}$ is itself "less stringent" with a numerically higher value.) This is easier and more exactly expressed in simple formulae – see 6.2, 6.3 and Clause 7.

6.1.3 Logical independence of parameters

A single factor or circumstance is accounted for only once in the overall assessment. That is also frequently expressed as a requirement for the "independency of protection layers".

It is not always unambiguous as to which parameter a specific element of an accident scenario is assigned. For example, the presence of a person can be expressed as a condition of the initiating event in I_R or in the parameter F_r – see 5.7. Likewise, risk mitigating actions of operators can be expressed in I_R (when the operator is not the exposed person) or in A_v (when the operator is the exposed person). Specific methodologies and tools may also be differentiated in this respect.

6.2 High demand or continuous mode of operation

For a safety function in high demand or continuous mode of operation, the above principles are expressed as follows.

The hazard rate H_R can be given as follows:

$$H_R = \text{PFH} \times P_r \times F_r \times (1 - A_v) \quad (6)$$

In Formula (6) above, the relation H_R = PFH can be obtained from the Henley / Kumamoto equation $H_R = \text{PFH} \times (1 - e^{-D_R \times T_I/2})$. This follows with the assumption that the safety demand rate (D_R) × proof test interval (T_I) is significantly greater than 1.

Accordingly, the safety function with PFH would need to satisfy the following condition:

$$\text{PFH} \times P_r \times F_r \times (1 - A_v) \leq L_{(S)} \quad (7)$$

The "rate of initiating events" I_R as discussed in 5.9.3 does not appear in Formula (6). The reason is that two conditions are always necessary for a hazardous event:

- An initiating cause is present and not mitigated by a protective measure or "layer of protection" other than the safety function. The related event rate is I_R.
- The safety function has failed. The related event rate is PFH.

In a "high demand or continuous mode of operation", the overall event rate for concurrence of both of the above is entirely dominated by the second, the failure of the safety function with the rate PFH. The hazard rate H_R is limited by the dangerous failure rate of the safety function.

Assume the safety function has failed, and that failure is not revealed by an overt process disturbance – factor P_r – or by the observation of an attentive operator or bystander – factor $(1 - A_v)$. In this case, the failure of the safety function will stay hidden, until the next initiating cause leads to a hazardous event. Depending on the application, the next hazardous event can occur a few seconds or a few weeks later. This is a huge variation in rate of initiating events I_R. However, in relation to the typical time between failures of a safety function, the typical time to the next initiating event does not make a difference. In a high demand mode of operation, the rate of accidents can be determined by the rate of safety function failures, according to Formula (6). This is also the case with the continuous demand mode.

6.3 Low demand mode of operation

For a safety function in low demand mode, the above principles can be expressed with:

$$H_R = \mathrm{PFD}_{avg} \times D_R = \mathrm{PFD}_{avg} \times I_R \times P_r \times F_r \times (1 - A_v) \quad (8)$$

and

$$\mathrm{PFD}_{avg} = 1/2 \times \mathrm{PFH} \times T_I = \mathrm{PFH} / (2 \times T_R) \quad (9)$$

Formula (7) can be given for a single channel function with a single proof test interval. For general function this and the derived formulae can be generalized accordingly. In the given context, this specific case sufficiently supports all conclusions.

The relation $H_R = D_R \times 1/2 \times \mathrm{PFH} \times T_I$ can be obtained from the Henley / Kumamoto equation $H_R = \mathrm{PFH} \times (1 - e^{-D_R \times T_I/2})$. This follows with the assumption that the safety demand rate (D_R) × proof test interval (T_I) is significantly lower than 1.

The safety function with PFD_{avg} would need to satisfy the following condition:

$$\mathrm{PFD}_{avg} \times I_R \times P_r \times F_r \times (1 - A_v) \leq L_{(S)} \quad (10)$$

7 Assignment of the demand mode

7.1 Demand mode – General

That a safety control function is treated as a function in low demand mode of operation means essentially that the overall quantification of risk accounts for proof testing. If proof testing is frequent enough with respect to the rate of demands, it allows to detect failures of the safety function before a demand occurs. Accounting for the proof test essentially distinguishes the low demand mode of operation on the one side from the high demand or continuous mode of operation on the other side. According to the basic logical rationale, the safety function can be treated as a function in:

- low demand, if a regular proof test interval is sufficiently short with respect to the average period between demands;
- high demand or continuous demand, if that is not the case.

