

**THE COLLECTION AND CATEGORISATION OF WORLDWIDE
STANDARDS RELEVANT TO THE USE OF PROGRAMMABLE
ELECTRONIC SYSTEMS IN SAFETY RELATED APPLICATIONS**

FINAL REPORT

ON WORK CARRIED OUT UNDER ORDER EC 9505531T FOR JRC ISPRA

BY

MEMBERS OF

THE EUROPEAN WORKSHOP ON INDUSTRIAL COMPUTER SYSTEMS

TECHNICAL COMMITTEE No. 7

Reliability, Safety & Security

EWICS TC7

July 1996

edited by

Meine van der Meulen

SIMTECH

and

Ian C Smith

Campbell Love Associates

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

THIS REPORT WAS PREPARED BY THE ORGANISATION(S) NAMED BELOW AS AN ACCOUNT OF WORK SPONSORED BY JRC ISPRA. NEITHER JRC ISPRA OR ANY MEMBER OF JRC ISPRA, THE ORGANISATION(S) NAMED BELOW, NOR ANY PERSON ACTING ON BEHALF OF ANY OF THEM;

(A) MAKES ANY WARRANTY OR REPRESENTATION WHATSOEVER, EXPRESS OR IMPLIED, (I) WITH RESPECT TO THE USE OF ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS REPORT, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, (II) THAT SUCH USE DOES NOT INFRINGE ON OR INTERFERE WITH PRIVATELY OWNED RIGHTS, INCLUDING ANY PARTY'S INTELLECTUAL PROPERTY, OR (III) THAT THIS REPORT IS SUITABLE TO ANY PARTICULAR USER'S CIRCUMSTANCE; OR

(B) ASSUMES RESPONSIBILITY FOR ANY DAMAGES OR OTHER LIABILITY WHATSOEVER (INCLUDING ANY CONSEQUENTIAL DAMAGES, EVEN IF JRC ISPRA OR ANY JRC ISPRA REPRESENTATIVE, OR THE ORGANISATION(S) NAMED BELOW OR ANY REPRESENTATIVE OF THESE ORGANISATION(S) HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) RESULTING FROM YOUR SELECTION OR USE OF THIS REPORT OR ANY INFORMATION, APPARATUS, METHOD, PROCESS, OR SIMILAR ITEM DISCLOSED IN THIS REPORT.

SIMTECH b.v.
CAMPBELL LOVE ASSOCIATES
EWICS TC7

Comments or questions to this report may be directed to

Udo Voges
Chairman EWICS TC 7
Forschungszentrum Karlsruhe
IAI
Postfach 3640
76021 Karlsruhe
GERMANY
udo.voges@iai.fzk.de

© EWICS TC7 2002

Contents

1.	Introduction	5
2.	Background	5
3.	Description of the project work program	6
4.	Details of work carried out.....	7
5.	Description of deliverables under the contract.....	7
6.	The next steps.....	8
7.	Conclusions and recommendations	9
8.	Appendices	9
8.1	List of Sectors and Countries	11
8.2	Coverage matrix	13
8.3	Details of individual contributions	15
8.4	Summaries of a sub-set of the identified standards.....	67
8.5	List of Standards Organisations	109

1. Introduction

This document describes work carried out by members of EWICS TC7 under a contract from JRC Ispra - Order No. EC 95095531 T. The work carried out was jointly funded by members affiliations and by the funding made available under the contract. The subject matter is “The Collection and Categorisation of Worldwide Standards relevant to the use of Programmable Electronic Systems in Safety Related Applications” and the work reported on was carried out within EWICS TC7 under the title of the EWICS TC7 Road Map Project.

EWICS TC7 (the European Workshop on Industrial Computer Systems - Technical Committee 7 Reliability, Safety & Security) meets four times per year. Its membership covers representatives from regulators, industrial users, researchers and members of standards committees. It produces guidelines, holds workshops and each October runs a specialist conference - SAFECOMP. EWICS TC7 has been an active group since the mid 70's - there is no restriction to membership - all interested experts are welcome to attend.

At the EWICS TC7 meeting held at Belgirate in October 1995, it was agreed in plenary session that a proposal should be submitted to JRC Ispra to carry out phase I of the Road Map project as a standalone activity. It was agreed that the proposal would be submitted by Campbell Love Associates - CLA on behalf of EWICS TC7. The contract with JRC Ispra would be taken on by CLA on behalf of EWICS TC7 and Ian Smith of Campbell Love Associates, would project manage the work.

2. Background

There exists a large and increasing volume of standards related to the manufacture and use of programmable electronic systems. There exist both national and international as well as sector specific standards. The burden imposed by the need to search through and interpret the wide range of documents available to ensure appropriate compliance is costly and time-consuming. This leads either to a high overhead to be recovered in the price of the end product or to running the risk of the product being non-compliant.

It was recognised by members of EWICS TC7 that it would be beneficial to industry, both vendors and users, and to regulators and standards organisations if a study could be undertaken of the existing standards to provide a road map through the mass of documents that currently exist. The work would involve making a collection of appropriate documents and then reviewing the collected documents against a life-cycle model or other basis. Out of this review process would hopefully emerge an appropriate structure for a guideline to aid interested parties in finding their way through to the specific documents most relevant to their needs. This broad concept formed the basis of the EWICS TC7 Road Map project. The end goal was to provide a guide through the standards both by country and by industrial sector.

As a first step the work described in this report was carried out viz. the collection of titles of relevant standards and other documents.

In carrying out the work use was made of the specific knowledge and experience of the members of EWICS TC7. Where expertise was not present within the existing membership approaches were made to individuals to provide suitable input.

3. Description of the project work program

At the EWICS TC7 meeting held at Belgirate in October 1995, the proforma attached to the proposal document as Appendix A was given out to a number of EWICS TC7 members. The members were invited to indicate on the proforma the areas that they personally could cover. On a second proforma attached to the proposal document as Appendix B, they were asked to add any categories that may have been overlooked in the Appendix A proforma.

Following this meeting completed proformas were received from 11 members and the data was entered into a database. The database had been developed by Meine van der Meulen prior to and outside of the work program being reported on in this document. Extensive use has however been made of the database in carrying out the work of the project. In addition contributions were made from other members of titles collected by accessing web sites on the Internet and by obtaining other collected titles.

By the time of the January 1996 meeting held at Cambridge, the database was populated with some 150 standards from several countries and application domains. At the Cambridge meeting forms were distributed to a further 5 members.

An editorial meeting was held at the SIMTECH offices at Rotterdam on 19 and 20 March 1996 and the data collected up to that time was reviewed to remove titles thought to be of only marginal relevance. By this time a number of summaries were also available and were entered into the database. The structure of the draft final report was agreed together with an outline of the contents of each of the sections.

A draft version of the final report was prepared and at the EWICS TC7 meeting at Hamburg in April this document and its contents were reviewed.

In June a final editorial meeting was held via e-mail and the final form of the deliverables was agreed.

The final version of the report was prepared and together with the other deliverables was sent to JRC Ispra on 26 July 1996.

4. Details of work carried out

A total of 35 EWICS TC7 members attended project meetings and contributed to discussion and debate regarding the collection of titles of relevant documents. Their names are given below.

Uwe Anders	Floor Koornneef
Stuart Anderson	Hamid Lesan
Helmut Bezecny	Christine Mazuet
Robin Bloomfield	Meine van der Meulen
George Cleland	Stuart Nunns
Andrew Coombes	Gerd Rabe
Ferdinand Dafelmair	Johannes Rainer
Peter Daniel	Erwin Schoitsch
Martyn Dowell	Ian Smith
L Emmet	Marcus Ullman
Wolfgang Ehrenberger	Michael Viola
Robert Genser	David Ward
Chris Gerrard	Albrecht Weinert
Janusz Gorski	Marc Willikens
Andy Harrison	Stefan Wittman
Dennis Inverso	William Wyatt-Millington
Jouko Jarvi	Z Zurakowski
Tjabbe Kloppenburg	

A total of 18 EWICS TC7 members provided specific input to the project and their names , together with details of their inputs are given in Appendix 9.5. All the collected data was entered by Meine van der Meulen into the database which he had previously developed. A list of the countries, application sectors and standards organisations represented within the list of titles was drawn up and is given in Appendix 9.3. Not all application sectors are represented in each of the countries and so a coverage matrix was prepared to show the coverage achieved. The coverage matrix is given in Appendix 9.4.

The list of titles was reviewed initially to remove any not felt to be sufficiently relevant. A draft final list was then reviewed to identify any serious omissions. The final list of titles is given in Appendix 9.6. A total of 493 titles were collected. Summaries were obtained for a subset of the identified documents. The text of 142 summaries is reproduced in Appendix 9.7.

5. Description of deliverables under the contract

The deliverables under the contract consist of:

- this report
- list of titles of relevant standards (included as Appendix 9.6 of this report)

- summaries of a subset of the collected titles (included as Appendix 9.7 of this report)
- a diskette containing files in Word 6.0 format of the text of this report and thus including the list of titles and of the summaries

6. The next steps

In light of the large number of standards that exist it will be necessary to provide some focus for the route ahead. It was proposed that this would be best achieved by identifying those standards and guidelines recognised by relevant Regulatory, Certifying and Testing Organisations or relevant Recognised User Groups. These organisations would need to be identified both by sector and by country. Some indication of the structure of the regulatory environment would also be beneficial.

The proposed route ahead for further work would be:

- to identify for each sector and each country
 - * the relevant Regulatory, Certifying and Testing Organisations
 - * the relevant Recognised User Groups
- to categorise collected standards and guidelines
 - * Required or mandated by regulatory bodies or recognised user groups
 - * Recommended or approved by regulatory bodies or recognised user groups
 - * Relevant and informative
- to review data already collected
 - * by sector
 - * by country
- to identify key missing data elements
 - * within the field of expertise of EWICS TC7 members
 - * outside the field of expertise of EWICS TC7 members

In an exploratory discussion already held, the following EWICS TC7 members indicated a willingness to identify for the following sectors and countries

- * the relevant Regulatory, Certifying and Testing Organisations

* the relevant Recognised User Groups

Z Zurakowski	Poland, Electrical Energy Sector (conventional)
Bill Wyatt-Millington	UK, Railway
Andy Coombes	UK Air
R Genser	Robotics, Security
E Schoitsch and J Rainer	Austria, Rail
S R Nunns	UK, Chemical
G Rabe	Germany, Medical and Industrial
D Ward	Automotive UK and (potentially) elsewhere
J Jarvi	Finland
U Anders	Germany, Medical and Industrial
H Lesan	various

This proposed route ahead should provide an insight as to the most appropriate structure for a guide through the available standards. The guide could be ordered by country or by application specific sector or both. The emphasis in the guidance document would be on the requirements laid down by the regulatory organisations and certification bodies and on the recommendations of recognised user groups.

7. Conclusions and recommendations

The work described in this report has confirmed the wide range of standards and related documents which exist covering the field of the use of computers in safety-related applications. The large number of relevant titles collected emphasises the desirability of providing a guide through the available documents.

A route ahead has been proposed which will identify those documents which are required by the relevant regulatory organisations and certification bodies in individual countries and application sectors. By this means an appropriate structure for a suitable guidance document can be developed with initial complete examples for selected countries and application sectors.

It is recommended that the feasibility of starting a new work item based on the above conclusions be investigated.

8. Appendices

THIS PAGE HAS BEEN LEFT DELIBERATELY BLANK

8.1 List of Sectors and Countries

<u>Application Specific Sectors</u>	<u>Countries</u>
Defence	Austria
Energy	Australia
Nuclear	Canada
Conventional	Finland
Industrial	France
Chemical	Germany
Oil & Gas	Holland
Food & Drugs	Japan
Process	Poland
Mining	Sweden
Medical	Turkey
Transportation	United Kingdom
Air	USA
Sea	
Road	
Rail	

8.2 Coverage matrix

Standards & Guidelines	Application specific sectors										
	Medical	Defence	Transportation				Industrial				Other General
			Air	Sea	Road	Rail	Chemical	Oil & Gas	Process	Nuclear	
Austria						X			X		
Australia											X
Canada										X	
Finland							X		X		
France						X				X	
Germany							X	X	X	X	
Holland	X										
Japan									X	X	
Poland		X							X	X	X
Sweden									X		
Turkey									X	X	X
United Kingdom		X	X			X			X	X	X
USA		X	X				X	X	X	X	X

8.3 Details of individual contributions

Ferdinand Dafelmair
Company: TUV BAYERN
Westendstrasse 199
D-80686 MUNCHEN
Phone: +49-89-57911464
Fax: +49-89-57912157

List of standards for the Energy - Nuclear in Germany

List of the relevant safety standards issued by Kerntechnischer Ausschuss (KTA) Geschäftsstelle and the approved draft safety standards

- KTA 3501 Reactor Protection System and Monitoring Equipment of the Safety System
- KTA 3502 Incident Instrumentation
- KTA 3503 Type Testing of Electrical Modules for the Reactor Protection System
- KTA 3504 Electrical Drives of the Safety System in Nuclear Power Plants
- KTA 3505 Type Testing of Sensors and Transducers of the Reactor Protection System
- KTA 3506 Tests and Inspections of the Instrumentation and Control Equipment of the Safety System of Nuclear Power Plants
- KTA 3507 Factory Tests, Post-Repair Tests and Demonstration of Successful Service for the Instrumentation and Control Equipment of the Safety System
- KTA 3705 Switchgear Facilities, Transformers and Distribution Networks for the Electrical Power Supply of the Safety System in Nuclear Power Plants
- KTA 3901 Communication Devices for Nuclear Power Plants

Andrew Coombes
Company: University of York
Heslington
YORK YO1 5DD
Phone: +44-1904-432787
Fax: +44-1904-432708

List of standards for the Transportation - Air in the UK

- ARP 4754 Certification considerations for Highly-Integrated or Complex Aircraft Systems by Systems Integration Requirements Task Group, AS-IC, ASD,
- MOD00-55 UK MoD Directorate of Standardization, Interim Defence Standard 00-55, The procurement of Safety Critical Software in Defence Equipment, 1991.

MOD00-56 UK MoD Directorate of Standardization, Interim Defence Standard 00-56, Requirements for the Analysis of Safety Critical Hazards, 1991.

DRA/CIS/6/5 DRA Systems Engineering Procedures (Draft copy)

Andy Harrison
Company: Railtrack
40 Bernard Street
LONDON WC1 N1BY
Phone: +44-171-922-2450
Fax:

List of standards for the Transportation- Rail sector in the UK and Europe

CENELEC prEN50126 Railway applications - The specification and demonstration of dependability - Reliability, Availability, Maintainability and Safety (RAMS), Draft 1.0, August 1995.

