

THE ENGINEERING EQUIPMENT AND MATERIALS USERS' ASSOCIATION

Guide to the
Application of IEC 61511
to safety instrumented systems
in the UK process industries

PUBLICATION 222

Edition 1

Released by IHS
Not for resale



Copyright © 2009 The Engineering Equipment and Materials Users' Association.
A company limited by guarantee. Registered in England. Company number 477838.

ISBN 0 85931 168 6 Imprint reference 06-2009
Registered and Trading Address
10-12 Lovat Lane London EC3R 8DN
Telephone: +44 (0)20 7621 0011
Fax: +44 (0)20 7621 0022
E-mail: sales@eemua.org
Website: www.eemua.org

This is a preview. [Click here to purchase the full publication.](#)

ABOUT THE PUBLISHERS

The Engineering Equipment and Materials Users' Association, more commonly known as EEMUA, is a European non-profit membership Association helping companies that own or operate industrial facilities - the *users* of engineering equipment and materials.

EEMUA aims to improve the safety, environmental and operating performance of industrial facilities in the most cost-effective way, thereby demonstrating and pursuing leadership in asset management.

EEMUA Members pursue these aims through collaboration for mutual benefit, sharing engineering experiences and expertise and by promoting their distinct interests as the users of engineering products.

Specifically, the aims of EEMUA Member companies are achieved by:

- providing the organisation within which networking, information sharing and collaboration on non-competitive technical matters can take place;
- influencing the way written regulations are interpreted and applied in practice;
- presenting and promoting Members' views, and encouraging the application of good, sound engineering practices;
- developing user guides, specifications, training and competency schemes;
- facilitating Members' participation in national and international standards making;
- influencing relevant national and European legislation and regulations.

Formed in 1949 as the Engineering Equipment Users Association, and re-named in 1983 (as a result of taking over the materials association, OCMA), EEMUA has for more than fifty years given companies that own and operate process plants, power stations and other significant industrial facilities, a collaborative voice in addressing technical and engineering related issues that impact on good integrity management and asset management practices. The Association is open to companies of all sizes that meet its 'engineering user' criteria. Further details of current Members of EEMUA is available on the Association's website, www.eemua.org.

EEMUA activities often lead to the production of publications. These are prepared for Members' use and are often offered for sale as well.

A list of EEMUA publications for sale is given at the end of this Publication. The full list is also on the Association's website, including details of on-line shopping facilities.

To enquire about corporate Membership, write to enquiries@eemua.org or call +44 (0)20 7621 0011.

ABOUT THIS PUBLICATION

Each authorised copy of this Publication is supplied with an electronic version on CD-rom: attached in a wallet overleaf.

Legal Aspects

All rights, title and interest in this Publication shall belong to EEMUA. All rights are reserved. No part of this Publication, including the CD-rom, may be reproduced, stored in a retrieval system, or transmitted in any form or by any means: electronic, mechanical, photocopying, recording or other, without the express prior written agreement of the EEMUA Executive Director.

Infringement of copyright is illegal and also reduces the Association's income thereby jeopardising its ability to fund the production of future publications.

It has been assumed in the preparation of this Publication that: the user ensures selection of those parts of its contents appropriate to the intended application; and that such selection and application is correctly carried out by appropriately qualified and competent persons for whose guidance this Publication has been prepared. EEMUA and the individual members of the Work Group that prepared this EEMUA Publication do not, and indeed cannot, make any representation or give any warranty or guarantee in connection with material contained herein. EEMUA and the individual members of the Work Group that prepared this EEMUA Publication expressly disclaim any liability or responsibility for damage or loss resulting from the use or reliance on this Publication. Any recommendations contained herein are based on the most authoritative information available at the time of writing and on current good engineering practice, but it is essential for the user to take account of pertinent subsequent developments and/or legislation.

Any person who encounters an inaccuracy or ambiguity when making use of this Publication is asked to notify EEMUA without delay so that the matter may be investigated and appropriate action taken.

Consultation and Feedback

EEMUA encourages constructive comments on this Publication from both Members of the Association and others.