For a single channel with a single proof test interval, the threshold ratio of event rates can be derived by inserting the defining formula for PFD_{avg} Formula (9) in the calculation of the hazard rate Formula (8). Re-sorting the parameters yields

$$H_R = PFH \times [I_R / (2 \times T_R)] \times P_r \times F_r \times (1 - A_v) \quad (11)$$

Formula (11) applies directly to the low demand mode of operation. It is identical with the analogous Formula (6) for the high and continuous demand of operation, except for one additional parameter on the right side: $I_R / (2 \times T_R)$.

This parameter can be named "proof test factor" PTF:

$$PTF_{lin} = I_R / (2 \times T_R) \quad (12)$$

The proof test factor can be used to describe the risk reduction by proof testing. The proof test begins to become effective if the proof test frequency is in the order of magnitude of the initiating event. The more proof testing reduces the risk with safety function failures, the more frequently it occurs in relation to initiating events. The proof test factor would attain a value of 1 or higher if the initiating event rate is too high in comparison with the proof test rate, or if there is no proof testing at all. The transition point between Formulae (6) and (8) above can be determined by:

$$I_R / (2 \times T_R) = 1, \text{ or } I_R = 2 \times T_R \quad (13)$$

If the initiating event rate is higher than twice the proof test frequency, the proof test factor would not be used anymore. That is equivalent with using it with a value of 1.

The formulae in Clause 6 are approximations describing cases which are either strictly high demand/continuous demand, or strictly low demand. Real statistics do not discontinuously change from one type of statistics to another. Consequently, there is another generalized expression for Formulae (6) and (9), describing a smooth transition. This transition is frequently described with the Henley / Kumamoto equation in the literature. Adapted to the current notation, this would give:

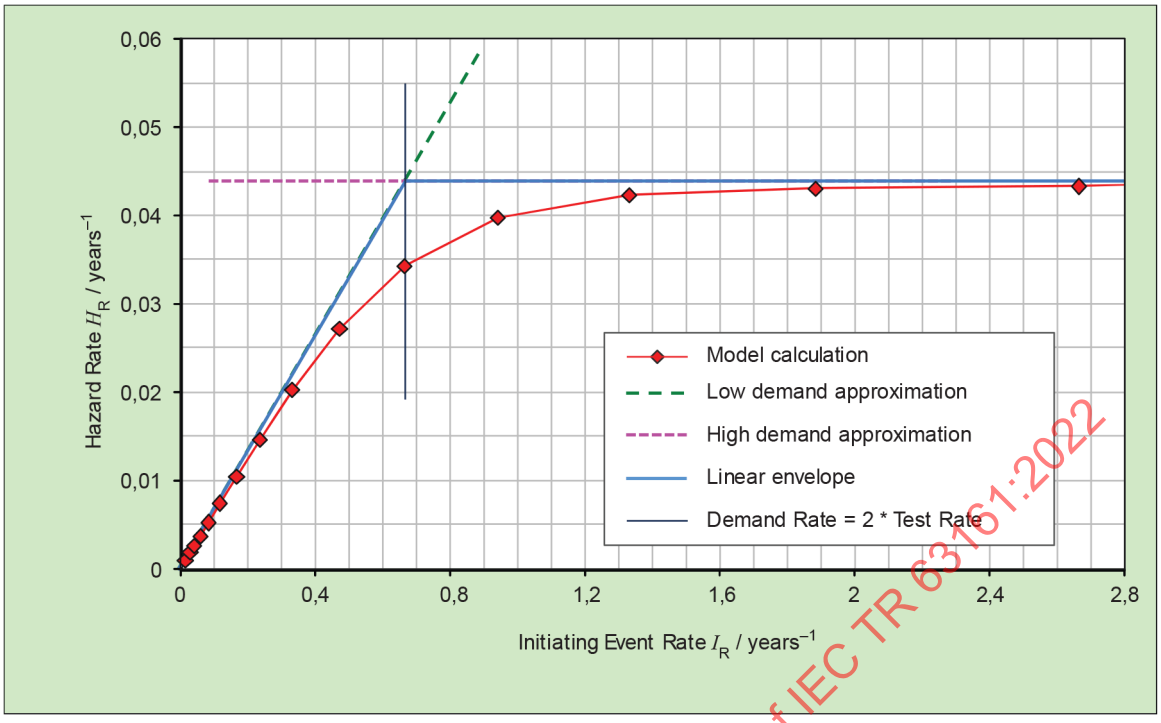
$$PTF_{H\&K} = 1 - e^{-D_R \times T_I/2} \quad (14)$$

Using the Henley / Kumamoto equation for the proof test factor yields for the hazard rate H_R:

