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.

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 7
2 Normative references 7
3 Terms and definitions 7
4 Risk based quantitative approach 10
4.1 General 10
4.2 Sequence of steps in functional safety assignment 10
4.3 Reference information 12
4.3.1 General 12
4.3.2 Accident scenario 13
4.3.3 Hazard zone 13
4.3.4 Severity of harm 13
4.3.5 Safety control function 14
5 Quantified parameters of a functional safety assignment 14
5.1 General 14
5.2 Parameter types 14
5.2.1 General 14
5.2.2 Probability 14
5.2.3 Event rate 14
5.3 Probability of occurrence of harm 15
5.4 Quantification of risk 15
5.5 Target failure measure 15
5.6 Probability of occurrence of a hazardous event – P_{r} 16
5.7 Exposure parameter – F_{r} 17
5.8 Probability of avoiding or limiting harm – A_{v} 18
5.8.1 General 18
5.8.2 Vulnerability (V) 18
5.8.3 Avoidability (A) 19
5.9 Demand types and related event rates 19
5.9.1 Event classes 19
5.9.2 Demand and demand rate 20
5.9.3 Initiating events and rate of initiating events I_{R} 20
5.9.4 Safety demands and safety demand rate D_{R} 21
5.9.5 Tolerable risk limit – Parameter $L_{(\mathrm{S})}$ 22
5.10 Additional parameters 23
6 General principle of functional safety assignment 25
6.1 Basics 25
6.1.1 Applicability to complete functions 25
6.1.2 Risk relation 25
6.1.3 Logical independence of parameters 25
6.2 High demand or continuous mode of operation 25
6.3 Low demand mode of operation 26
7 Assignment of the demand mode 27
7.1 Demand mode – General 27

7.2 Assignment criteria 30
8 Relation to ISO 12100 30
9 Tools for functional safety assignment 31
9.1 General 31
9.2 Selection of independent parameters 32
9.3 Logarithmizing parameters 32
9.4 Discretization of parameters 32
9.5 Parameter scores 33
9.6 Scoring methods in strict sense 34
Annex A (informative) Examples of SIL assignment tools numerical analysis 35
A.1 General 35
A.2 Assignment of score values to parameter entries 35
A.3 Extraction of tolerable risk limits 36
A.4 Risk matrix of IEC 62061 38
A.5 Risk graph of ISO 13849 41
A.6 Risk graphs for low demand mode of operation 43
Bibliography 46

Figure 1 – Sequence of steps in functional safety assignment 12
Figure 2 – Protection layers, event rates and their relation 22
Figure 3 – Hazard rate according to the Henley / Kumamoto equation 29
Figure 4 – Elements of risk according to ISO 12100 31
Figure 5 – Discretization of parameters 33
Figure A.1 – Extraction of tolerable risk limits 37
Figure A.2 – Risk matrix based on IEC 62061 38
Figure A.3 – Maximum allowable PFH as function of the score sum for the different severity levels 39
Figure A.4 – Representation by a continuous numerical interpolation 40
Figure A.5 – Risk graph of ISO 13849-1 41
Figure A.6 – Interpolation per severity level 43
Figure A.7 – Risk graph for low demand mode of operation 44
Figure A.8 – Risk graph for low demand mode of operation – from Figure 7 of VDMA 4315-1 45

Table 1 – Parameters overview 24
Table A.1 – Relation between PLs and ranges in PFH 42

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*