CENELEC prEN50128 Railway Applications: Software for Railway Control and Protection Systems.

CENELEC prEN50129 Railway Applications: Safety Related Electronic Railway Control and Protection Systems.

UK RIA 23 The RIA 23 specification applies the IEC65A procedures to railway signalling. It is based on three prime concepts: integrity levels, lifecycle models and roles/responsibilities of individuals and organisations.

UK RIA 24 Railway Industry Association (UK), Safety Related Software for Railways (Signalling).

UK HSE Railway Safety Case Regulation

UK HSE Safety Critical Work Regulations

UK HSE Transport and Works Act and Regulations

ISO9001 International Organization for Standardization, ISO 9001, Quality Systems - Model for Quality Assurance in Design/Development, Production, Installation and Servicing, 1987.

Christine Mazuet
Company: Schneider Electric
Usine M3
F-38050 GRENOBLE Cedex
Phone: +33-76-606480
Fax: +33-76-605787

List of standards applied to develop systems dedicated to the nuclear sector in France

RCC-E Design and construction rules for Electronic Components of PWR (pressurized water reactor) nuclear islands (it is the specific French recommendations guide accepted as the reference by the French authorities to deliver the equipment qualification. The following list is built up through standards issued from the RCC-E).

General Standards

- IEC 364-1 to 364-5 Building electrical installations
- IAEA 50-SG-D3 Protection systems and additional systems in nuclear power plants
- IAEA 50-SG-D8 Safety related instrumentation and driving systems in nuclear power plants
- IAEA 50-SG-D11 General safety rules in nuclear power plants design

Dependability and Testability standards

- IEC 231 Guidance for the design and use of components intended for mounting on boards with printed wiring and printed circuits
- IEC 671 Periodic test and monitoring of the protection system of nuclear reactors
- IEC 300-3-1 Dependability management. Part 3 : application guide - section 1 : analysis techniques for dependability : guide on methodology

Software standards

- IEC 880 Software for computers of nuclear power plants safety systems
- IEC 1131 Programmable Logic Controllers
- IEC 1226 Nuclear power plants - Instrumentation and control systems important to safety- Classification

Gerd Rabe
Company: TUV Nord e.V.
Grosse Bahnstrasse 31
D-22525 HAMBURG
Phone: +49-40-8557-2101
Fax: +49-40-8557-2429

List of standards for the Process and Chemical sectors in Germany

- DIN V 19250 Control technology; fundamental safety aspects to be considered for measurement and control equipment

DIN V 19251	Process control technology - MC protection equipment - Requirements and measures for safeguarded function
DIN VDE 801	Principles for computers in safety-related systems
DIN VDE 801/A1	Principles for computers in safety-related systems; Amendment A1:1994-10
DIN VDE 0116	Electrical equipment of furnaces
DIN IEC 880	Software for computers in the safety systems of nuclear power stations; identical with IEC 880, edition 1986
VDI/VDE 2180	Safeguarding of industrial processing plants by means of instrumentation and control technology; calculating methods for reliability characteristics of safety facilities
VDI/VDE 2180	Safeguarding of industrial processing plants by means of instrumentation and control technology; classification of measurement and control systems
ZHI/170	Safety rules for the control of printing and paper processing machines
TRbF 301/RFF	Guideline for long distance pipelines for the transportation of dangerous liquids - RFF -
TRA 200	Passenger elevators, freights elevators, goods elevators
DIN 13252	Inhalational anaesthetic apparatus, requirements for safety and testing
DIN 13254	Breathing machines; safety requirements and testing
DIN VDE 0750-215	Medical electrical equipment; lung ventilators; particular requirements for safety; identical with IEC 62D(Central Office)36
DIN VDE 0750-232	Medical electrical equipment; particular requirements for safety of infusion pumps and controllers; identical with IEC 62D(Central Office)61
IEC 1131	Programmable Logic Controllers
IEC TC65A	Various documents
IEC 9126	Information technology - Software product evaluation - Quality characteristics and guidelines for their use

Floor Koornneef

Company: TU Delft
Safety Science Group
Mekelweg 4
NL-2628 CD DELFT
Phone: +31-152786437
Fax: +31-152786437
+31-152622235

List of standards for the Medical sector in Holland

NPR 3137	1984 (2nd draft) Safe application of medical electrical equipment
NEN 3134	1986 Safety requirements for low-voltage installations in medically used rooms
NPR 10513 (=IEC 513)	1976 Basic aspects of the safety philosophy of electrical equipment used in medical practice
NEN 10 601-1 (=IEC 601-1)	1991 1988 Medical electrical equipment : Part 1: general safety requirements
NEN 10 601-2-1 (=IEC 601-2-1)	1983 1981 Part 2: Particular requirements for medical electron accelerators in the range 1 MeV to 50 MeV section 1: general section 2: radiation safety for equipment section 3: electrical and mechanical safety for equipment
NEN 10 601-2-2 (=IEC 601-2-2)	1985 1982 Part 2: Particular requirements for the safety of high frequency surgical equipment
NEN 10 601-2-4 (=IEC 601-2-4)	1985 1983 International Electrotechnical Commission, IEC 601-2-4, Medical Electrical Equipment; Part 2: Particular Requirements for the Safety of Cardiac Defibrillator Monitors, 1983.

Wolfgang Ehrenberger

Company: Fachhochschule Fulda
Marquardstrasse
D-3639 FULDA
Phone: +49-661-9640325
Fax: +49-661-9640349

List of standards for German industry and list of organisations

Michael Viola
Company: ONTARIO HYDRO
700 University Ave.
TORONTO, ONT. M5G 1X6
CANADA
Phone: +1-416-5928276
Fax: +1-416-5928802

Supply of three Canadian standards

Standard for Software Engineering of Safety Critical Software, CE-1001-STD Rev 1
Software Engineering of Category II Software, 907-C-H-69002-0100 Rev 0
Software Engineering of Category III Software, 907-C-H-69002-0200 Rev 0

Robin Bloomfield
Company: Adelard
3 Coburn Road
LONDON E3 2DA
Phone: +44-181-983-0217
Fax: +44-181-983-1845

Lists of standards from various sources

Review paper relating to standards

Chris Gerrard
Company: Gerrard Software Ltd
Venture House
Cross Street
Macclesfield
Cheshire, UK SK11 7PG
Phone: +44(0)1625-612846
Fax: +44(0)1625-616327

List of standards from

Contact name for UK Off-shore Oil standard

Information on ERA/DTI report on PLC's

Jouko Jarvi

Company: Technical Inspection Centre
Teknillinen tarkastuskeskus
P.O. Box 204
FIN-00181 HELSINKI
Phone: +358-0-616-7514
Fax: +358-0-616-7466

List of Finnish and Swedish recommendations, guidelines and directives on safety-related programmable control systems for the process industries.

Finnish documents

Audits of Safety Related Control Systems. TTK-Directive C1-94, 13.1.1994, Finland. Summary and main headings in available in English.

TTK-Recommendation 1 - 1994 - Guidelines for Safety Instrument Systems. Contents list available in English as Annex 1of TTK-Directive C1-94, 13.1.94. Full text of the recommendation in Finnish only.

Ohjelmoitavien turvallisuuteen liittyvien ohjausjärjestelmeihin arviointiohjeet. TTK-suositus 1-1994. Teknillinen tarkastuskeskus, Helsinki, 1994, 102p. ISBN 952-9588-48-8.
Paineastiat. Tarkastus, sijoitus, varustelu ja käyttö. SFS-kasikirja 15, 6, painos. Suomen Standardisoimisliitto SFS r.y., Helsinki, joulukuu 1993, 388p. ISBN 952-9591-49-7

Kattilalaitosten turvallisuusohjeet, Automaatio ja instrumentointi. Suojeluohje G 10, Teollisuusvakuutus, Helsinki, 1985, 18p. ISSN 0781-0261. (This is being thoroughly updated according to the principles of the draft IEC1508.)

Swedish documents

Anvisningar för icke-mekaniska saker hetsutrustningar. SIS-Tryckkarlskommissionen, Stockholm, December 1991, 21p. + i-page Annex. ISBN 91-85254-47-9

Meine van der Meulen
Company: SIMTECH b.v.
Oostmaaslan 71
NL-3063 AN ROTTERDAM
Phone: +31-10-4244386
Fax: +31-10-4244253

Use of developed database
Entry of data plus data management activities
Collection of ~100 titles
Summaries of standards

Ian Smith

Company: Campbell Love Associates
42, Widworthy Drive
Broadstone
Dorset, UK BH18 9BD
Phone: +44-1202-696205
Fax: +44-1202-696205

List of ANSI/IEEE standards
List of standards applicable to the nuclear sector in US
Project management activities
Preparation of draft final report

Company: Janusz Gorski
EFP
Mansfelda 4
P.O.Box 31
60-854 Poznan
Poland
Phone: +48 61 48 34 06
Fax: +48 61 48 35 82

Polish standards

The main standards Organisation in Poland is Polski Komitet Miar I Jakosci (Polish Committee of Measures and Quality)

List of standards

Nuclear

PN-89/j-01101
Control and safety systems of nuclear reactors

Avionics

PN-80/Z-08051 (OB)
Equipment of automatic flight control systems

General (industry)

PN-80/Z-8202 (OB)
Labor protection. Control elements of machines and devices used in production. General requirements

PN-93/T-42107 (OB)
Safety of information technology equipment and electric business equipment

PrPN-93/T-42107/A2
Safety of information technology equipment and electric business equipment

Mining

PN-93/G-50000

Labor protection. Machines and devices applied in mining. General requirements for safety and ergonomics.

Electricity

BN-85/5574-01

Signalisation of the high voltage danger zone - general requirements

Zdzislaw Zurakowski
Company: Institute of Power Systems Automation
ul. Wystawowa 1
51-618 Wroclaw
Poland
Phone: +48 71 48 42 21
Fax: +48 71 44 19 25

Recognised conventional electrical power sector worldwide standards

ANS/IEEE C 37.1-1987

Definition, specification and analysis of systems used for supervisory control, data acquisition, and automatic control

Type : Standard

Size : 48 pages

Scope : The standard applies to systems used for monitoring, switching, and controlling electrical apparatus in unattended or attended substations, generating stations, and power utilisation and conversion facilities. The standard does not apply to electromechanical or static, protective-relaying equipment.

Principal topics: definitions, functional characteristics, interfaces, environmental conditions, characteristics concerning: reliability; maintainability; availability; security; expandability; changeability; tests and inspections; documentation.

Keywords : Supervisory control, automatic control and data acquisition in electric power systems; functional characteristics; reliability; maintainability; availability; security; expandability; changeability; documentation.

ANSI/IEE STD 493-1990

IEEE Recommended practice for the design of reliable industrial and commercial power systems

Type : Recommended practice

Size : 415 pages

Scope : The fundamentals of reliability analysis as it applies to the planning and design of industrial and commercial electric power distribution systems are presented. The

presentation is self-contained and should enable trade-off studies during the design of industrial and commercial power systems.

Principal topics : Basic concepts of reliability analysis by probability methods, fundamentals of electric power systems reliability evaluation, economic evaluation of reliability, cost of power outage data, equipment reliability data, evaluation and improvement of the reliability of an existing plant, preventive maintenance, emergency and standby power, exemplified by reliability analysis and cost evaluation.

Keywords : Designing reliable industrial and commercial power systems, equipment reliability data, industrial and commercial power systems reliability analysis, reliability analysis.

Selected IEC and ISO standards.

Hazards analysis

IEC 1025(1990): Fault tree analysis

IEC TC56(Central office)137: Reliability block diagram method

Quality assurance and assessment

IEC 362(1971): Guide for collection of reliability, and maintainability data from field performance of electronic items

IEC TC65C/WG1: Time critical architecture

IEC TC65A/77B(Secretariat)135/100 Electromagnetic compatibility for electrical and electronic equipment. Part 3: Immunity to radiated radio-frequency electromagnetic fields

IEC TC65A/77B(Secretariat)136/101 Electromagnetic compatibility for electrical and electronic equipment. Part 5: Surge immunity requirements

IEC TC65A/77B(Secretariat)145/110 and 159/137 Electromagnetic compatibility for electrical and electronic equipment. Part 6: Immunity to conducted disturbances induced by radio-frequency fields

ISO TR12178; 1994 Industrial automation. time-critical communications architectures. User requirements.

Computer systems design

IEC TC65B(Secretariat)179 - IEC 1134-4 Programmable controllers. Part 4: User guidelines.

IEC TC65B(Secretariat)102 Guide to the implementation and application of programmable controllers languages.

IEC TC65A(U.S.A.)22 Programmable Electronic Systems (PES) for use in safety applications

ISO/IEC JTC1/SC22/WG19 IN9: VDM specification language prostandard, draft, 1991

Other standards

NF F 71-011 (French standard)

Railway fixed equipment and rolling stock, Data processing, Software dependability - General, 1990
NF F 71-012 (French standard)
Railway fixed equipment and rolling stock, Data processing, Software dependability - Constraints on software, 1990.
Pr F 71-013 (French standard)
Railway fixed equipment and rolling stock, Data processing, Software dependability - Adapted methods for software safety analysis.
ISO 1161
Industrial automation systems - Safety of integrated manufacturing systems - Basic requirements.
MOD 00-56
Ministry of Defence, Interim Defence Standard 00-56, Hazard Analysis and Safety Classification of the Computer and Programmable Electronic System Elements of Defence Equipment, Issue 1, 5 April 1991.

Erwin Schoitsch
Company: Seibersdorf Ges.m.b.H.
Osterreichisches Forschungszentrum
Seibersdorf
A-2444 Seibersdorf
Austria
Phone: +43 2254 780 3166
Fax: +43 2254 72133

Two references concerning Austrian Railway Standards

OeVE(Austrian Electrotechnical Association)-T3/1979 Elektrische Eisenbahnsicherungsanlagen und -geraete (Electrotechnical Railway Interlocking Systems and Devices)
OeVE-T3a/1983 Nachtrag a zu den Bestimmungen ueber Elektrische Eisenbahnsicherungsanlagen und -geraete (Addendum a to the Standards for Electrotechnical Railway Interlocking Systems and Devices)

Other relevant standards e.g. in the context of electricity providers.