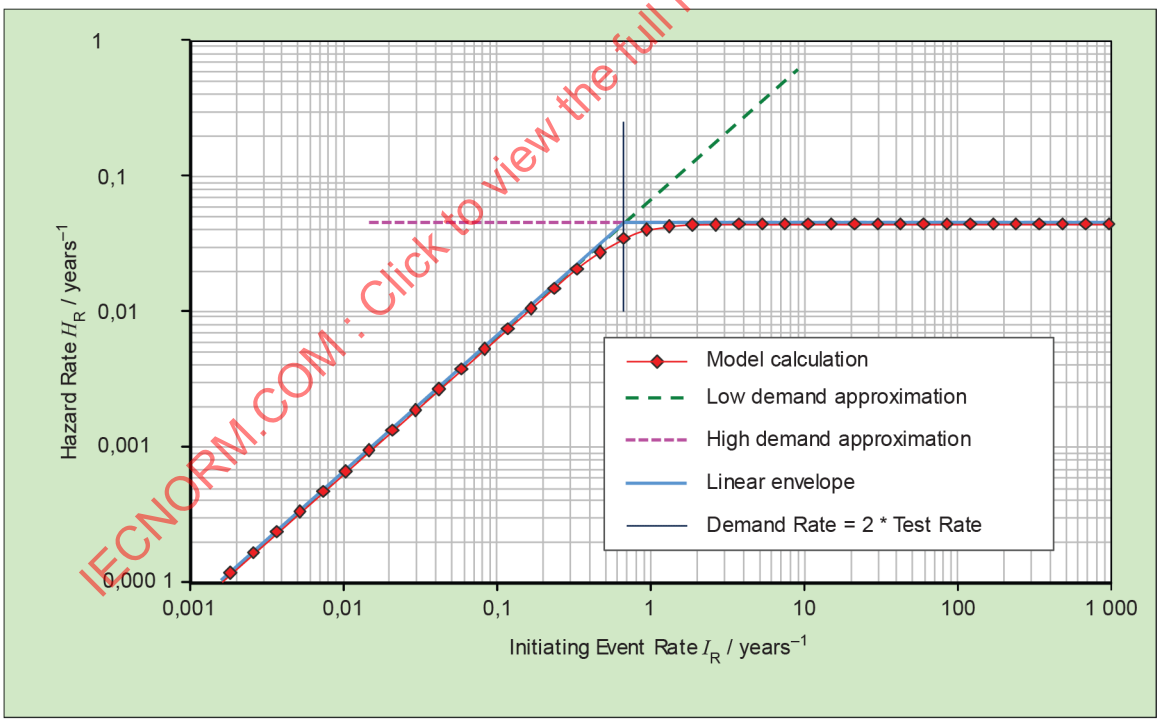
$$H_R = PFH \times [1 - e^{-D_R \times T_I/2}] \times P_r \times F_r \times (1 - A_v) \quad (15)$$

In Formula (15), the approximations for high/continuous demand and low demand are generalized in a single expression. For practical application, it would be sufficient to use one of the two boundary case approximations according to 6.3 (low demand) or 6.2 (high/continuous demand), whichever is more suitable. The criteria are given in 7.2.

Figure 3 illustrates an example model calculation for a single channel safety function with a dangerous failure rate PFH of 5 × 10^{-6}/h (corresponding to 0,044/year) and test rate T_R 1/3 years.



a) Linear scales



b) Logarithmic scales

Figure 3 – Hazard rate according to the Henley / Kumamoto equation

7.2 Assignment criteria

The safety function can be treated as a function of low demand mode of operation, if both of the following in a) and b) applies. If either a) or b) does not apply, the applicable mode of operation is high demand or continuous demand.

a) Proof tests at regular intervals are foreseen and practicable in the use environment of the safety function.

b) The proof test interval is no longer than twice the average period between "initiating events": D_R / $2T_R$ < 1, then D_R < $2T_R$ or T_I < 2 D_I.

IEC 61508-4 and safety standards derived from this basic safety publication define another criterion:

c) The safety function can be treated as a function in low demand mode, if the "demand rate" is less than once per year. See for example in IEC 61508-4:2010, 3.5.16.

This is a bit unclear insofar as the term "demand rate" is not defined in IEC 61508-4. It could be any of the three definitions identified in 5.10. Whichever of these definitions is finally used, a limit of "once per year" for distinguishing the demand rate as "high/continuous" or "low" cannot be derived from the consideration of the basic rationale.

