IEC/TR 61508-0

Edition 1.0 2005-01

TECHNICAL REPORT

RAPPORT TECHNIQUE

Functional safety of electrical/electronic/programmable electronic safety-related systems –
Part 0: Functional safety and IEC 61508

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité –
Partie 0: La sécurité fonctionnelle et la CEI 61508

IEC/TR 61508-0:2005

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: 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 corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:
Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

A propos de la CEI

La Commission Electrotechnique Internationale (CEI) est la première organisation mondiale qui élabore et publie des normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications CEI

Le contenu technique des publications de la CEI est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

- Catalogue des publications de la CEI: www.iec.ch/searchpub/cur_fut-f.htm

Le Catalogue en-ligne de la CEI vous permet d'effectuer des recherches en utilisant différents critères (numéro de référence, texte, comité d'études,…). Il donne aussi des informations sur les projets et les publications retirées ou remplacées.

- Just Published CEI: www.iec.ch/online_news/justpub

Restez informé sur les nouvelles publications de la CEI. Just Published détaille deux fois par mois les nouvelles publications parues. Disponible en-ligne et aussi par email.

- Electropedia: www.electropedia.org

Le premier dictionnaire en ligne au monde de termes électroniques et électriques. Il contient plus de 20 000 termes et définitions en anglais et en français, ainsi que les termes équivalents dans les langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International en ligne.

- Service Clients: www.iec.ch/webstore/custserv/custserv_entry-f.htm

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions, visitez le FAQ du Service clients ou contactez-nous:
Email: csc@iec.ch
Tél.: +41 22 919 02 11
Fax: +41 22 919 03 00

IEC/TR 61508-0

Edition 1.0 2005-01

TECHNICAL REPORT

RAPPORT TECHNIQUE

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 0: Functional safety and IEC 61508

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 0: La sécurité fonctionnelle et la CEI 61508

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

PRICE CODE
CODE PRIX
Q

ICS 13.110; 25.040; 29.020; 35.240.50

ISBN 2-8318-7816-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/ PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 0: Functional safety and IEC 61508

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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
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.

The main task of IEC technical committees is to prepare International Standards. However, a technical committee may propose the publication of a technical report when it has collected data of a different kind from that which is normally published as an International Standard, for example "state of the art".

IEC 61508-0, which is a technical report, has been prepared by subcommittee 65A: System Aspects, of IEC technical committee 65: Industrial-process measurement and control.

The text of this technical report is based on the following documents:

Enquiry draft	Report on voting
65A/413/DTR	65A/422/RVC

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

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The parts of this publication, IEC 61508, under the general title *Functional safety of electrical/electronic/programmable electronic safety-related systems* are listed in 4.6.

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

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

INTRODUCTION

The purpose of this Technical Report is to introduce the concept of functional safety and to give an overview of the IEC 61508 series of standards.

You should read it if you are:

- wondering whether IEC 61508 applies to you,
- involved in the development of electrical, electronic or programmable electronic systems which may have safety implications, or
- drafting any other standard where functional safety is a relevant factor.

Clause 3 of this document gives an informal definition of functional safety, describes the relationship between safety functions, safety integrity and safety-related systems, gives an example of how functional safety requirements are derived, and lists some of the challenges in achieving functional safety in electrical, electronic or programmable electronic systems. Clause 4 gives details of IEC 61508, which provides an approach for achieving functional safety. The clause describes the standard's objectives, technical approach and parts framework. It explains that IEC 61508 can be applied as is to a large range of industrial applications and yet also provides a basis for many other standards.

FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/ PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS –

Part 0: Functional safety and IEC 61508

1 Scope

This Technical Report introduces the concept of functional safety and gives an overview of the IEC 61508 series.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61508-1:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*

IEC 61508-2:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*

IEC 61508-3:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements*

IEC 61508-4:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*

IEC 61508-5:1998, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels*

IEC 61508-6:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*

IEC 61508-7:2000, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures*

IEC Guide 104, *The preparation of safety publications and the use of basic safety publications and group safety publications*

ISO/IEC Guide 51, *Safety aspects – Guidelines for their inclusion in standards*

3 Functional safety

3.1 What is functional safety?

We begin with a definition of *safety*. This is freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.