OeNORM M 8100 (1.4.1985) (teilw. uebereinstimmend mit (partially identical with) DIN 31051 (1982)) Instandhaltung von Anlagen, Maschinen und Geraeten: Benennungen, Definitionen und Massnahmen (Maintenance of plants (facilities), machinery and devices: naming conventions, definitions and measures).

OeNORM M 8103 (1.4.1989) Zuverlaessigkeit und Verfuegbarkeit von Anlagen, Maschinen und Geraeten (Reliability and Availability of plants (facilities), Machinery and devices).

NOTE: These standards are now input to CEN 319 standards on Maintenance.
Markus Ullman and Stefan Wittman

Company: B.S.I.
Godesberger Allee 183
Postfach 20 03 63
Bonn
Germany
Phone: +49 228 9582 142
Fax: +49 228 9582 455

List of standards on security.

8.4 List of standards identified

AFSC88

Department of the Air Force, Headquarters Air Force Systems Command, Andrews Air Force Base DC 20334-5000 Headquarters Air Force Logistics Command, Wright-Patterson Air Force Base OH 45433-5001, Software Risk Abatement, AFSC/AFLC Pamphlet 800-45, 30 September 1988.

AIAA013

AIAA, ANSI/AIAA R-013, Recommended Practice for Software Reliability, 1992.

AIChE CCPS93

American Institute of Chemical Engineers, Center for Chemical Process Safety, Guidelines for the Safe Automation of Chemical Processes, New York, 1993, ISBN 0816905541.

ALLIANZ87

Allianz Versicherungs AG, Allianz Handbook of Loss Prevention, 1987, ISBN 3924934010, ISBN 3184191036.

AMJ25.1309

Joint Airworthiness Authority, AMJ25.1309 (Advisory Material Joint relating to JAR25.1309), System Design and Analysis, Amendment 90/1, 1990.

ANS4.1

American Nuclear Society, ANS 4.1, Design Basis Criteria for Safety Systems in Nuclear Power Generating Stations, 1978.

ANS4.5

American Nuclear Society, ANS 4.5, Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors, 1980.

ANS8.3

American Nuclear Society, ANS 8.3, Criticality Accident Alarm System, 1986.

ARP 4754

Certification considerations for Highly-Integrated or Complex Aircraft Systems by Systems Integration Requirements Task Group, AS-IC, ASD, SAE

AS2529

Standards Australia, AS2529, Collection of reliability, availability and maintainability data for electronics and similar engineering use, 1982.

AS3563

Standards Australia, Australian Standard 3563, Software Quality Management System, 1991 (Adopted by IEEE as IEEE-Std-1298, 1992).

AS3563-2

Standards Australia, AS 3563-2, Software quality management system - Implementation guide, 11-4-1991.

AS3900-1

Standards Australia, AS 3900-1, Quality management and quality assurance Standards-Guidelines for selection and use, 1987.

AS3900-4

Standard Australia, AS 3900-4, Quality management and quality assurance Standards-Guide to dependability program management, 18 April 1994.

AS3930

Standards Australia, AS 3930, Reliability and maintainability - Introductory guide, 17 January 1992.

AS3960

Standards Australia, AS 3960, Guide to reliability and maintainability program management, 1990.

ASAE EP456

ASAE, ASAE EP456, Test and Reliability Guidelines (R 1991).

ASME NQA1

American Society of Mechanical Engineers, ASME NQA-1, Quality Assurance Requirements for Nuclear Facility Applications, 1994.

ASME NQA2a

American Society of Mechanical Engineers, ASME NQA-2a-1990, Part 2.7, Quality Requirements of Computer Systems for Nuclear Facility Applications, 1990.

AT&T90

Klinger, D.J., Y. Nakada, M.A. Menendez, AT&T Reliability Manual, Van Nostrand Reinhold, New York, 1990, ISBN 0 442 31848 0.

BCS SCT

British Computer Society Specialist Group in Software Testing, Draft Standard for Software Component Testing, Edited by D.R. Graham, Grove Consultants, 9 November 1990.

BCS81205

British Computer Society, 81205, System Safety Instruction - System Safety Engineering in Software Development, 1989.

BS3811

British Standards Institute, BS3811, Glossary of terms used in terotechnology, 15 December 1993.

BS4778

British Standards Institution, BS 4778, Part 1, Quality Vocabulary - International Terms, May 1987.

BS5750-13

British Standards Institution, Quality systems. Guide to the application of BS5750: Part 1 to the development, supply and maintenance of software.

BS5750-14

British Standards Institution, BS5750, part 14, Quality systems. Guide to dependability programme management, 15 November 1993.

BS5760-0

British Standards Institution, BS5760, Part 0, Reliability of constructed or manufactured products, systems, equipments and components. Introductory guide to reliability, 31 October 1986.

BS5760-1

British Standards Institution, BS5760, Part 1, Reliability of constructed or manufactured products, systems, equipments and components. Guide to reliability and maintainability programme management, 29 November 1985.

BS5760-10

British Standards Institution, BS5760, Part 10, Reliability of systems, equipment and components. Guide to reliability testing, 15 February 1993.

BS5760-10.3

British Standards Institution, Reliability of systems, equipment and components. Guide to reliability testing. Design of test cycles, 1993.

BS5760-10.5

British Standards Institution, BS5760-10.5, Reliability of systems, equipment and components. Guide to reliability testing. Compliance test plans for success ratio, 1993.

BS5760-11

British Standards Institution, BS5760, Part 11, Reliability of systems, equipment and components. Collection of reliability, availability, maintainability and maintenance support data from the field, 15 August 1994.

BS5760-12

British Standards Institution, BS5760, Part 12, Reliability of systems, equipment and components. Guide to the presentation of reliability, maintainability and availability predictions, 15 November 1993.

BS5760-13

British Standards Institution, BS5760, Part 13, Reliability of systems, equipment and components. Guide to reliability test conditions for consumer equipment. Conditions providing a low degree of simulation for indoor portable equipment, 15 December 1993.

BS5760-13.2

British Standards Institute, Reliability of systems, equipment and components. Guide to reliability test conditions for consumer equipment. Conditions providing a high degree of simulation for equipment for stationary use in weatherprotected locations, 15 December 1993.

BS5760-13.3

British Standards Institute, BS5760-13.3, Reliability of systems, equipment and components. Guide to reliability test conditions for consumer equipment. Conditions providing a low degree of simulation for equipment for stationary use in partially weatherprotected locations, 1993.

BS5760-13.4

British Standards Institution, BS5760-13.4, Reliability of systems, equipment and components. Reliability test conditions for consumer equipment. Conditions providing a low degree of simulation for equipment for portable and non-stationary use, 1993.

BS5760-14

British Standards Institution, BS5760, Part 14, Reliability of systems, equipment and components. Guide to formal design review, 15 October 1993.

BS5760-15

British Standards Institution, BS5760, Part 15, Reliability of systems, equipment and components. Guide to the application of Markow techniques, 15 July 1995.

BS5760-2

British Standards Institution, BS5760, Part 2, Reliability of systems, equipment and components. Guide to the assessment of reliability, 15 October 1994.

BS5760-3

British Standards Institution, BS5760, Part 3, Reliability of systems, equipments and components. Guide to reliability practice: examples, 30 July 1982.

BS5760-4

British Standards Institution, BS5760, Part 4, Reliability of constructed or manufactured products, systems, equipments and components. Guide to specification clauses relating to the achievement and development of reliability in new and existing items, 30 September 1986.

BS5760-5

British Standards Institution, BS5760, Part 5, Reliability of systems, equipment and components. Guide to failure modes, effects and criticality analysis (FMEA and FMECA), 20 December 1991.

BS5760-6

British Standards Institution, BS5760, Part 6, Reliability of systems, equipment and components. Guide to programmes for reliability growth, 29 November 1991.

BS5760-7

British Standards Institution, BS5760, Part 7, Reliability of systems, equipment and components. Guide to fault tree analysis, 20 December 1991.

BS5760-9

British Standards Institution, BS5760-9, Reliability of systems, equipment and components. Guide to the block diagram technique, 1994.

BS61078

British Standards Institution, BS EN 61078, Reliability of systems, equipment and components. Guide to the block diagram technique, 15 October 1992.

BS6913-7

British Standards Institution, BS6913, Part 7, Operation and maintenance of earth-moving machinery. Glossary for machine availability, 28 June 1991.

BS7501

British Standards Institution, BS7501, General criteria for the operation of testing laboratories, 1989.

BS97714

British Standards Institution, Draft for Development Document 89/97714, Guide to the Assessment of Reliability of Systems Containing Software, 12 September 1989.

BSI HB10007

British Standards Institution, HB10007, Reliability, Maintainability and Risk, 1 January 1992.

BSI-ST

British Standards Institution, Draft Standard, Edited by D.R. Graham, Grove Consultants, for the British Computer Society Specialist Group in Software Testing, Issue 1.2, 9 November 1990.

BSI22

British Standards Institution, BSI Handbook NO.22 Part 2, Reliability and Maintainability (G), 1992.

BSI7105

Bundesamt fuer Sicherheit in der Informationstechnik, BSI7105, Handbuch fuer sichere Anwendung der Informationstechnik, Version 1.0, Maerz 1992.

BSI7119

Bundesamt fuer Sicherheit in der Informationstechnik, BSI 7119, BSI-Zertifizierung - Kriterien fuer die Begutachtung von Software-Werkzeugen.

BfA FB664

Bundesanstalt fuer Arbeitsschutz, FB664, Software-Diversitaet fuer Steuerungen mit Sicherheitsverantwortung.

CAA B7-1

CAA, Chapter B7-1 APP 08.83, General Reliability.

CAA J2-1

CAA, Chapter J2-1 APP#3 09.66, System Reliability.

CAA K6-12

CAA, Chapter K6-12 APP1 10.92, Systems Reliability.

CE-1001-STD

Candu Computer Systems Engineering Centre of Excellence, Standard for Software Engineering of Safety

Critical Software, CE-1001-STD, Revision 1, January 1995.

CEN TC44-232

CEN, CEN/TC44x/JWG6/N232, Safety related parts of control systems, safety of machinery, design categories, 1992.

CEN prEN50121-4

CEN/CENELEC, prEN50121-4, Railway Applications: Electro-Magnetic Compatibility (EMC) - Requirements for Signalling and Telecommunications.

CEN prEN50124

CEN/CENELEC, prEN50124, Railway Applications: Insulation Coordination.

CEN prEN50126

DIN, prEN50126, Railway applications - The specification and demonstration of dependability - Reliability, Availability, Maintainability and Safety (RAMS), Draft 1.0, August 1995.

CEN prEN50126-2

CEN/CENELEC, prEN50126-2, Dependability (RAMS) for Guided Transport Systems - Part 2: Safety.

CEN prEN50127

CENELEC, prEN50127, Guide to the Specification of a Guided Transport System.

CEN prEN50128

CEN/CENELEC, prEN50128, Railway Applications: Software for Railway Control and Protection Systems.

CEN prEN50129

CEN/CENELEC, prEN50129, Railway Applications: Safety Related Electronic Railway Control and Protection Systems.

CEN prEN50155-2

CEN/CENELEC, prEN50155-2, Railway Applications: Electronic Equipment used in Fixed Installations.

CEN/TC114

CEN/TC114 N221, Safety of Machinery: Principles for the Design of Safety Related Control Systems, 1991.

CENELEC HD485

CENELEC HD 485, Analysis Techniques for System Reliability - Procedure for Failure Mode and Effects Analysis (FMEA).

CEPT45

CEPT T/N 45-01 E, Testing the Compliance of an Equipment with Its Reliability, Maintainability and Availability Specifications.

CFR50.59

Code of Federal Regulations, Part 50.59, Changes, Tests, and Experiments.

CFR50.62

Code of Federal Regulations, Part 50.62, Requirements for Reduction of Risk from Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants.

CFR50.90

Code of Federal Regulations, Part 50.90, Application for Amendment of Licence or Construction Permit.

CNS B8006

CNS B8006, Glossary of Terms for Reliability (General).

CNS C5029

CNS C5029, General Rules for Reliability Assured Electronic Components.

CNS C5155

CNS C5155, Data Processing Vocabulary; Part 14: Reliability, Maintenance and Availability.

CNS C6303

CNS C6303, Method of Test for Reliability of Household Audio Product.

CNS C6304

CNS C6304, Method of Test for Reliability of Video Product.

CSA286

Canadian Standards Association, CAN3-N286.2-86, Design Quality Assurance for Nuclear Power Plants, 1986.

CSA286.2

Canadian Standards Association, CAN3-N286.2-86, Design Quality Assurance for Nuclear Power Plants, 1986.

CSA396.1.1

Canadian Standards Association, CAN/CSA-Q396.1.1-89, Quality Assurance Program for the Development of Software Used in Critical Applications, 1989.

CSA396.1.2

Canadian Standards Association, CSA Q 396.1.2, Quality Assurance Program for Previously Developed Software Used in Critical Applications, 1989.

CTCPEC

CTCPEC, Canadian Trusted Computer Product Evaluation Criteria.

DIN0116

Deutsches Institut fuer Normung, DIN VDE 0116, Electrical equipment of furnaces, October 1989.

DIN0298

Deutsches Institut fuer Normung, DIN EN 298, Automatic gas burner control systems for gas burners and gas burning appliances with or without fan, February 1994.

DIN0801

Deutsches Institut fuer normung, DIN V/VDE 0801, Principles for Computers in Safety-Related Systems, 1989.

DIN19250

Deutsches Institut fuer Normung, DIN V 19250, Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen, May 1994.

DIN19251

Deutsches Institut fuer Normung, DIN-V-19251, Process control technology - MC protection equipment - Requirements and measures for safeguarded function.

DIN31000

Deutsches Institut fuer Normung, DIN 31000/VDE 1000, General Guide for Designing of Technical Equipment to Satisfy Safety Requirements, 1979.

DIN40041

Deutsches Institut fuer Normung, DIN40041, Zuverlaessigkeit, Begriffe.

DIN44300/1

Deutsches Institut fuer Normung, DIN 44300 part 1, Information Processing; Definitions; General Definitions.

DIN61069-5

Deutsches Institut fuer Normung, DIN61069-5, Industrial-process measurement and control - Evaluation of system properties for ..., September 1995.

DIN61078

Deutsches Institut fuer Normung, DIN 61078, Analysis techniques for dependability - Reliability block diagram method ..., October 1994.

DOD AFISC SSH 1-1

Department of Defence, AFISC SSH 1-1, Software System Safety, 1985.

DOD MIL0105E

MIL-HDBK-0105E, Sampling Procedures and Tables for Inspection by Attributes.