There is an upper limit for the proof test rate that can be reasonably implemented in a given application of a safety control function. Assuming that the "demand rate" as devised in IEC 61508-4 can be best expressed with the initiating event rate according to 5.9.3, the proof test factor I_R / (2 × T_R) would relate the limit of 1 per year for the demand rate to a maximum viable proof test frequency of ½ per year, i.e., one proof test every two years. Accordingly, proof tests more frequently than once every two years would not be regarded effective for detecting safety function failures before the next demand occurs.

It is not generally supported in the current technical literature that proof tests should not be required more frequently than once every two years. There is no evidence that consensus on this point has been established within the safety standards themselves. The one-year-limit of the demand of the safety function may be substantiated by considerations outside of the scope of this document. It is not supported by the "basic rationale". The one-year-limit can be used as a criterion for differentiating between high/continuous and low demand mode of operation without logical conflict with other contents of this document.

Still another criterion can be defined as follows: The applicable mode of operation is high demand or continuous demand irrespective of other criteria, if the safety function is the only protection layer that prevents an initiating event from escalating to an accident.

This criterion is not based on a strictly probabilistic argument. The criterion can reflect reservations against the permissibility of proof testing as a measure for preventing accidents. The criterion can also reflect societal or political concerns. In relation to catastrophic accidents, it can appear unacceptable that an unfunctional state is conceded to the addressed safety system for any length of time. However, this is already implied as soon as a "probability of failure" is defined as a property of a technical system at all. Whether assignment of the high or continuous demand mode of operation really leads to a more acceptable situation would need to be determined on a case by case basis. This is not part of the "basic rationale".

8 Relation to ISO 12100

The definitions in this document can be related to the definitions given in ISO 12100:2010 (see also Figure 3 of ISO 12100:2010). Risk and severity of harm are defined identically in ISO 12100:2010 and in this document.

The "probability of occurrence of harm" in Figure 4 would be called a "demand rate" rather than a "probability" in the terminology of this document.

The probability of "occurrence of a harm", as per ISO 12100:2010 is composed of 3 elements:

1) The risk element "exposure of person(s) to the hazard" in ISO 12100:2010 is expressed with the exposure parameter according to 5.7.
2) The risk element "possibility to avoid or limit the harm" is expressed with the probability of avoiding of limiting harm according to 5.8.
3) The "occurrence of a hazardous event" in Figure 3 of ISO 12100:2010 can be identified with
   - ($I_R \times P_r$), if no safety function is present;
   - (PFH $\times P_r$) for a safety function in high/continuous demand mode of operation;
   - ($PFD_{avg} \times I_R \times P_r$) for a safety function in low demand mode of operation.

The "probability of occurrence of harm" in Figure 3 would be called a "demand rate" rather than a "probability" in the terminology of this document.

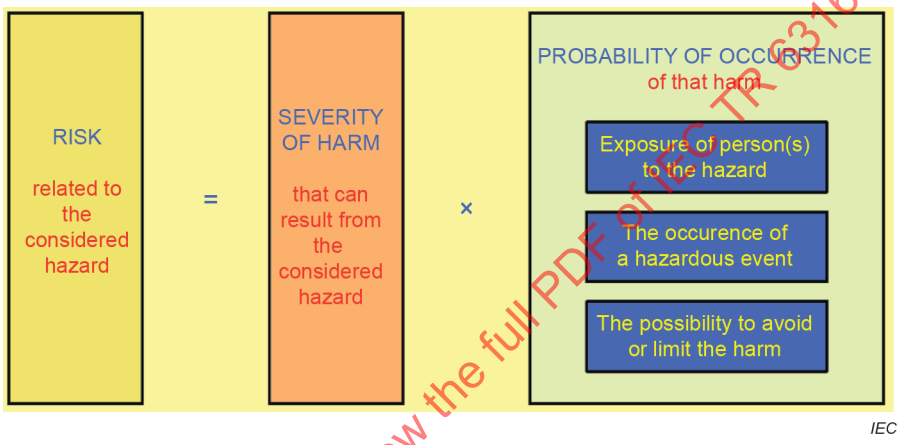


Figure based on ISO 12100:2010, Figure 3 (modified)

Figure 4 – Elements of risk according to ISO 12100

9 Tools for functional safety assignment

9.1 General

Tools for assignment of SIL or PL, risk graphs, risk matrices, scoring methods, and similar are essentially representations of the Formulae (7) or (10), using graphical means or tables. These representations can be derived from the given formulae with the following steps:

- selection of the parameters to be used;
- logarithmizing the parameters;
- discretizing the logarithmic parameters;
- assigning score values to the single discrete parameter settings;
- coding the relations between scores and required safety integrity in a graphical decision tree (risk graph) or in a table (risk table, risk matrix);
- tuning and adaptation, such as for example restriction of offered path (parameter combinations) at the extreme cases of the graph, "tuning" of parameters and similar.

