# 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 It also gives information on projects, replaced and withdrawn publications.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.

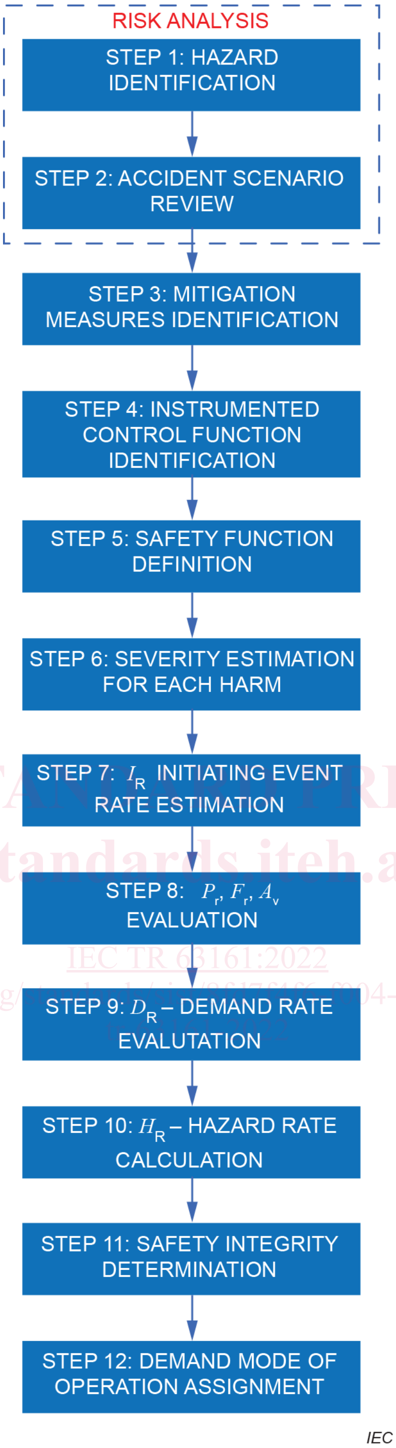




**Figure 1 – Sequence of steps in functional safety assignment**

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.