DOD MIL0108

MIL-Hdbk-H-108, Sampling Procedures and Tables for Life and Reliability Testing (Based on Exponential Distribution).

DOD MIL0189

MIL-Hdbk-189, Reliability Growth Management.

DOD MIL0202

MIL-Std-202F, Test Methods for Electronic and Electrical Component Parts.

DOD MIL0217

MIL-Hdbk-217f, Reliability Prediction of Electronic Equipment, DoD Washington, Rev. F, Not. 1, 1992.

DOD MIL0280

MIL-Std-280, Definition of Item Levels, Item Exchangeability, Models and Related Terms.

DOD MIL0338

MIL-Hdbk-338, Electronics Reliability, Design, 1989.

DOD MIL0470B

MIL-Std-470b, Maintainability program for systems and equipment, 1989.

DOD MIL0471A

MIL-Std-471a, Maintainability Demonstration, 1978.

DOD MIL0472

MIL-HDBK-472, Maintainability Prediction, Not. 1, 12 June 1984.

DOD MIL0483

MIL-Std-483a, Configuration Management Practices for Systems, Equipment, Munitions, and Computer Programs, Rev. A, Not. 1, 1992.

DOD MIL0690C

MIL-Std-690C, Failure Rate Sampling Plans and Procedures.

DOD MIL0721C

MIL-Std-721c, Definitions of Terms for Reliability and Maintainability, Rev. C, Not. 1, 1992.

DOD MIL0728

MIL-HDBK-728, NonDestructive Testing (NDT).

DOD MIL0756B

MIL-Std-756B, Reliability Modeling and Prediction.

DOD MIL0764

MIL-Hdbk-764, System Safety Engineering Design Guide for Army Materiel, 1990.

DOD MIL0781

MIL-Std-781, Reliability Testing for engineering and development, qualification and production.

DOD MIL0781D

MIL-Std-781D, Reliability Design Qualification and Production Acceptance Tests: Exponential/ Distribution.

DOD MIL0785B

MIL-Std-785b, Reliability Program for Systems and Equipment Development and Production, Rev. B, Notice 2, 1988.

DOD MIL0790E

MIL-Std-790E, Reliability Assurance Program for Electronic Parts Specifications.

DOD MIL0791

DOD-Hdbk-791, Maintainability Design Techniques.

DOD MIL0810

MIL-Std-810, Environmental test methods and engineering guidelines.

DOD MIL0882C

MIL-Std-882C, System Safety Program Requirements, 1993.

DOD MIL0883

MIL-Std-883, Test methods and procedures for microelectronics, 1995.

DOD MIL0973

MIL-Std-973, Configuration Management, Not. 1, 1992.

DOD MIL1521

MIL-Std-1521b, Technical Reviews and Audits for Systems, Equipments and Computer Software, Rev. B, Not. 1, 1985 (superseded by MIL-Std-973).

DOD MIL1543B

MIL-STD-1543B, Reliability Program Requirements for Space and Missile Systems.

DOD MIL1574

MIL-Std-1574, System Safety Program for Space and Missile Systems, 1979

DOD MIL1576

MIL-Std-1576, Electroexplosive Subsystem Safety Requirements and Test Methods for Space Systems.

DOD MIL1591
MIL-Std-1591, On Aircraft, Fault Diagnosis, Subsystems, Analysis/Synthesis of

DOD MIL1629A
MIL-Std-1629A, Procedures for performing a Failure Mode Effects Analysis.

DOD MIL1843
MIL-Std-1843, Reliability-Centered Maintenance for Aircraft, Engines and Equipment.

DOD MIL2074
MIL-Std-2074, Failure Classification for Reliability Testing.

DOD MIL2084
MIL-Std-2084, Maintainability of avionic and electronic systems and equipment.

DOD MIL2155
MIL-Std-2155, Failure Reporting, Analysis and Corrective Action System (FRACAS).

DOD MIL2164
MIL-Std-2164, Environmental Stress Screening process for electronic equipment, 1985.

DOD MIL2165A
MIL-Std-2165a, Testability program for electronic systems and equipments, 1993.

DOD MIL2173
MIL-Std-2173, Reliability-Centered Maintenance Requirements for Naval Aircraft, Weapons Systems and Support Equipment.

DOD MIL45662
MIL-Std-45662, Calibration System Requirements.

DOD1679
Department of Defence, DOD-Std-1679a, Software Development, Rev. A, 1983
(superseded by DOD-Std-2167).

DOD2167
Department of Defence, DOD-Std-2167a, Defence System Software Development, Rev. A,
1988.

DOW22
Dow Europe, Critical Instrument Systems, European Safety Guide Number 22, 3rd Version,
March 1995.

EIA JEP70
Electronics Industry Association, EIA JEP70, Quality and Reliability Standards.

EIA RB4-A
Electronics Industry Association, EIA RB4-A, Reliability Quantification.

EIA RB9

Electronics Industry Association, EIA RB9, Failure Mode and Effect Analyses.

EIA SEB6-A

Electronics Industry Association, SEB 6-A, System Safety Engineering in Software Development, 1990.

EN22247

CEN/CENELEC, EN22247, Packaging: Vibration Test.

EN22248

CEN/CENELEC, EN22248, Packaging: Vertical Impact Test.

EN292

EN292, Safety of Machinery - Basic Concepts, General Principles for Design, 1991.

EN418

Nederlands Normalisatie Instituut, EN418, Safety of machinery. Emergency stop equipment, functional aspects. Principles for design.

EN45001

EN 45001, Algemene Criteria voor het Functioneren van Beproevinglaboratoria, November 1991.

EPRI NP5652

Electric Power Research Institute, EPRI NP-5652, Utilization of Commercial Grade Items in Nuclear Safety Related Applications.

EPRI TR100516

Electric Power Research Institute, EPRI TR-10051, Nuclear Power Plant Equipment Qualification Reference Manual.

EPRI TR102323

Electric Power Research Institute, EPRI TR-102323, Guide to Electromagnetic Interference Susceptibility Testing for Digital Safety Equipment in Nuclear Power Plants.

EPRI TR7343

Electric Power Research Institute, EPRI TR-7343, Integrated Instrumentation and Control Upgrade Plan.

ERRI A155-RP01 European Rail Research Institute, Review of published literature and analysis of applications, September 1982.

ERRI A155-RP02

European Railway Research Institute, Theoretical background of transmission of safety information, December 1982.

ERRI A155-RP03

European Rail Research Institute, Software for safety systems - an overview, April 1985.

ERRI A155-RP04

European Rail Research Institute, A survey of the available measures for the protection of safety information during transmission, September 1984.

ERRI A155-RP05

European Rail Research Institute, Errors in digital transmission systems, April 1985.

ERRI A155-RP06

European Rail Research Institute, Computer based safety systems requirements specification, September 1985.

ERRI A155-RP07

European Rail Research Institute, The design of computer based safety systems, April 1986.

ERRI A155-RP08

European Rail Research Institute, On proving the safety of transmission systems, April 1986.

ERRI A155-RP09

European Rail Research Institute, Software design for computer based safety systems, September 1986.

ERRI A155-RP10

European Rail Research Institute, Transmission of safety information using non-safety-specific systems or equipment, September 1987.

ERRI A155-RP11

European Rail Research Institute, Proof of safety of computer-based safety systems, September 1987.

ERRI A155-RP12

European Rail Research Institute, Failure catalogue for electronic components, April 1988.

ERRI A155-RP13

European Rail Research Institute, Recommendations for protection techniques and standards appropriate to the transmission of safety information, April 1988.

ESA-01-21

European Space Agency, ESA PSS 01-21, Software Product Assurance Requirements for ESA Space Systems, Issue 2, May 1991.

ESA-01-40

European Space Agency, ESA PSS-01-40, System Safety Requirements for ESA Space Systems and Associated Equipment, 1988

ESA-01-404

European Space Agency, ESA-01-404, Risk Assessment Requirements and Methods, Issue 1, May 1992.

ESA-05-0

European Space Agency, ESA PSS-05-0, Guide to the Software Engineering Standards, 1991.

ESA-05-01

European Space Agency, ESA PSS-05-01, Guide to the Software Engineering Standards, Issue 1, October 1991.

ESA-05-02

European Space Agency, ESA PSS-05-02, Guide to the User Requirements Definition Phase, Issue 1, October 1991.

ESA-05-03

European Space Agency, ESA PSS-05-03, Guide to the Software Requirements Definition Phase, Issue 1, October 1991.

ESA-05-04

European Space Agency, ESA PSS-05-04, Guide to the Software Architectural Design Phase, Issue 1, January 1992.

ESA-05-05

European Space Agency, ESA PSS-05-05, Guide to the Software Detailed Design Production Phase, Issue 1, May 1992.

EURO DEC/81/11953

EURO DEC/81/11953, Reliability Military Data Exchange guide.

EURO EC/EEPSG

EURO EC/EEPSG/73/1944, Standard Format for Presentation of Reliability and Maintainability Information for Equipment Suppliers to Prime Constructors.

EURO PSC/83

EURO PSC/83/12418, Supply of Basic Maintainability and Reliability Data.

EURO11953

EURO DEC/81/11953, Reliability Military Data Exchange guide (2nd Edition).

EURO12418

EURO PSC/83/12418, Supply of Basic Maintainability and Reliability Data.

EURO1944

EURO EC/EEPSG/73/1944, Standard Format for Presentation of Reliability and Maintainability Information for Equipment Suppliers to Prime Constructors.

HSE87

Health and Safety Executive, Software for Computers in Safety Related Applications, London 1991.

IAEA-50-SG-D11

International Atomic Energy Agency, IAEA-50-SG-D11, Safety Related Instrumentation and Driving Systems in Nuclear Power Plants.

IAEA-50-SG-D3

International Atomic Energy Agency, IAEA-50-SG-D3, Protection Systems and Additional Systems in Nuclear Power Plants.

IAEA-50-SG-D8

International Atomic Energy Agency, IAEA-50-SG-D8, Safety Related Instrumentation and Driving Systems in Nuclear Power Plants.

IAEA-QA

International Atomic Energy Agency, Manual on Quality Assurance for Computer Software, April 1987.

ICChE85

Institute of Chemical Engineers, Nomenclature for Hazard and Risk Assessment in the Process Industries, 1985, ISBN 852951841.

IEC TC45A-184

International Electrotechnical Commission, TC45A(Sec)184, Nuclear Power Plants - Instrumentation and Control Systems Important to Safety - Functional Requirements for Multiplexed Data Transmission Systems (draft), 1994.

IEC TC48B-286

International Electrotechnical Commission, TC48B(Sec)286, Technical report; guide for estimating the reliability of electrical connectors ..., February 1994.

IEC TC56-107

International Electrotechnical Commission, TC56(Central Office)107, Electrical engineering; equipment reliability testing; part 2: guidance for the ..., November 1985.

IEC TC56-137

Reliability block diagram method

IEC TC56-148

International Electrotechnical Commission, TC56(Central Office)148, Guide on Formal Design Review.

IEC TC56-150

International Electrotechnical Commission, TC56(Secretariat)150, Reliability Growth Models and Estimation Models.

IEC TC56-269

International Electrotechnical Commission, TC56(Secretariat)269, Parts Count Reliability Prediction.

IEC TC56-273

International Electrotechnical Commission, TC56(Secretariat)273, Reliability growth models and estimation models.

IEC TC56-280

International Electrotechnical Commission, TC56(Secretariat)280, Application of Markov Techniques.

IEC TC56-311

International Electrotechnical Commission, TC56(Sec)311, Analysis of reliability and maintainability of software, 1989.

IEC TC56-341

International Electrotechnical Commission, IEC 56(secretariat)341, IEC-300-Dependability Complement to ISO9000.

IEC TC56-349

International Electrotechnical Commission, TC56(Sec)349, Dependability management; part 3: application guide; section X: software aspects ..., November 1992.

IEC TC56-359

International Electrotechnical Commission, TC56, IEC56(Sec)359, Dependability management. Part 2. Guide to dependability programme elements and ..., 10 March 1992.

IEC TC56-373

International Electrotechnical Commission, TC56(Sec)373, Dependability management. Part 3. Application guide. Section X. Guide to the spe ..., 15 August 1994.

IEC TC65-298

International Electrotechnical Commission, IEC TC65 (Industrial-Process Measurement and Control) WG4 (Electromagnetic Interference), prEN298, Electromagnetic Compatibility for Industrial-Process Measurement and Control Equipment, Part 5: Surge Immunity Requirements, 1992.

IEC TC65A-22

Programmable Electronic Systems (PES) for use in safety applications (U.S.A.)

IEC TC65A-94

International Electrotechnical Commission, TC65A(Sec)94, Software for Systems in the Application of Industrial Safety-Related Systems, August 1989 (Superseded by IEC TC65A-122).

IEC TC65A-96

International Electrotechnical Commission, TC65A(Sec)96, Functional Safety of Programmable Electronic Systems - Generic Aspects (Superseded by IEC TC65A-123).

IEC TC65A-122

International Electrotechnical Commission, TC65A(Sec)122, Software for Systems in the Application of Industrial Safety-Related Systems, November 1991 (Superseded by IEC 1508).

IEC TC65A-123

International Electrotechnical Commission, TC65A(Sec)123, Functional Safety of Electrical/Electric/Programmable Electronic Safety-Related Systems - Generic Aspects, 1992 (Superseded by IEC 1508).

IECTC65A-135/100

Electromagnetic compatibility for electrical and electronic equipment. Part 3: Immunity to radiated radio-frequency electromagnetic fields

IEC TC65A-136/101

Electromagnetic compatibility for electrical and electronic equipment. Part 5: Surge immunity requirements

IEC TC65A-145/110

Electromagnetic compatibility for electrical and electronic equipment. Part 6: Immunity to conducted disturbances induced by radio-frequency fields (and IEC TC65A-159/137)

IEC TC65B-102

Guide to the implementation and application of programmable controllers languages.

IEC0050(191)

International Electrotechnical Commission, IEC 50(191), International Electrotechnical Vocabulary - Chapter 191: Dependability and Quality of Service, August 1994.

IEC0050(303)

International Electrotechnical Commission, IEC 50(303), International Electrotechnical Vocabulary - Chapter 303: Electronic Measuring Instruments, 1983.

IEC0050(351)

International Electrotechnical Commission, IEC 50(351), International Electrotechnical Vocabulary - Chapter 351: Automatic Control, 1975.

IEC0050(55)

International Electrotechnical Commission, IEC 50(55), International Electrotechnical Vocabulary - Chapter 55: Telegraphy and Telephony, 1970.