A given tool is applicable only to either "high/continuous" or to "low" demand mode in all typical cases. The decision between "high/continuous demand" versus "low demand" mode of operation is already made before a graphical tool, table, or scoring methods for the SIL assignment are used.

This document does not give preference to any of the described tools for SIL assignment. Neither does this document give preference to the use of such tools or to working with the mathematical relations in a fully quantitative manner. Numerical exactness is not a primary concern for SIL assignment. The assignment is based on a small number of input parameters, which can be quantified in most cases by estimations with a limited accuracy only. On this basis, a fair degree of numerical inexactness can be conceded to an assignment tool, if this facilitates the task for the user or if it is required as a compromise with respect to other boundary conditions. However, the basic logic should not be violated, which is represented by the choice and inherent meaning of the parameters, by their dimensions (i.e. basically time^{-1} or dimensionless) and by their relations.

Application examples of functional safety assignment tools are available in Annex A.

9.2 Selection of independent parameters

An assignment tool does not necessarily use each of the parameters in the Formulae (7) or (10) as independent entry. Logically, this is equivalent to using certain probabilities only with a value of 1.

For example, if in a specific technical application area all relevant safety function failures are considered to be "hidden failures", the parameters P_r, F_r, and $(1 - A_v)$ would not need to be used in a SIL assignment tool for that particular application. These parameters would always assume the value of 1 in the given context.

As a more common example, the customary risk graphs for SIL assignment to functions in low demand mode use a "W-parameter" ("W" for "Wahrscheinlichkeit", i.e. probability). The parameter W can stand for the product $I_R \times P_r$ in Formula (10). These risk graphs do not consider initiating event rate I_R and P_r separately. See IEC 61511-3:2016, Annexes D and E.

9.3 Logarithmizing parameters

The multiplications in the basic Formulae (7) and (10) for SIL assignment can be implemented in graphical tools or methods by logarithmizing the parameters. Thus, multiplications can be executed as additions. This allows the construction of nomograms, for example.

9.4 Discretization of parameters

More typical than nomograms are tools with a graphical decision tree or tabular structure, where the user can only choose discrete entries for the parameters in use. In these tools, the parameters are discretized. Most typically, they are discretized in equidistant steps on logarithmic scales.

"Discretization" means that a continuous numerical range is represented by a set of discrete numbers. This can be illustrated with the scale of PFH, which is frequently represented only as a set of discrete SIL levels, SIL0, SIL1, SIL2, and so on. In the sequence of SILs each discrete level replaces and represents an entire decade on the continuous scale of PFH in the unit h^{-1}, or of PFD_{avg} – see Figure 5. The principle of "Discretization" of a continuous numerical parameter is shown with the scale of PFH in units of [h^{-1}], discretized to a set of SILs.

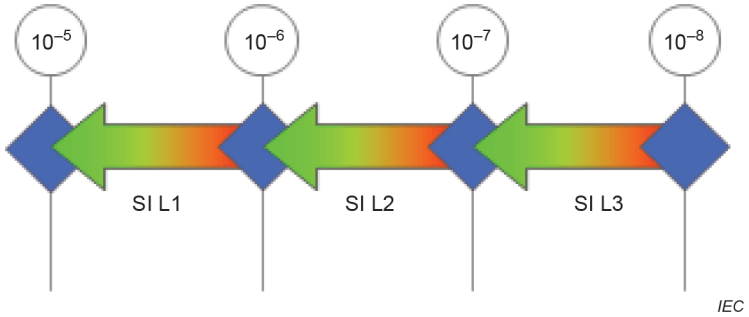


Figure 5 – Discretization of parameters

9.5 Parameter scores

If the input parameters for SIL assignment are used in a logarithmic discretized format, they can be represented by small natural numbers or scores. A graphical, or tabular assignment tool yields the required SIL as a result of the total score sum. The addition of scores can be done graphically in a decision tree. This is the working principle of a risk graph. Risk tables or risk matrices relate the score sum on one axis and the severity parameter on the other axis to the indicator of the required safety integrity.