Functional safety is part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

For example, an overtemperature protection device, using a thermal sensor in the windings of an electric motor to de-energise the motor before it can overheat, is an instance of functional safety. But providing specialised insulation to withstand high temperatures is not an instance of functional safety (although it is still an instance of safety and could protect against exactly the same hazard).

Neither safety nor functional safety can be determined without considering the systems as a whole and the environment with which they interact.

3.2 Safety functions and safety-related systems

Generally, the significant hazards for equipment and any associated control system in its intended environment have to be identified by the specifier or developer via a hazard analysis. The analysis determines whether functional safety is necessary to ensure adequate protection against each significant hazard. If so, then it has to be taken into account in an appropriate manner in the design. Functional safety is just one method of dealing with hazards, and other means for their elimination or reduction, such as inherent safety through design, are of primary importance.

The term *safety-related* is used to describe systems that are required to perform a specific function or functions to ensure risks are kept at an accepted level. Such functions are, by definition, *safety functions*. Two types of requirements are necessary to achieve functional safety:

- *safety function requirements* (what the function does) and
- *safety integrity requirements* (the likelihood of a safety function being performed satisfactorily).

The safety function requirements are derived from the hazard analysis and the safety integrity requirements are derived from a risk assessment. The higher the level of safety integrity, the lower the likelihood of dangerous failure.

Any system, implemented in any technology, which carries out safety functions is a *safety-related system*. A safety-related system may be separate from any equipment control system or the equipment control system may itself carry out safety functions. In the latter case, the equipment control system will be a safety-related system. Higher levels of safety integrity necessitate greater rigour in the engineering of the safety-related system.

3.3 Example of functional safety

Consider a machine with a rotating blade that is protected by a hinged solid cover. The blade is accessed for routine cleaning by lifting the cover. The cover is interlocked so that whenever it is lifted an electrical circuit de-energises the motor and applies a brake. In this way, the blade is stopped before it could injure the operator.

In order to ensure that safety is achieved, both hazard analysis and risk assessment are necessary.

a) The *hazard analysis* identifies the hazards associated with cleaning the blade. For this machine it might show that it should not be possible to lift the hinged cover more than 5 mm without the brake activating and stopping the blade. Further analysis could reveal that the time for the blade to stop shall be 1 s or less. Together, these describe the *safety function*.

b) The *risk assessment* determines the performance requirements of the safety function. The aim is to ensure that the *safety integrity* of the safety function is sufficient to ensure that no one is exposed to an unacceptable risk associated with this hazardous event.

The harm resulting from a failure of the safety function could be amputation of the operator's hand or could be just a bruise. The risk also depends on how frequently the cover has to be lifted, which might be many times during daily operation or might be less than once a month. The level of safety integrity required increases with the severity of injury and the frequency of exposure to the hazard.

The safety integrity of the safety function will depend on all the equipment that is necessary for the safety function to be carried out correctly, i.e. the interlock, the associated electrical circuit and the motor and braking system. Both the safety function and its safety integrity specify the required behaviour for the systems as a whole within a particular environment.

To summarise, the hazard analysis identifies what has to be done to avoid the hazardous event, or events, associated with the blade. The risk assessment gives the safety integrity required of the interlocking system for the risk to be acceptable. These two elements, "What safety function has to be performed?" – the *safety function requirements* – and "What degree of certainty is necessary that the safety function will be carried out?" – the *safety integrity requirements* – are the foundations of functional safety.

3.4 Challenges in achieving functional safety

Safety functions are increasingly being carried out by electrical, electronic or programmable electronic systems. These systems are usually complex, making it impossible in practice to fully determine every failure mode or to test all possible behaviour. It is difficult to predict the safety performance, although testing is still essential.