IEC0068

International Electrotechnical Commission, IEC 68, Environmental testing.

IEC0077

International Electrotechnical Commission, IEC 77, Rules for Electric Traction Equipment, 1977.

IEC0231

International Electrotechnical Commission, IEC 231, Guidance for the Design and Use of Components Intended for Mounting on Boards with Printed Wiring and Printed Circuits.

IEC0271

International Electrotechnical Commission, IEC 271, List of Basic Terms, Definitions and Related Mathematics for Reliability, 1974.

IEC0300

International Electrotechnical Commission, IEC 300, Reliability and Maintainability Management, 2nd Edition, 1984.

IEC0300-1

International Electrotechnical Commission, IEC 300-1, Dependability management; part 1: dependability programme management, April 1993.

IEC0300-3-1

International Electrotechnical Commission, IEC 300-3-1, Dependability management; Part 3: application guide; Section 1: analysis techniques for reliability: Guide on methodology, November 1991.

IEC0300-3-2

International Electrotechnical Commission, IEC 300-3-2, Dependability management; part 3: application guide; section 2: collection of dependability data from the field, October 1993.

IEC0300-3-9

International Electrotechnical Commission, IEC 300-3-2, Dependability management; part 3: application guide; section 9: Risk analysis of technological systems, October 1993.

IEC0319

International Electrotechnical Commission, IEC 319, Presentation of reliability data on electronic components (or parts), 1978.

IEC0362

International Electrotechnical Commission, IEC 362, Guide for Collection of Reliability, Availability and Maintainability Data from Field Performance of Electronic Items, 1971. (Currently under revision as TC56(Secretariat)267).

IEC0409

International Electrotechnical Commission, IEC 409, Guide for the inclusion of reliability clauses into specifications for component (or parts) for electronic equipment, 1981.

IEC0410

International Electrotechnical Commission, IEC 410, Sampling plans and procedures for inspection by attributes, 1973.

IEC0419

International Electrotechnical Commission, IEC 419, Guide for the inclusion of lot-by-lot and periodic inspection procedures in specifications for electronic components (or parts), 1973.

IEC0513

International Electrotechnical Commission, IEC 513, Basic Aspects of the Safety Philosophy of Electrical Equipment Used in Medical Practice.

IEC0571

International Electrotechnical Commission, IEC 571, Electronic Equipment used on Rail Vehicles.

IEC0601-1

International Electrotechnical Commission, IEC 601, Medical Electrical Equipment; Part 1: General Requirements for Safety, 1991.

IEC0601-2-2

International Electrotechnical Commission, IEC 601-2-2, Medical Electrical Equipment; Part 2: Particular Requirements for the Safety of High Frequency Surgical Equipment, 1982.

IEC0601-2-4

International Electrotechnical Commission, IEC 601-2-4, Medical Electrical Equipment; Part 2: Particular Requirements for the Safety of Cardiac Defibrillator Monitors, 1983.

IEC0605-1

International Electrotechnical Commission, IEC 605-1, Equipment reliability testing. Part 1 : General requirements, 1978, 1st amendment 1982.

IEC0605-2

International Electrotechnical Commission, IEC 605-2, Equipment reliability testing - Part 2: Design of test cycles, 1994.

IEC0605-3-1

International Electrotechnical Commission, IEC 605-3, Equipment reliability testing. Part 3 : Preferred test conditions. Indoor portable equipment - Low degree of simulation, 1986.

IEC0605-3-2

International Electrotechnical Commission, IEC 605-3-2, Equipment reliability testing. Part 3 : Preferred test conditions. Equipment for stationary use in weatherprotected locations - High degree of simulation, 1986.

IEC0605-3-3

International Electrotechnical Commission, IEC 605-3-3, Equipment reliability testing; part 3: preferred test conditions; section 3: test cycle 3: Equipment for stationary use on partially weatherprotected locations - Low degree of simulation, 1992.

IEC0605-3-4

International Electrotechnical Commission, IEC 605-3-4, Equipment reliability testing; part 3: preferred test conditions; section 4: test cycle 4: Equipment for portable and non-stationary use - Low degree of simulation, 1992.

IEC0605-4

International Electrotechnical Commission, IEC 605-4, Equipment reliability testing. Part 4 : Procedures for determining point estimates and confidence limits from equipment reliability determination tests, 1986, 1st amendment 1989.

IEC0605-6

International Electrotechnical Commission, IEC 605-6, Equipment reliability testing. Part 6 : Tests for the validity of a constant failure rate assumption, 1986, 1st amendment 1989.

IEC0605-7

International Electrotechnical Commission, IEC 605-7, Equipment reliability testing. Part 7 : Compliance test plans for failure rate assuming constant failure rate, 1978, 1st amendment 1990.

IEC0643

International Electrotechnical Commission, IEC 643, Application of Digital Computers to Nuclear Reactor Instrumentation and Control, 1979.

IEC0671

International Electrotechnical Commission, IEC 671, Periodic Tests and Monitoring of the Protection System of Nuclear Reactors, 1980.

IEC0706-1

International Electrotechnical Commission, IEC 706, Part 1, Guide on maintainability of equipment; Sections One, Two and Three. Introduction, requirements and maintainability programs, 1982.

IEC0706-2

International Electrotechnical Commission, IEC 706, Part 2, Guide on maintainability of equipment; section five; maintainability studies during the design phase, 1990.

IEC0706-3

International Electrotechnical Commission, IEC 706, Part 3, Guide on maintainability of equipment; Sections Six and Seven - Verification and collection, analysis and presentation of data, 1987.

IEC0706-4

International Electrotechnical Commission, IEC 706, Part 4, Guide on maintainability of equipment; section 8: maintenance and maintenance support planning, September 1992.

IEC0706-5

International Electrotechnical Commission, IEC 706, Part 5, Guide on maintainability of equipment; Section 4: Diagnostic testing, November 1994.

IEC0706-6

International Electrotechnical Commission, IEC 706, Part 6, Guide on maintainability of equipment; section 9: Statistical methods in maintainability evaluation, December 1994.

IEC0709

International Electrotechnical Commission, IEC 709, Separation within the Reactor Protection System, 1981.

IEC0721

International Electrotechnical Commission, IEC 721, Classification of Environmental Conditions.

IEC0801

International Electrotechnical Commission, IEC 801, Electromagnetic Compatibility for Industrial Process Measurement and Control Equipment.

IEC0801-1

International Electrotechnical Commission, IEC 801, Part 1, Electromagnetic compatibility for industrial-process measurement and control equipment. Part 1 : General introduction., 1984.

IEC0801-2

International Electrotechnical Commission, IEC 801, Part 2, Electromagnetic compatibility for industrial-process measurement and control equipment; part 2: electrostatic discharge requirements, April 1991.

IEC0801-4

International Electrotechnical Commission, IEC 801, Part 4, Electromagnetic compatibility for industrial-process measurement and control equipment. Part 4: Electrical fast transient/burst requirements, 1988.

IEC0812

International Electrotechnical Commission, IEC 812, Analysis Techniques for System Reliability - Procedure for Failure Mode and Effect Analysis (FMEA), 1985.

IEC0863

International Electrotechnical Commission, IEC 863, Presentation of reliability, maintainability and availability predictions, 1986.

IEC0880

International Electrotechnical Commission, IEC 880, Software for Computers in the Safety Systems of Nuclear Power Stations, 1986.

IEC0880/Supplement 1

International Electrotechnical Commission, IEC 880/Supplement 1, Software for Computers Important to Safety for Nuclear Power Plants (draft), 1994.

IEC0902

International Electrotechnical Commission, IEC 902, Industrial Process Measurement and Control - Terms and Definitions, 1987.

IEC0960

International Electrotechnical Commission, IEC 960, Functional Design Criteria for a Safety Parameter Display System for Nuclear Power Stations, 1988.

IEC0987

International Electrotechnical Commission, IEC 987, Programmed Digital Computers Important to Safety for Nuclear Power Stations, 1989.

IEC1014

International Electrotechnical Commission, IEC 1014, Programmes for reliability growth, 1989.

IEC1025

International Electrotechnical Commission, IEC 1025, Fault tree analysis (FTA), October 1990.

IEC1069-1

International Electrotechnical Commission, IEC 1069-1, Industrial-process measurement and control - Evaluation of system properties for the purpose of system assessment; Part 1: General considerations and methodology, 1991.

IEC1069-2

International Electrotechnical Commission, IEC 1069-2, Industrial-process measurement and control - Evaluation of system properties for the purpose of system assessment; Part 2: Assessment methodology, 1993.

IEC1069-5

International Electrotechnical Commission, IEC 1069-5, Industrial-process measurement and control - Evaluation of system properties for the purpose of system assessment; Part 5: Assessment of system dependability, December 1994.

IEC1070

International Electrotechnical Commission, IEC 1070, Compliance test procedures for steady-state availability, 1991.

IEC1078

International Electrotechnical Commission, IEC 1078, Analysis techniques for dependability; reliability block diagram method, November 1991.

I

IEC1126

International Electrotechnical Commission, IEC 1126, Reliability testing; compliance test plans for success ratio, December 1991.

IEC1131-1

International Electrotechnical Commission, IEC 1131-1, Programmable Controllers; Part 1, General Information, 1992.

IEC1131-2

International Electrotechnical Commission, IEC 1131-2, Programmable Controllers; Part 2: Equipment requirements and test, 1992.

IEC1131-3

International Electrotechnical Commission, IEC 1131-3, Programmable Controllers; Part 3: Programming Languages, 1993.

IEC 1134-4

International Electrotechnical Commission, IEC 1131-2, Programmable controllers; Part 4: User guidelines.

IEC1140

International Electrotechnical Commission, IEC 1140, Protection Against Shock: Common Aspects for Installation and Equipment.

IEC1160

International Electrotechnical Commission, IEC 1160, Formal Design Review, August 1992.

IEC12119

International Electrotechnical Commission, ISO/IEC 12119, Information Technology - Software Packages - Quality Requirements and Testing.

IEC1226

International Electrotechnical Commission, IEC 1226, The Classification of Instrumentation and Control Systems Important to Safety for Nuclear Power Plants, 1993.

IEC1508

International Electrotechnical Commission, IEC 1508, Functional Safety: Safety-Related Systems, Draft, 1995.

IEC1609

International Electrotechnical Commission, IEC 1609, Industrial-Process Measurement and Control - Evaluation of System Properties for the Purpose of System Assessment, Draft.

IEE1988

Institute of Electrical Engineers, IEE1988, Guidelines for Assuring Testability, ISBN 0863411290, 1988.

IEE5

Institute of Electrical Engineers, IEE 5, Software in Safety-Related Systems, 1989.

IEEE C37.1

Institute of Electrical and Electronics Engineers, C37.1, Definition, specification and analysis of systems used for supervisory control, data acquisition, and automatic control, 1987

IEEE/SE

Institute of Electrical and Electronics Engineers, IEEE Standards Board, IEEE Standards Collection; Software Engineering Standards, 1994, ISBN 155937442X.

IEEE0308

Institute of Electrical and Electronics Engineers, IEEE 308, IEEE Standard Criteria for Class 1E Power Systems for Nuclear Power Generating Stations, 1980.

IEEE0338

Institute of Electrical and Electronics Engineers, IEEE 338, IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems, 1987.

IEEE0352

Institute of Electrical and Electronics Engineers, ANSI/IEEE-Std-352, IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protecting Systems, 1975.

IEEE0379

Institute of Electrical and Electronics Engineers, IEEE 379, IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems, 1988.

IEEE0384

Institute of Electrical and Electronics Engineers, IEEE 384, IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits, 1981.

IEEE0493

Institute of Electrical and Electronics Engineers, ANSI/IEEE-Std-493, Recommended practice for the design of reliable industrial and commercial power stations, 1990.

IEEE0494

Institute of Electrical and Electronics Engineers, IEEE-Std-494, IEEE Method for Identification of Documents Related to Class 1E Equipment and Systems for Nuclear Power Generating Stations, 1973

IEEE0497

Institute of Electrical and Electronics Engineers, IEEE-Std-497, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, 1981

IEEE0500

Institute of Electrical and Electronics Engineers, IEEE-Std-500, Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations, 2nd Edition, 1984.

IEEE0500-P&V

Institute of Electrical and Electronics Engineers, IEEE 500 P&V, Standard Reliability Data for Pumps and Drivers, Valve Actuators, and Valves.

IEEE0577

Institute of Electrical and Electronics Engineers, ANSI/IEEE 577, Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations, 1992.

IEEE0603

Institute of Electrical and Electronics Engineers, IEEE-Std-603, Standard Safety Criteria for Safety Systems for Nuclear Power Generating Stations, 1991.

IEEE0610

Institute of Electrical and Electronics Engineers, IEEE-Std-610.12, Glossary of Software Engineering Terminology, Corrected Edition 1991, February 1991, ISBN 155937067X.

IEEE0627

Institute of Electrical and Electronics Engineers, IEEE-Std-627, IEEE Standard for Design Qualification of Safety Systems Equipment Used in Nuclear Power Generating Stations, 1980.

IEEE0729

Institute of Electrical and Electronics Engineers, IEEE-Std-729, IEEE Standard Glossary of Software Engineering Terminology, 1983.

IEEE0730

Institute of Electrical and Electronics Engineers, IEEE-Std-730, IEEE Standard for Software Quality Assurance Plans, 1989.

IEEE0762

Institute of Electrical and Electronics Engineers., ANSI/IEEE 762, Standard Definitions for Use in Reporting Electric Generating Unit Reliability, Availability, and Productivity.

IEEE0828

Institute of Electrical and Electronics Engineers, IEEE-Std-828, IEEE Standard for Software Configuration Management Plans, 1990.

IEEE0829

Institute of Electrical and Electronics Engineers, IEEE-Std-829, IEEE Standard for Software Test Documentation, 1983.

IEEE0830

Institute of Electrical and Electronics Engineers, IEEE-Std-830-1984, IEEE Guide to Software Requirements Specification, 1984.

IEEE0982

Institute of Electrical and Electronics Engineers, IEEE-Std-982.1, IEEE Standard Dictionary of Measures to Produce Reliable Software, 1988.

IEEE0982.1

Institute of Electrical and Electronics Engineers, IEEE-Std-982.1, IEEE Standard Dictionary of Measures to Produce Reliable Software, 1988.

IEEE0982.2

Institute of Electrical and Electronics Engineers, IEEE-Std-982.2, IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software, 1988.