The scoring system would comply with the following principles in all cases, which are analysed in Annex A:

- for the parameters P_r, F_r, $(1 - A_v)$, and I_R, the score value is increasing with increasing parameter value;
- for the parameter S, the score value is increasing with increasing severity level. Accordingly, the score value is increasing with decreasing tolerable risk limit $L_{(S)}$;
- likewise, for the safety integrity indicator, the score value is increasing with increasing integrity requirement, i.e. increasing with decreasing value of the implied target failure measure, i.e. PFH or PFD_{avg}.

Assuming compliance with the above principles, the relations in Formulae (7) and (10) can be transformed into the following form, which is suitable for graphical or tabular representation:

– for high/continuous demand mode of operation, based on Formula (7):

$$SIL \geq A \times SC(S) + B \times [SC(P_r) + SC(F_r) + SC(1 - A_v)] + C \quad (16)$$

– for low demand mode of operation, based on Formula (10):

$$SIL \geq A \times SC(S) + B \times [SC(P_r) + SC(F_r) + SC(1 - A_v) + SC(I_R)] + C \quad (17)$$

where:

$SC(S)$	is the score value for the severity such as S, P_r, A_v;
$SC(P_r)$	is the score value for the parameter P_r;
$SC(F_r)$	is the score value for the parameter F_r;
$SC(1 - A_v)$	is the score value for the parameter $1 - A_v$;
$SC(I_R)$	is the score value for the parameter I_R. The coefficients A and B in Formulae (16) and (17) are required where different logarithmic scales were used for discretizing different parameters;
parameter C	is required to adjust the arbitrarily chosen zero point of the score scale to the intended tolerable risk.

In Annex A, it is shown in examples how the parameters of relations Formulae (16) or (17) can be extracted from actual risk graphs or risk matrices. As far as this is possible, the respective risk graph or risk table is in accordance with Formula (7) for high/continuous demand or with the relation in Formula (10) for low demand.

9.6 Scoring methods in strict sense

The term "scoring method" is occasionally used in a stricter sense for methods which quantify a given parameter as a sum of scores that are related to qualitative aspects of the application. These aspects are captured in questions, with a predefined set of potential responses, each related to a score. A total parameter score can be defined as the resulting sum for all questions related to the parameter. For example, the parameter $(1 - A_V)$ can be quantified by questions such as:

- How quickly does the accident develop from first indication of a disturbance to complete exposure to the hazard?
  - In less than 30 seconds: score 10
  - In 30 seconds to 2 minutes: score 7
  - In 2 minutes to 15 minutes: score 3
  - In more than 15 minutes: score 0
- How acquainted is the potentially exposed personnel with the machinery/process in question?
  - little: score 10
  - fair: score 5
  - very well: score 0
- and so on.

It is not within the scope of this document to discuss the adequacy of particular questions, potential responses, and the related scoring. Generally, this is a potential way of getting to quantitative estimates from qualitative descriptions with fair reproducibility, if the scoring questions are adequate and clear, and if the scores are appropriately set.

This document gives examples of the parameters and their inherent meaning, which can be the target of scoring questions. In 6.1, basic principles are given as examples which could also apply to the target aspects of scoring questions:

- Each aspect, which is targeted by a scoring question would need to be effective as a risk mitigation measure by itself. For example, the speed of development of a hazardous event is a partial measure for the related risk only where potentially exposed persons have means to avert the upcoming exposure within the given times. With machinery or industrial processes, this is usually the case.
- The correlation should be weak between different aspects, i.e. between answers for different questions for a single parameter. This means answering one question should not give strong preferences to the answers that will be given to other questions.

This document also describes an example method for extracting the implicit quantitative basis from a given scoring system. All statements in 9.5 can be applied to scoring methods in a strict sense as well.

Annex A
(informative)

Examples of SIL assignment tools numerical analysis

A.1 General

This Annex A describes with a few typical examples how the numerical structure according to the basic relations Formula (7) and Formula (10) for SIL assignment can be extracted from a given risk graph or tabular tool. This verifies the statement that the widely established tools can indeed be understood as particular expressions of the basic relations.

The choice of input parameters gives a first consistency criterion. For a safety function in high/continuous mode of application, the following parameters are common:

- event severity;
- probability of occurrence of a hazardous event P_r;
- exposure F_r;
- probability of avoiding or limiting harm A_v.

A parameter for "event severity" is always required, since it carries the setting of the tolerable risk limit. Other parameters may be left out, i.e. used with a value of 1 only, if the parameter is not relevant in the given application area. A single parameter can be split up into specific aspects, according to the example which was given for the probability of avoiding or limiting harm in 5.9, by splitting up the parameter in "avoidability" in a stricter sense and "vulnerability".

