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

FOREWORD....3
INTRODUCTION....5

1 Scope....6
2 Normative references....6
3 Functional safety....7
3.1 What is functional safety?....7
3.2 Safety functions and safety-related systems....7
3.3 Example of functional safety....8
3.4 Challenges in achieving functional safety....8
4 IEC 61508 – Functional safety of E/E/PE safety-related systems....9
4.1 Objectives....9
4.2 E/E/PE safety-related systems....9
4.3 Technical approach....10
4.4 Safety integrity levels....11
4.5 Example of functional safety revisited....11
4.6 Parts framework of IEC 61508....12
4.7 IEC 61508 as a basis for other standards....14
4.8 IEC 61508 as a stand-alone standard....14
4.9 Further information....15

Annex A (informative) List of frequently asked questions from IEC “functional safety” zone....16

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*

SOMMAIRE

AVANT-PROPOS 19
INTRODUCTION 21

1 Domaine d'application 22
2 Références normatives 22
3 Sécurité fonctionnelle 23
3.1 Qu'est ce que la sécurité fonctionnelle ? 23
3.2 Fonctions de sécurité et systèmes relatifs à la sécurité 23
3.3 Exemple de sécurité fonctionnelle 24
3.4 Défis rencontrés dans l'atteinte de la sécurité fonctionnelle 24
4 CEI 61508 – Sécurité fonctionnelle des systèmes E/E/PE relatifs à la sécurité 25
4.1 Objectifs 25
4.2 Systèmes E/E/PE relatifs à la sécurité 25
4.3 Approche technique 26
4.4 Niveaux d'intégrité de sécurité 27
4.5 Exemple de sécurité fonctionnelle revisitée 27
4.6 Structure de la CEI 61508 28
4.7 La CEI 61508, base pour d'autres normes 30
4.8 La CEI 61508 comme norme autonome 30
4.9 Autres informations 31

Annexe A (informative) Liste de questions fréquemment posées, tirée de la zone « sécurité fonctionnelle » du site de la CEI 32

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ FONCTIONNELLE DES SYSTÈMES ÉLECTRIQUES/ÉLECTRONIQUES/ÉLECTRONIQUES PROGRAMMABLES RELATIFS A LA SÉCURITÉ –

Partie 0: La sécurité fonctionnelle et la CEI 61508

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de la CEI"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec la CEI, participent également aux travaux. La CEI collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI n'a prévu aucune procédure de marquage valant indication d'approbation et n'engage pas sa responsabilité pour les équipements déclarés conformes à une de ses Publications.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à la CEI, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de la CEI, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de la CEI ou de toute autre Publication de la CEI, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de la CEI peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. La CEI ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et de ne pas avoir signalé leur existence.

La tâche principale des comités d'études de la CEI est l'élaboration des Normes internationales. Toutefois, un comité d'études peut proposer la publication d'un rapport technique lorsqu'il a réuni des données de nature différente de celles qui sont normalement publiées comme Normes internationales, cela pouvant comprendre, par exemple, des informations sur l'état de la technique.

La CEI 61508-0, qui est un rapport technique, a été établie par le sous-comité 65a: Aspects systèmes, du comité d'études 65 de la CEI: Mesure et commande dans les processus industriels.

Le texte de ce rapport technique est issu des documents suivants:

Projet d'enquête	Rapport de vote
65A/413/DTR	65A/422/RVC

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de ce rapport technique.

Cette publication a été rédigée selon les Directives ISO/CEI, Partie 2.

Les parties de cette publication, la CEI 61508, présentées sous le titre général *Sécurité fonctionnelle des systèmes électriques/électroniques/ électroniques programmables relatifs à la sécurité* sont données en 4.6.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de maintenance indiquée sur le site web de la CEI sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite;
- supprimée;
- remplacée par une édition révisée, ou
- amendée.

INTRODUCTION

L'objet de ce rapport technique est d'introduire le concept de sécurité fonctionnelle et de donner une vue d'ensemble de la série de normes CEI 61508.

Il convient de lire ce document dans les cas suivants:

- si vous voulez savoir comment la CEI 61508 s'applique à vous,
- si vous êtes impliqués dans le développement de systèmes électriques, électroniques ou électroniques programmables qui on trait à la sécurité,
- si vous participez à l'élaboration d'autres normes pour lesquelles la sécurité fonctionnelle est un élément pertinent.

L'Article 3 de ce document donne une définition informelle de la sécurité fonctionnelle, décrit les relations entre les fonctions de sécurité, l'intégrité de sécurité et les systèmes relatifs à la sécurité, donne un exemple de comment les exigences de sécurité fonctionnelle sont déduites et liste en partie les points à surmonter pour atteindre la sécurité fonctionnelle dans les systèmes électriques, électroniques et électroniques programmables. L'Article 4 donne des détails sur la CEI 61508, qui procure une approche pour l'atteinte de la sécurité fonctionnelle. L'article décrit les objectifs de la norme, l'approche technique et la structure en différentes parties. Il explique que la CEI 61508 peut être appliquée en l'état à un large éventail d'applications industrielles et qu'elle fournit une base à beaucoup d'autres normes.

SÉCURITÉ FONCTIONNELLE DES SYSTÈMES ÉLECTRIQUES/ÉLECTRONIQUES/ÉLECTRONIQUES PROGRAMMABLES RELATIFS A LA SÉCURITÉ –

Partie 0: La sécurité fonctionnelle et la CEI 61508

1 Domaine d'application

Le présent rapport technique introduit le concept de sécurité fonctionnelle et donne une vue d'ensemble de la série CEI 61508.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

CEI 61508-1:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 1: Prescriptions générales*

CEI 61508-2:2000, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Prescriptions pour les systèmes électriques /électroniques /électroniques programmables relatifs à la sécurité*

CEI 61508-3:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 3: Prescriptions concernant les logiciels*

CEI 61508-4:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 4: Définitions et abréviations*

CEI 61508-5:1998, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 5: Exemples de méthodes de détermination des niveaux d'intégrité de sécurité*

CEI 61508-6:2000, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 6: Lignes directrices pour l'application de la CEI 61508-2 et de la CEI 61508-3*

CEI 61508-7:2000, *Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 7: Présentation de techniques et mesures*

Guide CEI 104, *Elaboration des publications de sécurité et utilisation des publications fondamentales de sécurité et publications groupées de sécurité*

Guide ISO/CEI 51, *Aspects liés à la sécurité – Principes directeurs pour les inclure dans les normes*