Comments should be sent on the standard feedback form, a copy of which is provided towards the end of this Publication. An electronic version of the feedback form is available from EEMUA - e-mail your request for a copy to enquiries@eemua.org, telephone your request to +44 (0)20 7621 0011, or download the form from the EEMUA website at www.eemua.org. Submit comments by e-mail (preferred) or post.

Comments are considered by the relevant EEMUA Technical Committee and may be incorporated in future editions of this Publication. New editions are published on the EEMUA website.

Contents

Foreword	1
1. Scope	3
2. Terms, Definitions and Acronyms	5
2.1 Terms and Definitions	5
2.2 Acronyms	7
3. Overview of IEC 61511	9
3.1 Background	9
3.2 Scope and Application of IEC 61511	9
3.3 Relationship between IEC 61508 and IEC 61511	9
3.4 Parts of IEC 61511-1	10
3.5 Lifecycle Approach	11
4. Legal Aspects	13
4.1 Health and Safety Legislation	13
4.2 Health and Safety Legislation (Onshore Facilities)	14
4.3 Health and Safety Legislation (Offshore Installations)	14
4.4 Application to Existing Installations	15
4.5 Civil Liabilities	15
5. Common Requirements for all Activities	17
5.1 Responsibilities	17
5.2 Competency	17
5.3 Planning	18
5.4 Verification	18
5.5 Validation	19
5.6 Functional Safety Assessment	19
5.7 Conformity Assessment	22
5.8 Management of Lifecycle Activities	23
5.9 Documentation	23
6. Requirements for Specific Activities	25
6.1 Front End Activities	25
6.2 Application Design and Specification	26
6.3 Integration	34
6.4 Product Supply	39
6.5 Installation	41
6.6 Commissioning	44
6.7 Operation and Maintenance	47
6.8 Modification and Decommissioning	50
Annex A SIL Determination Methods and Calibration	53
Annex B Technology Issues	60
Annex C Example of a Functional Safety Plan Overview	69
Annex D Example Competency Scheme	73
Annex E Example Supplier Safety Validation Plan	82
Annex F Reliability Data and Calculations	94
7. References	99

Tables

Table 1 Application of IEC 61508 and IEC 61511.....	11
Table A.1 Risk graph parameter explanations.....	55
Table A.2 Example consequence equivalence.....	57
Table A.3 Layer of protection analysis (LOPA).....	58
Table D.1 Example generic competence standard.....	75
Table E.1 Quality and functional safety control matrix.....	84
Table F.1 Failure rate data for typical SIS subsystems.....	96
Table F.2 PFD values.....	97

Figures

Figure 1 Safety lifecycle.....	12
Figure 2 Functional safety assessment.....	20
Figure A.1 Risk graph.....	54
Figure F.1 Reliability block diagram.....	96

Foreword

This Guide has been prepared by representatives of EEMUA, the Engineering Equipment and Materials Users' Association; EIC (the Energy Industries Council); Oil & Gas UK (formerly UKOOA) and the Health and Safety Executive (HSE).

It refers throughout to the international standard IEC 61511, which is published in the UK by BSI as BS EN 61511.

This Guide is intended to explain how to use IEC 61511 effectively. It addresses the responsibility and deliverables of organisations involved in the specification, supply and maintenance of safety instrumented systems (SIS). It should be read in conjunction with IEC 61511-1 and, where appropriate, IEC 61508. In any case of apparent discrepancy between this Guide and IEC 61511 or IEC 61508, the IEC standard should be deemed to take precedence.

Chapter 3 provides an overview of IEC 61511-1, Chapter 4 provides an overview of the legal aspects, Chapter 5 focuses on issues that affect all users, and Chapter 6 addresses activities of specific users covering the whole lifecycle of the SIS. Technical detail and examples are given in the annexes.

This Guide takes the form of guidance and recommendations. It should not be quoted as if it was a specification and particular care should be taken to ensure that claims of compliance are not misleading. It must not be used as a basis for conformity assessment.

Where this guidance identifies specific techniques it does not preclude the use of other suitable approaches which comply with IEC 61511.

Whilst every effort has been made to ensure the accuracy of the information contained in this publication, neither EEMUA, EIC, Oil & Gas UK nor any of their members assume liability for any use made thereof.