IEEE0990

Institute of Electrical and Electronics Engineers, IEEE-Std-990, IEEE Recommended Practice for ADA as a Program Design Language, 1987.

IEEE1002

Institute of Electrical and Electronics Engineers, IEEE-Std-1002, IEEE Standard Taxonomy for Software Engineering Standards, 1987.

IEEE1008

Institute of Electrical and Electronics Engineers, IEEE-Std-1008, IEEE Standard for Software Unit Testing, 1987.

IEEE1012

Institute of Electrical and Electronics Engineers, IEEE-Std-1012, IEEE Standard for Software Verification and Validation, 1987.

IEEE1028

Institute of Electrical and Electronics Engineers, IEEE-Std-1028, Software Reviews and Audits, 1988.

IEEE1042

Institute of Electrical and Electronics Engineers, IEEE-Std-1042, Software Configuration Management, 1987.

IEEE1044

Institute of Electrical and Electronics Engineers, IEEE-Std-1044, IEEE Standard Classification for Software Anomalies, 1993.

IEEE1044.1

Institute of Electrical and Electronics Engineers, IEEE 1044.1, IEEE Guide to Classification of Software Anomalies, 1995.

IEEE1046

Institute of Electrical and Electronics Engineers, IEEE 1046, IEEE Application Guide for Distributed Digital Control and Monitoring for Power Plants, 1991

IEEE1059

Institute of Electrical and Electronics Engineers, IEEE-Std-1059, IEEE Guide for software Verification and Validation Plans, 1993.

IEEE1061

Institute of Electrical and Electronics Engineers, IEEE-Std-1061, IEEE Standard for a Software Quality Metrics Methodology, 1992.

IEEE1062

Institute of Electrical and Electronics Engineers, IEEE-Std-1062, IEEE Recommended Practice for Software Acquisition, 1992.

IEEE1074

Institute of Electrical and Electronics Engineers, IEEE-Std-1074, IEEE Standard for Developing Software Life Cycle Processes, 1991.

IEEE1074.1

Institute of Electrical and Electronics Engineers, IEEE 1074.1, Guide for Developing Software Life Cycle Processes, 1995.

IEEE1219

Institute of Electrical and Electronics Engineers, IEEE-Std-1219, IEEE Standard for Software Maintenance, 1992.

IEEE1228

Institute of Electrical and Electronics Engineers, IEEE-Std-1228, IEEE Standard for Software Safety Plans, 1994.

IEEE1298

Institute of Electrical and Electronics Engineers, IEEE-Std-1298, Software Quality Management Systems, Part 1: Requirements, 1992.

IEEE7-4.3.2.

Institute of Electrical and Electronics Engineers, IEEE-Std-7-4.3.2., Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 1993.

IPC D-330

IPC D-330 2.3.4.1, Reliability (Design Guide).

IS402

IS402, Technical Specification for the Supply of Electronic Equipment for the Safety of Signalling Systems.

ISA SP84

Instrument Society of America, ISA SP 84, Programmable Electronic Systems for Use in Safety Applications, Draft, 1994.

ISA-dS84/16N

Instrument Society of America, Application of Safety Instrumented Systems for the Process Industries, draft 16N, January 1995.

ISO DP9126

International Organization for Standardization, ISO/IEC JTC1/SC7/WG3, DP9126, Software Product Evaluation - Quality Characteristics and Guidelines for their Use, 1990.

ISO FSQA

International Organization for Standardization,ISO/IEC JTC1/SC7/WG3/SG2, Foundations of Software Quality Assessment, R.E. Nance and J.D. Arthur, Systems Research Center and The Department of Computer Science, Virginia Tech, 1990.

ISO N136

International Organization for Standardization,ISO/IEC JTC1/SC7/WG3, N-136, Evaluation of Methods and Tools, 1989.

ISO SQA

International Organization for Standardization, ISO/IEC JTC1/SC7/WG3/SG2, R.E. Nance and J.D. Arthur, Systems Research Center and The Department of Computer Science, Foundations of Software Quality Assurance, 1990.

ISO11161

International Organization for Standardization, ISO 11161, Industrial automation systems - Safety of integrated manufacturing systems - Basic requirements.

ISO2382/1

International Organization for Standardization, ISO, ISO2382/1, Information Technology - Vocabulary - Part 1: Fundamental Terms, 1993.

ISO2382/11

International Organization for Standardization, Information Processing Systems - Vocabulary - Part 11: Processing Units, 1987.

ISO2382/14

International Organization for Standardization, ISO 2382/14, Data processing; Vocabulary; Section 14 : Reliability, maintenance and availability.

ISO2382/15

International Organization for Standardization, Data Processing - Vocabulary - Part 15: Programming Languages, 1985.

ISO2382/2

International Organization for Standardization, ISO 2382/2, Data Processing - Vocabulary - Section 02: Arithmetic and Logic Operations, 1976.

ISO2382/7

International Organization for Standardization,, ISO 2382/7, Information Technology - Vocabulary - Part 07: Computer Programming, 2nd edition, 1984.

ISO2382/8

International Organization for Standardization,, ISO 2382/8, Information Processing Systems - Vocabulary - Part 08: Control, Integrity and Security, 1st edition, 1986.

ISO6527

International Organization for Standardization, ISO 6527, Nuclear power plants; Reliability data exchange; General guidelines, October 1982.

ISO7385

International Organization for Standardization, ISO 7385, Nuclear power plants; Guidelines to ensure quality of collected data on reliability, August 1983.

ISO8107

ISO 8107, Nuclear Power Plants - Maintainability - Terminology.

ISO8402

International Organization for Standardization, ISO 8402, Quality Management and Quality Assurance - Vocabulary, April 1994.

ISO8807

International Organization for Standardization, ISO 8807, Information Processing Systems - Open Systems Interconnection - LOTOS - A Formal Description Technique Based on the Temporal Ordering of Observational Behaviour, 1989.

ISO8930

International Organization for Standardization, ISO 8930, General principles on reliability for structures; list of equivalent terms, March 1991.

ISO12178; 1994 Industrial automation. time-critical communications architectures. User requirements.

ISO9000-3

International Organization for Standardization, ISO 9000-3, Quality Management and Quality Assurance Standards, Part 3 - Guidelines for the Application of ISO9001 to the Development, Supply and Maintenance of Software, 1990.

ISO9000-4

International Organization for Standardization, ISO 9000-4, Quality management and quality assurance standards; part 4: guide to dependability programme management, April 1993.

ISO9001

International Organization for Standardization, ISO 9001, Quality Systems - Model for Quality Assurance in Design/Development, Production, Installation and Servicing, 1987.

ISO9074

International Organization for Standardization, ISO 9074, Information Processing Systems - Open Systems Interconnection - Estelle - A Formal Description Technique Based on an Extended State Transition Model, 1987.

ISO TR12178

Industrial automation - time-critical communications architectures. User requirements, 1994.

ITG6.2/04

ITG Recommendations: Reliability Definitions with Regard to Complex Software and Hardware.

ITSEC

ITSEC, Information Technology Security Evaluation Criteria, Provisional Harmonised Criteria, June 1991.

ITSEM

ITSEM, Information Technology Security Evaluation Manual, Provisional Harmonised Methodology, September 1993.

JEAC4101

JEAC 4101, Guide for Quality Assurance of Nuclear Power Plants.

JEAC4604

JEAC 4604, Guidelines for Design of Safety Protection Systems for Nuclear Power Plants.

JEAC4609

JEAC 4609 Application Guidelines for Programmatic Digital Computer Systems in Safety-Protection Systems of Nuclear Power Plants, 1989.

JIS C5700

JIS C 5700, General Rules for Reliability Assured Electronic Components.

JIS X0014

JIS X 0014, Glossary of Terms Used in Information Processing (Reliability, Maintenance and Availability).

JIS8115

Japanese Standards Association, JIS Z 8115, Presentation of Reliability, Maintainability and Availability Presentation for S ..., 1 August 1981.

JSP188

Requirements for the Documentation of Software in Military Operational Real Time Computer Systems.

JTC1/SC7/WG9-P7.30

International Organization for Standardization, ISO/IEC JTC1/SC7/WG9, Project 7.30, International Standard, Information Technology - Classification and Assignment; Software Integrity Levels, Working Draft 1.0 , 16 June 1994.

JTC1/SC22/WG19-IN9

VDM specification language prostandard, draft, 1991

KTA3501

KTA, KTA3501, Reaktorschutzsystem und Ueberwachungseinrichtungen des Sicherheitssystems, Juni 1985.

KTA3502

KTA, KTA3502, Stoerfallinstrumentierung, Juni 1994.

KTA3503

KTA, KTA3503, Typpruefung von elektrischen Baugruppen des Reaktorschutzsystems, November 1986.

KTA3504

KTA, KTA3504, Elektrische Antriebe des Sicherheitssystems in Kernkraftwerken, September 1988.

KTA3505

KTA, KTA3505, Typpruefung von Messwertgebern und Messumform-Reaktorschutzsystems, November 1984.

KTA3506

KTA, KTA3506, Typpruefung der leittechnischen Einrichtungen des Sicherheitssystems in Kernkraftwerken, November 1984.

KTA3507

KTA, KTA3507, Werkspruefungen, Pruefungen nach Instandsetzung und Nachweis der Betriebsbewaehrung fuer leittechnische Einrichtungen des Sicherheitssystems, November 1986.

KTA3705

KTA, KTA3705, Schaltanlagen, Transformatoren und Verteilungsnetze zur elektrischen Energieversorgung des Sicherheitssystems in Kernkraftwerken, September 1988.

KTA3706

KTA, KTA3706, Wiederkehrender Nachweis der Kuehlmittel-Verlust-Stoerfallfestigkeit von elektro- und leittechnischen Komponenten des Sicherheitssystems, Juni 1994.

LOGAN93

LOGAN, Fault Tree and Logic Network Analysis Program, R M Consultants Ltd., 1993.

M&W82

Martz, H.F. & R.A. Waller, Bayesian Reliability Analysis, Wiley, 1982, ISBN 0471864250.

MIL DOD1701

DOD-Std-1701, Hardware Diagnostic Test System Requirements.

MOD NES1017

UK MoD Directorate of Standardization, NES 1017, Requirements for Maintainability Demonstrations of Naval Systems, Issue 3, January 1993.

MOD00-40

UK MoD Directorate of Standardization, Defence Standard 00-40, Reliability and Maintainability.

MOD00-41

UK MoD Directorate of Standardization, Defence Standard 00-41, Reliability and Maintainability MoD. Guide to Practices and Procedures, Issue 3 (Supersedes All Previously Issued Separate Parts), June 1993.

MOD00-43/1

UK MoD Directorate of Standardization, Defence Standard 00-43, Reliability and Maintainability Assurance Activity; Part 1: In-Service Reliability Demonstrations, Issue 1, January 1993.

MOD00-44/1

UK MoD Directorate of Standardization, Defence Standard 00-44, Reliability and Maintainability Data Collection and Classification; Part 1: Maintenance Data & Defect Reporting in the Royal Navy, the Army and the Royal Air Force, Issue 1, March 1993. (Supersedes Def Stan 05-59).

MOD00-44/2

UK MoD Directorate of Standardization, Defence Standard 00-44, Reliability and Maintainability Data Collection and Classification; Part 2: Data Classification and Incident Sentencing, Issue 1, April 1994. (Supersedes Def Stan 05-59).

MOD00-5

UK MoD Directorate of Standardization, Defence Standard 00-5, Design Criteria for Reliability, Maintainability and Maintenance of Land Service Materiel.

MOD00-55

UK MoD Directorate of Standardization, Interim Defence Standard 00-55, The procurement of Safety Critical Software in Defence Equipment, 1991.

MOD00-56

Ministry of Defence, Interim Defence Standard 00-56, Hazard Analysis and Safety Classification of the Computer and Programmable Electronic System Elements of Defence Equipment, Issue 1, 1991.

MOD05-48

UK MoD Directorate of Standardization, Defence Standard 05-48, Reliability of a Series System, March 1978.

MOD05-63

UK MoD Directorate of Standardization, Defence Standard 05-63, Guidelines for Classifying Incidents for Reliability Estimation of Tracked and Wheeled Vehicles, Issue 1, October 1984.

MU8004

Deutsche Bundesbahn, MU8004 (Munich 8004).

MUSA87

Musa, J., A. Iannino and K. Okumoto, Software Reliability; Measurement, Prediction, Application, New York: McGraw-Hill, 1987.

NASA NSS740.13

National Aeronautics and Space Administration, NSS 1740.13, Software Safety Standard, June 1994.

NATO AC/35-D/1027

NATO, AC/35-D/1027, NATO Trusted Computer System Evaluation Criteria.

NATO ARMP-1

North Atlantic Treaty Organization, ARMP-1, NATO Requirements for Reliability and Maintainability.

NATO ARMP-2

North Atlantic Treaty Organization, General Application Guidance on the Use of ARMP-1.

NATO ARMP-3

North Atlantic Treaty Organization, ARMP-3, Application of National R and M Documents.

NATO ARMP-4

North Atlantic Treaty Organization, ARMP-4, Guidance for Writing NATO R & M Requirements Documents.

NATO ARMP-5

North Atlantic Treaty Organization, ARMP-5, Guidance on Reliability and Maintainability Training.

NATO ARMP-6

North Atlantic Treaty Organization, ARMP-6, In-Service R & M.

NATO ARMP-8

North Atlantic Treaty Organization, ARMP-8, Reliability & Maintainability in the Procurement of Off-The- Shelf Equipment.

NATO STANAG 4174

North Atlantic Treaty Organization, STANAG 4174, Allied Reliability and Maintainability Publications.

NATO STANAG 4404

North Atlantic Treaty Organization, NATO STANAG 4404, Safety Design Requirements and Guidelines for Munition Related Safety Critical Computing Systems - Draft, March 1989.

NAVORD-OD-44942

NAVORD-OD-44942, System Safety Engineering Guidelines.

NEN10050(191)

Nederlands Normalisatie Instituut, NEN10050(191), Dependability and quality of service, June 1991.

NEN10319

Nederlands Normalisatie Instituut, NEN 10319, Presentation of reliability data on electronic components (or parts), July 1980.

NEN10671

Nederlands Normalisatie Instituut, NEN 10671, Nuclear reactors; Periodic tests and monitoring of the protection system, November 1981.

NEN11069-1

Nederlands Normalisatie Instituut, Industrial-process measurement and control; Evaluation of system properties for the purpose of system assessment; Part 1: General considerations and methodology.