The challenge is to design the system in such a way as to prevent dangerous failures or to control them when they arise. Dangerous failures may arise from

- incorrect specifications of the system, hardware or software;
- omissions in the safety requirements specification (e.g. failure to develop all relevant safety functions during different modes of operation);
- random hardware failure mechanisms;
- systematic hardware failure mechanisms;
- software errors;
- common cause failures;

- human error;
- environmental influences (e.g. electromagnetic, temperature, mechanical phenomena);
- supply system voltage disturbances (e.g. loss of supply, reduced voltages, re-connection of supply).

IEC 61508 contains requirements to minimise these failures and is described in the next clause.

4 IEC 61508 – Functional safety of E/E/PE safety-related systems

4.1 Objectives

IEC 61508 aims to

- release the potential of E/E/PE technology to improve both safety and economic performance;
- enable technological developments to take place within an overall safety framework;
- provide a technically sound, system based approach, with sufficient flexibility for the future;
- provide a risk-based approach for determining the required performance of safety-related systems;
- provide a generically-based standard that can be used directly by industry but can also help with developing sector standards (e.g. machinery, process chemical plants, medical or rail) or product standards (e.g. power drive systems);

- provide a means for users and regulators to gain confidence when using computer-based technology;

- provide requirements based on common underlying principles to facilitate:
  - improved efficiencies in the supply chain for suppliers of subsystems and components to various sectors,
  - improvements in communication and requirements (i.e. to increase clarity of what needs to be specified),
  - the development of techniques and measures that could be used across all sectors, increasing available resources,
  - the development of conformity assessment services if required.

IEC 61508 does not cover the precautions that may be necessary to prevent unauthorized persons damaging, and/or otherwise adversely affecting, the functional safety achieved by E/E/PE safety-related systems.

4.2 E/E/PE safety-related systems

IEC 61508 is concerned with functional safety, achieved by safety-related systems that are primarily implemented in electrical and/or electronic and/or programmable electronic (E/E/PE) technologies, i.e. E/E/PE safety related systems. The standard is generic in that it applies to these systems irrespective of their application.

Some requirements of the standard relate to development activities where the implementation technology may not yet have been fully decided. This includes development of the overall safety requirements (concept, scope definition, hazard analysis and risk assessment). If there is a possibility that E/E/PE technologies might be used, the standard should be applied so that the functional safety requirements for any E/E/PE safety-related systems are determined in a methodical, risk-based manner.

Other requirements of the standard are not solely specific to E/E/PE technology, including documentation, management of functional safety, functional safety assessment and competence. All requirements that are not technology-specific might usefully be applied to other safety-related systems although these systems are not within the scope of the standard.

The following are examples of E/E/PE safety-related systems:

- emergency shut-down system in a hazardous chemical process plant;
- crane safe load indicator;
- railway signalling system;
- guard interlocking and emergency stopping systems for machinery;
- variable speed motor drive used to restrict speed as a means of protection;
- system for interlocking and controlling the exposure dose of a medical radiotherapy machine;
- dynamic positioning (control of a ship's movement when in proximity to an offshore installation);
- fly-by-wire operation of aircraft flight control surfaces;
- automobile indicator lights, anti-lock braking and engine-management systems;
- remote monitoring, operation or programming of a network-enabled process plant;
- an information-based decision support tool where erroneous results affect safety.

An E/E/PE safety-related system covers all parts of the system that are necessary to carry out the safety function (i.e. from sensor, through control logic and communication systems, to final actuator, including any critical actions of a human operator).
Since the definition of E/E/PE safety-related system is derived from the definition of safety, it also concerns freedom from unacceptable risk of both physical injury and damage to the health of people. The harm can arise indirectly as a result of damage to property or the environment. However, some systems will be designed primarily to protect against failures with serious economic implications. IEC 61508 can be used to develop any E/E/PE system that has critical functions, such as the protection of equipment or products.

4.3 Technical approach

IEC 61508

- uses a risk based approach to determine the safety integrity requirements of E/E/PE safety-related systems, and includes a number of examples of how this can be done;
- uses an overall safety lifecycle model as the technical framework for the activities necessary for ensuring functional safety is achieved by the E/E/PE safety-related systems;