For future updates of this Guide please use the feedback form at the back of this Publication.

Acknowledgements

EEMUA, EIC and Oil & Gas UK acknowledge participation of the following in the development of this Guide

Matt Atkinson	Stone and Webster Ltd
Simon Brown	Health and Safety Executive
Parvez Butt	Energy Industries Council (affiliation at time of participation)
Mervyn Currie	BP Exploration Operating Company Ltd
Alan Lewendon	Energy Industries Council (affiliation at time of participation)
Roy Lord	BP Oil UK Ltd (affiliation at time of participation)
Huw Morgan	BP Chemicals Ltd
Don Muir	Hydrocarbon Resources Ltd
Ian Parry	Hima-Sella Ltd
Jeff Pearson	Health and Safety Executive
Ian Ramsay-Connell	Trinity Integrated Systems Ltd
Ken Simpson	Functional Safety Consultancy Ltd
John Todman	AMEC plc
Wayne Vernon	Health and Safety Executive

This page is intentionally blank.

1. Scope

This Guide provides guidance and recommendations on IEC 61511-1 and, as appropriate, IEC 61508 for the specification and implementation of safety instrumented systems (SIS) in the UK process industries.

It provides guidance only where it is considered necessary or useful. The relevant sub-clauses of IEC 61511-1 are referenced in a right-hand column. Clauses marked ** give recommendations beyond the scope of IEC 61511-1 where they are worthy of consideration. Such recommendations are considered to be good practice in the UK. This Guide does not take precedence over, repeat or replace any requirement of IEC 61511-1 or IEC 61508.

This Guide is applicable to process industries such as onshore and offshore oil and gas, non-nuclear power generation, chemicals and petrochemicals. Other process industries may choose to use the guidelines at their own discretion.

It outlines general information for all users, plus guidance on organisational responsibilities for end users, designers, suppliers (of systems and products), integrators, installers and maintainers. It does not provide checklists or detail on how to design, operate and maintain such systems.

This Guide is for use in applications relating to safety of people, but its principles may also be applied to environmental and asset/commercial protection.

Note on Terminology

The words "clause" and "sub-clause" refer to parts of IEC 61511, the words "Chapter" and "Section" refer to parts of this Guide.

This page is intentionally blank.

2. Terms, Definitions and Acronyms

2.1 Terms and Definitions

For the purposes of this Guide, the terms and definitions defined in IEC 61511-1, IEC 61508-4 and the following apply.

Availability	<p>Ability of the SIS (under combined aspects of its reliability, maintainability and maintenance support) to perform its required function at a stated time or over a stated period of time.</p> <p>Proportion of time that an item is capable of operating to specification within a large time interval (Smith ^[1]).</p>
Commissioning	Testing of the full functionality of the installed equipment as applicable, e.g. SIS, in order to demonstrate the system meets agreed requirements.
Competent	<p>For a person to be competent they need qualifications, experience and qualities appropriate to their duties. These include:</p> <ul style="list-style-type: none"> - such training as would ensure acquisition of the necessary knowledge of the field for the tasks that they are required to perform - adequate knowledge of the hazards and failures of the equipment for which they are responsible - knowledge and understanding of the working practices used in the organisation for which they work - the ability to communicate effectively with their peers, with any staff working under their supervision and with their supervisors - an appreciation of their own limitations and constraints, whether of knowledge, experience, facilities, resources, etc., and a willingness to point these out. <p>(Managing competence for safety-related systems, Part 1^[2])</p>
Diagnostic	Automatic function that detects and reports failures or malfunctions of components in the system.
Down time	Period of time that any system or subsystem is not available to perform its required function.
Duty holder	<p>Organisation that has a specific legal duty under health and safety legislation.</p> <p><i>Note: Depending on the legislation being considered, the duty holder may be an end user, designer, supplier, integrator, installer or maintainer.</i></p>
Engineering/ design body	Engineering organisation carrying out application design but not equipment design, and potentially also procurement of SIS subsystems on behalf of the end user.
Installation	Setting down and fixing equipment in required locations, interconnection of services and signals, and unpowered testing of the equipment and connectivity.
Legacy system	Existing installed system which may or may not conform to current standards.