NEN11069-5

Nederlands Normalisatie Instituut, NEN11069-5, Industrial-process measurement and control; Evaluation of system properties for the purpose of system assessment; Part 5: Assessment of system dependability (IEC 1069-5: 1994), May 1995.

NEN264

Nederlands Normalisatie Instituut, NEN EN 264, Safety shut-off devices for combustion plants using liquid fuels; Safety requirements and testing, April 1992.

NEN3134

Nederlands Normalisatie Instituut, NEN 3134, Veiligheidsbepalingen voor laagspanningsinstallaties in medisch gebruikte ruimten, 1994.

NEN540

Nederlands Normalisatie Instituut, NEN-EN-540, Klinisch Onderzoek van Medische Hulpmiddelen, 1991.

NF71011

NF71011, Railway fixed equipment and rolling stock; Data processing; Software dependability - General, 1990.

NF71012

NF71012, Railway fixed equipment and rolling stock; Data processing; Software dependability - Constraints on software, 1990.

NF71013

NF71013, Railway fixed equipment and rolling stock; Data processing; Software dependability - Adapted methods for software safety analysis.

NPR3137

NPR, NPR 3137, Safe Application of Medical Electrical Equipment, 1984.

NSA-FC

NIST, NSA, Federal Criteria for Information Technology Security, Draft Version 1.0.

NSAC105

Nuclear Safety Analysis Center, NSAC-105, Guidelines for Design and Procedure Changes in Nuclear Power Plants.

NSAC125

Nuclear Safety Analysis Center, NSAC-125, Guidelines for 10CFR50.59 Safety Evaluations.

NSAC38

Nuclear Safety Analysis Center, NSAC 38, Verification and Validation for Safety Parameter Display Systems, 1981.

NUREG0492

NUREG, 0492, Fault Tree Handbook.

NUREG1.152

NUREG, Regulatory Guide 1.152, Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants.

NUREG1.75

NUREG, Regulatory Guide 1.75, Physical Independence of Electrical Systems.

NUREG4640

NUREG/CR-4640, PNL-5787, Handbook of Software Quality Assurance Techniques Application to the Nuclear Industry.

O'Connor81

O'Connor, P.D.T., Practical Reliability Engineering, John Wiley & Sons, Chichester, 1981, ISBN 0471905518.

OH CE-1001

Ontario Hydro & Atomic Energy of Canada Limited, OH CE-1001, Standard for Software Engineering of Safety Critical Software, 1995.

OeNORM M 8100

(teilw. uebereinstimmend mit (partially identical with) DIN 31051 (1982))

Instandhaltung von Anlagen, Maschinen und Geraeten: Benennungen, Definitionen und Massnahmen (Maintenance of plants (facilities), machinery and devices: naming conventions, definitions and measures), 1985.

NOTE: This standard is now input to CEN 319 standards on Maintenance.

OeNORM M 8103

Zuverlaessigkeit und Verfuegbarkeit von Anlagen, Maschinen und Geraeten (Reliability and NOTE: This standard is now input to CEN 319 standards on Maintenance.

OeVE-T3

Elektrische Eisenbahnsicherungsanlagen und -geraete (Electrotechnical Railway Interlocking Systems and Devices), 1979

OeVE-T3a

Nachtrag a zu den Bestimmungen ueber Elektrische Eisenbahnsicherungsanlagen und -geraete (Addendum a to the Standards for Electrotechnical Railway Interlocking Systems and Devices), 1983

OH690002

Ontario Hydro & Atomic Energy of Canada Limited, 907-C-H-690002-0200, Software Engineering of Category III Software.

OH69002

Ontario Hydro & Atomic Energy of Canada Limited, 907-C-H-690002-0100, Software Engineering of Category II Software.

ORE A118

ORE, The Use of Electronic Components for Signalling, Reports 1-13, 1971-1977.

ORE A155.1

ORE, Transmission of Safety Informations, Reports 1, 2, 4, 5, 8, 10, 13, 1982-1988.

ORE A155.2

ORE, Software for Safety Systems, Report 3, 6, 7, 9, 11, 1985-1987.

ORE A155.3

ORE, The use of Electronic Components for Signalling, Report 12, 1988.

OREDA92

OREDA, Offshore Reliability Data Handbook, Published by OREDA participants, Pennwell Publishing Company, 1992, ISBN 82 515 0188 1.

PEO

PEO, Guideline for the Use of Computer Software Tools by Professional Engineering and the Development of Computer Software Affecting Public Safety or Welfare, 1993.

PN80/Z-08051

Polish Committee of Measures and Quality, PN80/Z-08051, Equipment of automatic flight control systems.

PN80/Z-8202

Polish Committee of Measures and Quality, PN80/Z-8202, Labor protection. Control elements of machines and devices used in production.

PN89/J-01101

Polish Committee of Measures and Quality, PN89/J-01101, Control and safety systems of nuclear reactors.

PN93/G-50000

Polish Committee of Measures and Quality, PN93/G-50000, Labor protection. Machines and devices applied in mining. General requirements for safety and ergonomics.

PN93/T-42107

Polish Committee of Measures and Quality, PN93/T-42107, Safety of information technology equipment and electric business equipment.

PN93/T-42107/A2

Polish Committee of Measures and Quality, prPN93/T-42107/A2, Safety of information technology equipment and electric business equipment.

RAC CRTA-FMECA

RAC, CRTA-FMECA, Failure Mode, Effects, and Criticality Analysis (FMECA).

RAC EEMD-1

RAC, EEMD-1, Electronic Equipment Maintainability Data.

RAC EERD-2

RAC, EERD-2, Electronic Equipment Reliability Data.

RAC MDR-21

RAC, MDR-21, Microcircuit Device Reliability Trend Analysis.

RAC MFAT-2

RAC, MFAT-2, Characterization and Failure Analysis Techniques a Procedural Guide.

RAC NONOP-1

RAC, NONOP-1, Nonoperating Reliability Databook.

RAC NPRD

RAC, NPRD, Nonelectronic Parts Reliability Data.

RAC PRIM

RAC, PRIM, Primer for DOD Reliability, Maintainability, Safety, and Logistics Standards.

RAC RDSC-1

RAC, RDSC-1, Reliability Sourcebook.

RAC RMST-93

RAC, RMST-93, Reliability & Maintainability Software Tools.

RAC TOOLKIT

RAC, TOOLKIT, Reliability Engineer's Toolkit.

RCC-E

Design and construction rules for Electronic Components of PWR (pressurized water reactor) nuclear islands (it is the specific French recommendations guide accepted as the reference by the French authorities to deliver the equipment qualification).

RIA23

Railway Industry Association (UK), Safety Related Software for Railways (Signalling).

RIA24

Railway Industry Association (UK), Safety Related Software for Railways (Signalling).

RTCA DO178a

Radio Technical Commission for Aeronautics, RTCA DO178a, Software Considerations in Airborne Systems and Equipment Certification, March 1985.

RTCA DO178b

Requirements and Technical Concepts for Aviation, RTCA DO178-B, Software Considerations in Airborne Systems and Equipment Certification, 1992.

SAE AE-9

SAE, AE-9, Automotive Electronics Reliability Handbook, February 1987.

SAE AIR4276

SAE, ANSI/SAE AIR 4276, Survey Results: Computerization of Reliability, Maintainability & Supportability (RM&S) in Design.

SAE ARD50010

SAE, ARD 50010, Recommended RMS Terms and Parameters.

SAE ARD50046

SAE, ARD 50046, RMS Information Sourcebook.

SAE J1213/2

SAE, J 1213/2, Glossary of Reliability Terminology Associated with Automotive Electronics, Information Report, October 1988.

SEMI E10

SEMI, E10, Guideline for Definition and Measurement of Equipment Reliability, Availability, and Maintainability (RAM).

Smith81

Smith, D.J., Reliability and Maintainability in Perspective, Technical, Management and Commercial Aspects, The Macmillan Press Ltd., 1981, ISBN 0333310489/0333310497.

Smith89

Smith, D.J. & K.B. Wood, Engineering Quality Software, Elsevier Applied Science, 1989.

TCSEC

TCSEC, US DoD 5200.28-STD, Trusted Computer Systems Evaluation Criteria.

TS1914

Turkish Standards Institution, TS 1914, General Principles for the Verification of the Safety of Structures, 29 April 1975.

TS5580

Turkish Standards Institution, TS 5580, Nuclear Power Plants - Reliability Data Exchange General Guidelines, 14 March 1988.

TS5581

Turkish Standards Institution, TS 5581, Nuclear Power Plants - Guidelines To Ensure Quality of Collected Data On Reliability, 14 March 1988.

TS6650

Turkish Standards Institution, TS 6650, Reliability and Maintainability Management (Electrotechnical Products), 28 February 1989.

TS8024

Turkish Standards Institution, TS 8024, General Principles on Reliability for Structures-
List of Equipment- Terms, 27 February 1990.

TS8372

Turkish Standards Institution, TS 8372, Equipment Reliability Testing- Preferred Test
Conditions, Indoor Portable Equipment- Low degree of simulation, 12 April 1990.

TS8431

Turkish Standards Institution, TS 8431, Presentation of Reliability, Maintainability and
Availability Presentation for S ..., 14 April 1990.

TÜV86

Hölscher, H., R. Rader, Microcomputers in Safety Technique; an Aid to Orientation for
Developer and Manufacturer, Verlag TÜV Bayern, 1986.

UIC738R

UIC, The Processing and Transmission of Safety Related Informations, 1990.

UL1998

Underwriters' Laboratories, Draft UL 1998, Standard for Safety-Related Software, 1992.

VDE0801

DIN-V-VDE 0801, Principles for Computers in Safety-Related Systems, January 1990,
proof copy of english translation October 1991.

VDE0801/A1

Verein Deutscher Elektrotechniker, DIN V VDE 0801/A1, Principles for computers in
safety-related systems; Amendment A1, October 1994.

VDE0831

Verein Deutscher Elektrotechniker, DIN 57831, Electrical Equipment for Railway
Signalling.

VDE3542

VDI/VDE 3542 Blatt 1, Sicherheitstechnische Begriffe für
Automatisierungssysteme; Qualitative Begriffsbestimmungen.

VDE3542/4

VDI/VDE, VDI/VDE3542, Blatt 4, Sicherheitstechnische Begriffe fuer
Automatisierungssysteme, Zuverlaessigkeit und Sicherheit komplexer Systeme, 1995.

prEN0115

Nederlands Normalisatie Instituut, Safety rules for the construction and installation of
escalators.

prEN0954

Nederlands Normalisatie Instituut, prEN954, Safety of machinery; safety related parts of
control systems.

prEN1050

Nederlands Normalisatie Instituut, prEN1050, Safety of machinery; risk assessment.

8.4 Summaries of a sub-set of the identified standards

ANS8.3

Issuing agency: Professional society, American Nuclear Society

Type: Standard

Level: Application system

Size: 11 pages

Scope: Alarm systems in nuclear power reactors. Software is not directly discussed, though the standard would apply to computer-based alarm systems.

Principal topics:

General principles for design criticality alarms

Alarm system design criteria

Reliability

Seismic tolerance

Response time

etc.

Testing criteria

Operations

Training

Procedures

Evacuation drills

etc.

AS2529

Provides guidance on the collection of reliability data on the field performance of electronic components, equipment and systems to provide data for the comparison of actual and predicted reliability, the improvement of achieved reliability, and the derivation of availability and maintainability information. The Standard can be applied to any other field of engineering for which such data are requested.

Technically identical with IEC 362.

AS3563

Establishes the requirements for a software developer's quality management system and identifies the elements which will ensure that the software will meet the requirements of a purchase order or contract.

The Standard is presented in such a manner as to make obvious the equivalence to AS 3901/ISO 9001 and adds areas of particular relevance to the software development process.

AS3563-2

Provides guidance for implementing a software quality management system and should be read in conjunction with AS 3563.1. Gives practical guidance to software developers

implementing these requirements in response to customer demand or as an improvement in quality. Includes an informative set of appendices with explanatory forms and charts.

AS3900-1

Defines five key quality terms, discusses the principal concepts relevant to quality and provides guidance on the selection of the appropriate quality system Standard and factors which should be taken into consideration. Additional guidance is given in AS 3904.1. This Standard is identical with and has been reproduced from ISO 9000:1987. Identical with NZS 9000.1:1990 and produced as a Joint Australian/New Zealand Standard.

AS3930

Provides guidance on the basic concepts of reliability and maintainability applicable to any organization supplying or purchasing products, including both goods and services. Acquaints senior management of the need for an effective reliability and maintainability function as part of corporate strategy and of the benefit to be obtained.

AS3960

Provides guidance on reliability and maintainability program management, and discusses the essential features of planning, organization, direction and control of resources to produce products which will be reliable and maintainable.

ASME NQA1

Issuing agency: Professional society, ASME

Type : Standard

Level: Application system: some software

Size: 211 pages

Scope: Quality assurance programs in nuclear power plants. Contains a wealth of ideas that relate to quality assurance, and thus to facility safety. Much of this can be usefully transferred to other process control applications where safety is involved.

Principal topics:

Basic requirements for nuclear facilities

QA organization and responsibility

QA program

Design control

Procurement document control

Document control

Control of purchased items and services

Item identification and control

Control of processes

Inspections

Test control

Control of measuring and test equipment

Handling, storage and shipping

Inspection, test and operating status

Control of nonconforming items
Corrective action
QA records
Audits
QA requirements for nuclear facilities
(sections on various topics, such as concrete and steel)
QA requirements for computer software

Comment: This standard has gone through many revisions since it was first issued in 1979. The latest version incorporates both NQA-1 and NQA-2, and covers most aspects of nuclear facility quality assurance. Of particular interest is Part II, subpart 2.7, 'Quality Assurance Requirements for Computer Software for Nuclear Facility Applications'.

BS5750-13

Gives guidance to both supplier and purchaser on the quality systems requirements for the development, supply and maintenance of software.

BS5750-14

Outlines the essential features of a dependability programme, planned and managed to produce products that will be reliable and maintainable.

BS5760-0

Aimed at directors of companies looking for overall advantages, engineers not trained in quality and reliability to show how reliability can help in their technical decision making, and at middle management not specialized in engineering to demonstrate how reliability should be dovetailed in with other disciplines to give them the best result.

BS5760-1

Identifies the essential features of a comprehensive reliability and maintainability programme for the planning, organization, direction and control of resources to produce systems, equipments and components which will be reliable and maintainable. This guide is concerned mainly with what has to be done, and why, when and how it has to be done, but it cannot be specific about who should do it and where, because organizations and projects vary widely. Recommendations are given for the drafting of specifications for reliability and maintainability achievement. The main considerations for the assessment of reliability are reviewed and details are given of the means by which reliability data are transmitted from the point of collection and recording to the point of storage and/or usage.