If a tool or method is intended for low demand mode of application, an additional input parameter is required that includes the initiating event rate I_R. This parameter will have the dimension time^{-1}, typically in the unit "per year" or y^{-1}.

Accordingly:

- If no time-based input parameter is used, the tool will yield a safety integrity parameter for the high/continuous demand mode of operation, which can be related to PFH as target failure measure.
- If an input parameter is used with the dimension time^{-1}, the tool will yield a safety integrity parameter for the low demand mode of operation, which can be related to PFD_{avg} as target failure measure.

All assignment tools analysed in Clauses A.4, A.5 and A.6 would pass this basic consistency check.

A.2 Assignment of score values to parameter entries

In graphical or tabular assignment tools, the numerical score of a parameter is frequently suggested as an element of the entries. Where, for example, "F1" or "F2" can be chosen for the exposure parameter F_r, the SC(F_r) in Formulae (A.1) and (A.2) will naturally take the values 1 or 2. The same principle applies, e.g., to severity parameters S1, S2, and so on. Where the numerical score of a parameter is not directly evident as an element of the potential entries, it can be established by relating them to natural numbers by sequence, or by replacing an alphabetic sequence by numbers. For example, the series of performance levels from PL a to PL e can be related to the sequence of numbers from 1 to 5 – see Table A.1 in Clause A.5.

A.3 Extraction of tolerable risk limits

The tolerable risk limit can be extracted from SIL assignment tools by selecting a level of severity and from there by following the path, where the entries for P_r, F_r and (1 − A_v) are used with maximum score. These correspond to the parameter settings, which imply that there is no other risk mitigation than the safety function itself.

For a "high/continuous demand tool", this path will lead to the safety integrity indicator, which represents in terms of PFH the maximum event rate that is tolerated for the given severity. See Figure A.1 a).

For a "low demand tool", an additional selection needs to be made on the described path. This is the safety integrity indicator that represents PFD_{avg} with the value of 1. In SIL based methods, that setting is indicated as "SIL0", or "OM" for "other measures", or "A" or footnote "a" for "good engineering practice". This represents the numerical range $1 \leq PFD_{avg} < 10$. Hence, "SIL0" or the equivalent expressions include the value of 1 for PFD_{avg} as the most conservative assumption. The respective path leads to the time-based input parameter which represents in terms of I_R the maximum event rate that is tolerated for the given severity. See Figure A.1 b).

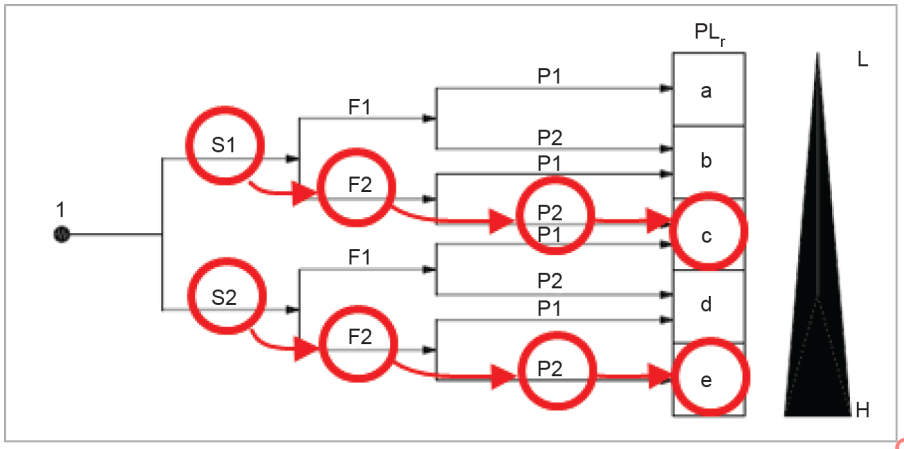
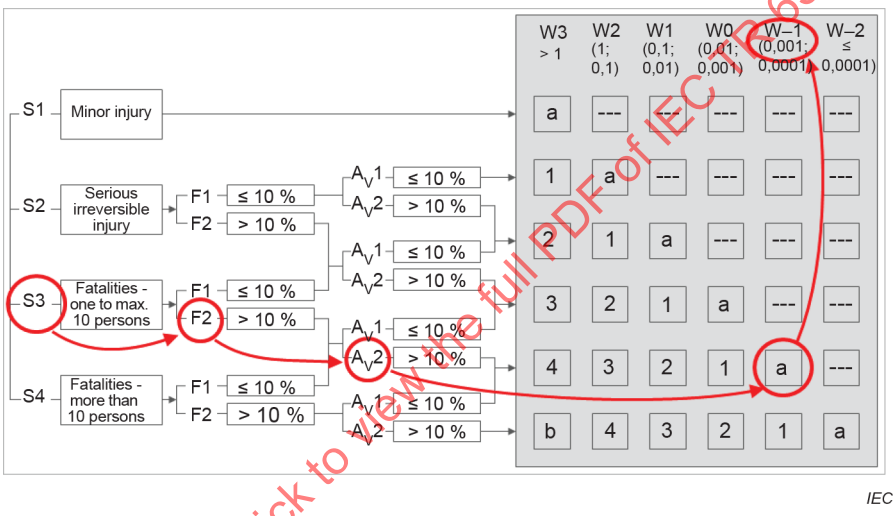


Figure based on ISO 13849-1:2015, Figure A.1 (modified)

a) Graph for determining required PL_r for safety function



b) Figure 8 from VDMA 4315-1:2013-02. Turbomachinery and generators[1]

Figure A.1 – Extraction of tolerable risk limits

Per the described approach, the risk graphs in Figure A.1 yield the following tolerable risk limits:

- Annex A of ISO 13849-1:2015, Severity S1 → PL c → PFH max. 3×10^{-6} / h → 1 event per 38 years
- Annex A of ISO 13849-1:2015, Severity S2 → PL e → PFH max. 1×10^{-7} / h → 1 event per 1 142 years
- VDMA 4315-1; Severity S3 → W1 → max. 0,001/y 1 → 1 event per 1 000 years

In the first instance, the results are approximate and obtained with the described approach. Not every risk graph is completely consistent with a numerical scheme without deviations. See the example in Clause A.4. If a tolerable risk limit is extracted from a single risk graph or risk matrix by different methods, it is possible that the results will deviate from each other in the order of numerical inconsistencies that are in the respective assignment tool.

1 Reproduced with the permission of VDMA.

A.4 Risk matrix of IEC 62061

See Figure A.2 for an example risk matrix taking into account IEC 62061. This SIL assignment tool is intended for use with machinery and with safety control function in high/continuous demand mode of operation. P_r, F_r, and (1 − A_v) are used as input parameters, in accordance with relation Formula (7). These parameters are represented as score sum, called "class" in this specific tool (column heading of the table). The safety integrity indicators are given in both established notions, as SIL and as PL, in relation to the severity levels.

Note that A_v in accordance with the risk matrix of Annex A of IEC 62061:2021, Figure A.2 of this document corresponds to (1 − A_v) in this document, i.e. the symbol A_v is used with a complementary meaning. Furthermore SIL 2 at Class 3 and 4 of IEC 62061:2021 is reduced to SIL 1 because of the low score for the classes of Frequency, Probability and Avoiding Harm.

Following the approach of Clause A.3, the tolerable risk limits can be extracted as approximate values from the column of the table with the maximum score or "Class". The maximum score is 15 in this tool. The following limits can be extracted:

- Severity S1 → SIL1 → PFH max. 1×10^{-5} / h → 1 event in ca 10 years, or
  PL c → PFH max. 3×10^{-6} / h → 1 event in ca 30 years
- Severity S2 → SIL2 → PFH max. 1×10^{-6} / h → 1 event in ca 100 years
- Severity S3 → SIL3 → PFH max. 1×10^{-7} / h → 1 event in ca 1 000 years
- Severity S4 → SIL3 → PFH max. 1×10^{-7} / h → 1 event in ca 1 000 years, i.e. the same tolerable risk limit as for S3.

<table>
<tr><th rowspan="2">Consequences</th><th rowspan="2">Severity Se</th><th colspan="13">Class Cl = F_r + P_r + A_v</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">No SIL (or PL) required</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">No SIL (or PL) required</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>

OM: Other Measures (e.g. basic safety principles)

NOTE 1 SIL 2 at Class 3 and 4 in IEC 62061:2021 is reduced in this table to SIL 1 because of the low score for the classes of Frequency, Probability and Avoiding Harm.

NOTE 2 SIL 2 at Class 5, 6 and 7 is not calibrated in line with the rest of this table because it is the intention to take account of the moderate score for the classes of Frequency, Probability and Avoiding Harm in combination with the possibility of death as a consequence.

NOTE 3 Owing to characteristics of risks present at machinery, SIL 4 is not considered. For SIL 4 see IEC 61508-1.

NOTE 4 The correspondence between SIL and PL$_r$ is valid only for the required level and not for the achieved level.

Figure A.2 – Risk matrix based on IEC 62061