BS5760-10

Provides guidance for in the laboratory and in the field, including the forms of testing, the principles involved and the procedures to be followed. Includes a flow chart for the preparation and execution of reliability.

BS5760-10.3

Reliability of systems, equipment and components. Guide to reliability testing. Compliance test procedures for steady-state availability.

BS5760-10.5

Defines procedures for preparing and applying plans for success or failure ratio.

BS5760-14

Guidance on implementing design reviews and details the contributions of various specialists including reliability, maintainability, quality and product safety.

BS5760-2

Includes human reliability and software reliability assessment techniques.

BS5760-3

Shows, by way of examples, how some of the principles described in Parts 1 and 2 are applied in industry. Each is a practical example of the use of reliability techniques although the names of the organizations have been omitted. Where appropriate, reference is made to the clauses in Parts 1 and 2 of BS 5760 that the examples illustrate.

BS5760-4

Guidance on the form and content of clauses concerned with the achievement of the reliability of products in the various types of specifications that cover the definition, use and maintenance of manufactured and constructed products. Information is also given on specifications related to the management of reliability programmes.

BS5760-5

Practical guide to the application of reliability analysis techniques for the development of more reliable designs or processes. FMEA identifies possible failures within a system which affect system performance. FMECA considers the probabilities of failures occurring and the severity of the consequences to provide measures of their criticalities. To be read in conjunction with BS 4778.

BS5760-6

Procedures employed to expose and remove weaknesses in hardware and software items in order to achieve acceptable reliability in a product. Explains basic concepts and describes the management, testing, failure analysis and corrective techniques involved. Mathematical modelling to estimate achieved reliability is outlined briefly.

BS5760-7

Describes the technique of the analysis and its application to identify the factors affecting the reliability and performance characteristics of a system. Explains the basic principles, procedures and assumptions necessary to carry out the analysis and provides identification rules and symbols.

BS5760-9

Describes how it is applied to model and evaluate reliability of elementary and more complex systems. Explains essential preliminary facts to be established and gives step-by-step procedure for development. Extends method to the calculation of system availability.

BS6913-7

Generally recognized terms and definitions relating to the availability of earth-moving machinery to assist in the communication and understanding of such terms.

BS7501

Criteria for the technical and management competence of testing laboratories.

BSI HB10007

Deals with all aspects of reliability, maintainability and safety related failures.

CSA396.1.2

Issuing agency: Standards agency, Canada

Type: Standard

Level: Software

Size: 14 pages

Scope: Acquisition of predeveloped software used in critical applications.

Principal topics:

Responsibilities for SQA program

Developer

Customer

SQA management

Organization

QA manual

Procedures

SQA audits

QA plans

SQA program elements

Requirements and design reviews

CM

Software documentation

Release control

SQA records

DOD AFISC SSH 1-1

Issuing agency: Government, Military, United States

Type: Guide

Level: Software

Size: 39 pages

Scope: Support acquisition programs which involve safety-critical computer and embedded-computer systems. It is intended to guide military program managers in the areas of safety and software engineering. The document assumes Mil Std 882B (which has been superseded by Mil Std 882C, qv).

Principal topics:

Introduction

- The software hazard

- Management considerations

Design guidelines for software system safety

- System considerations

- Hardware considerations

- Software life cycle considerations

Software safety analysis

- Software hazard analyses

Software hazard analysis methods

- Software fault tree analysis

- Software sneak circuit analysis

- Nuclear safety cross-check analysis

- Petri net analysis

Software system safety design rules and guidelines

DOD MIL0105E

This document addresses the subjects of sampling plans; lot size; inspection levels; average quality levels (AQLs); classification of defects; multiple sampling; and normal, tightened, and reduced sampling. For equipments where the sequential method of testing, based on operating time, may not tables showing accept-reject levels and operating characteristic curves for sampling plans. The sampling plans described in this document are applicable to AQL's of .01 percent or higher and are therefore not suitable for applications where quality levels in the defective parts per million range can be realized.

DOD MIL0108

This handbook provides procedures and tables based on the exponential distribution for life and reliability testing. It includes definitions required for the use of the life test sampling plans and procedures; general description of life test sampling plans; life tests terminated upon occurrence of preassigned number of failures; life tests terminated at preassigned time; and sequential life test sampling plans.

DOD MIL0189

This document is designed for both managers and analysts covering everything from simple fundamentals to detailed technical analysis. Included are concepts and principles of reliability growth, advantages of managing reliability growth, and guidelines and procedures used to manage reliability growth. It allows the development of a plan that will aid in developing a final system that meets requirements and lowers the life-cycle cost of the fielded system. The document includes sections on benefits, concepts, engineering analysis, and growth models.

DOD MIL0217

The purpose of this handbook is to establish and maintain consistent and uniform methods for estimating the inherent reliability of electronic equipment and systems. It provides a common basis for reliability predictions. This handbook includes two basic methods for reliability prediction of electronic equipment. The first method is the part stress analysis prediction technique, employing complex models using detailed stress analysis information as well as environment, quality applications, maximum ratings, complexity, temperature, construction, and a number of other application-related factors. The second is a simple method called the parts count reliability prediction technique, using primarily the number of parts of each category with consideration of part quality, environments encountered, and maturity of the production process. The simple method is beneficial in early trade-off studies and situations where the detailed circuit design is unknown. The complex method requires detailed study and analysis which is available when the circuit design has been defined. Samples of each type of calculation are provided.

DOD MIL0338

This handbook provides procuring activities and contractors with an understanding of the concepts, principles, and methodologies covering all aspects of electronic systems reliability engineering and cost analysis as they relate to the design, acquisition, and deployment of equipment or systems. Currently a two-volume set, it discusses the entire subject, heavily emphasizing the reasons for the reliability discipline. It includes general information, referenced documents, definitions, reliability theory, component reliability design considerations, application guidelines, specification control during acquisition, logistic support, failure reporting and analysis, reliability and maintainability theory, reliability specification allocation and prediction, reliability engineering design guidelines, reliability data collection and analysis, demonstration and growth, software reliability, systems reliability engineering, production and deployment reliability and maintainability (R&M), and R&M management considerations.

DOD MIL0470B

This document includes application requirements, tailorable maintainability program tasks, and an appendix with an application matrix and guidance and rationale for task selection. The topics covered are program surveillance and control, design and analysis, modeling, allocations, predictions, failure mode and effects analysis, and maintainability design criteria. Each task item includes a purpose, task description, and details to be specified. Software maintainability is not covered by this document.

DOD MIL0471A

This document provides procedures and test methods for verification, demonstration, and evaluation of qualitative and quantitative maintainability requirements. It also provides for qualitative assessment of various integrated logistic support factors related to and impacting the achievement of maintainability parameters and item downtime, e.g. technical manuals, personnel, tools and test equipment, maintenance concepts and provisioning.

DOD MIL0472

This document is to familiarize project managers and design engineers with maintainability prediction procedures. It provides the analytic foundation and application details of five prediction methods. Each procedure details applicability, point of application, basic parameters of measure, information required correlation, and cautionary notes. The highlights of each maintainability prediction procedure are presented in a clear and intelligible manner and include useful supplementary information applicable to specific procedures. Maintainability Prediction Procedures I and III are applicable solely to electronic systems and equipments. Procedures II and IV can be used for all systems and equipments. In applying Procedure II to non-electronic equipments the appropriate task times must be estimated. Procedure V can be used to predict maintainability parameters of avionics, ground and shipboard electronics at the organizational, intermediate and depot levels of maintenance.

DOD MIL0690C

This standard provides procedures for failure rate qualification, sampling plans for establishing and maintaining failure rate levels at selected confidence levels, and lot conformance inspection procedures associated with failure rate testing for the purpose of direct reference in appropriate military electronic parts established reliability (ER) specifications. Figures and tables throughout this standard are based on exponential distribution.

DOD MIL0721C

This standard defines terms and definitions used most frequently in specifying Reliability and Maintainability (R & M). Provides a common definition for the Department of Defense and defense contractors.

DOD MIL0728

The handbook is provided as a guide and describes general principles, procedures and safety items, of eddy current, liquid penetrate, magnetic particle, radiographic and ultrasonic testing. This handbook is not a training manual. Nor can it replace other written directives, procedures or specifications. However, it can serve as a ready reference to the important principles and facts relating to the employment of nondestructive testing, inspection and evaluation.

DOD MIL0756B

This standard establishes uniform procedures and ground rules for the generating mission reliability and basic reliability models and predictions for electronic,electrical,

electromechanical, mechanical, and ordnance systems and equipments. Model complexity may range from a complete system to the simplest subdivision of a system. It details the methods for determining service use (life cycle), creation of the reliability block diagram, construction of the mathematical model for computing the item reliability. Some simple explanations on the applicability and suitability of the various prediction sources and methods are included.

DOD MIL0764

This handbook presents system safety considerations for use in designing army materiel. The areas covered include safety engineering concepts and objectives, system safety analysis, hazard analysis, software analysis, and general design application considerations.

Issuing agency: Government, Military, US

Type: Guide

Level: Application system

Size: 300 pages

Scope: System safety within the U.S. Army has a chapter on software safety.

Principal topics:

Introduction to system safety

Philosophy

Product liability

System safety program requirements

Safety engineering concepts and objectives

Life cycle approach

Design criteria

Safety analyses

Safety verification

Safety design reviews

Risk management

System safety analysis

Methods and types of hazard analysis

Preliminary hazard analysis

Subsystem hazard analysis

FMECA, Fault HA, FTA, sneak circuit analysis

System hazard analysis

Software analysis techniques

PHA and Fault Hazard Analysis

Logic diagrams

Software FTA

Nuclear safety cross-check analysis

Software sneak circuit analysis

Operating hazard analysis

Operating and support hazard analysis

General design requirements

Hazard control methods

Types of hazards

Thermal, pressure, toxicity, vibration, noise,

radiation, chemical reactions, contamination, explosion, material deterioration, electrical, acceleration, mechanical

DOD MIL0781

This handbook provides test methods, test plans, and test environmental profiles which can be used in reliability testing during the development, qualification, and production of systems and equipment.

This handbook is designed to be used with MIL-STD-781. The test methods, test plans, and environmental profile data are presented in a manner which facilitates their use with the tailorable tasks of MIL-STD-781.

DOD MIL0781D

This document covers the requirements and provides details for reliability testing during the development, qualification, and production of systems and equipment with an exponential time-to-failure distribution. It establishes the tailorable requirements for reliability testing performed during integrated test programs specified in MIL-STD-785. Task descriptions for Reliability Development/ Growth Testing (RD/GT), Reliability Qualification Testing (RQT), Production Reliability Acceptance Tests (PRAT), and Environmental Stress Screening (ESS) are defined. Test time is stated in multiples of the design Mean Time Between Failures (MTBF). Specifying any two of three parameters, i.e., lower test MTBF, upper test MTBF, or their ratio, given the desired decision risks, determines the test plan to be utilized. This standard is applicable to six broad categories of equipment, distinguished according to their field service applications.

DOD MIL0785B

This document provides general requirements and specific tasks for reliability programs. It is used for reliability program planning and includes task descriptions for basic application requirements including sections on program surveillance and control, design and evaluation, development and production testing. An appendix for application guidance for implementation of reliability program requirements is also included. The subsections are in the form of purpose, task description, and details to be specified by the procuring activity. This is a program management document, not a typical detailed what-to-do standard document.

DOD MIL0790E

This document establishes the criteria for electronic and fiber optic parts product assurance programs which are to be met by manufacturers qualifying electronic parts to specification. Typical topics covered are document submission, organizational structure, test facilities, and failure analysis reports.

DOD MIL0791

This handbook supplies information on incorporating maintainability into Army materiel design. It defines maintainability and discusses its importance, quantitative measurement, and incorporation into the design process. Other subjects discussed in detail cover simplification, standardization and interchangeability, accessibility, modularization, identification and labeling, testability and diagnostic techniques, preventive maintenance, human factors, and environmental factors as they relate to maintainability.

DOD MIL0882C

This document provides requirements for developing and implementing a System safety program to identify the hazards of a system and to impose design requirements and management controls to prevent mishaps by eliminating hazards or reducing risks. It applies to every activity of the system life cycle; e.g., research, technology development, design, test and evaluation, production, construction, checkout/calibration, operation, maintenance and support, modification and disposal. Twenty-two tasks are defined in the areas of program management and control and design and evaluation. Typical tasks are system safety program plan, preliminary hazard analysis, and software hazard analysis. An appendix is provided to give some rationale and methods for satisfying the requirements previously detailed.

Issuing agency: Government, Military, US

Type: Standard

Level: Application system

Size: 128 pages

Scope: Applies to all US Dept. of Defense systems. Provides uniform requirements for developing and implementing a system safety program.

Principal topics:

General requirements

System safety program management and objectives

System safety design requirements

Risk assessment

Task-oriented requirements

Program management and control

System safety plan

Contractor management

System program reviews and audits

Hazard tracking and risk resolution

Design and integration

Preliminary hazard list

Preliminary hazard analysis

Safety requirements/criteria analysis

Subsystem hazard analysis

System hazard analysis

Operating and support hazard analysis

Health hazard assessment

Design evaluation

Safety assessment

Test and evaluation safety
Change analysis
Compliance and verification
Safety verification
Safety compliance assessment

DOD MIL1543B

This document establishes uniform reliability program requirements and tasks for use during design, development, fabrication, test, and operation of space and launch vehicles. Topics covered in this document are design for reliability; failure mode, effects, and criticality analysis (FMECA), reliability analysis; modeling and prediction; discrepancy and failure reporting; maximum preacceptance operation; effects of testing, storage, shelf life; packaging, transportation, handling, and maintainability. It gives application guidance and an appendix for FMEA for space and launch vehicle systems.

DOD MIL1576

The purpose of this document is to insure the safety of personnel, launch site facilities, and space vehicles from the hazards resulting from electroexplosive subsystem inadvertent initiation. The requirements and test methods contained in this document are not intended to insure all electroexplosive subsystem performance requirements except in those cases where failure to perform would create a hazard to personnel, launch site facilities, and space vehicles. The electroexplosive subsystem is composed of all components from the power source to, and including, the electroexplosive device; safe and arm devices, arm/disarm switches, relays and all electrical wiring used to monitor, control, arm and fire ordnance are specifically included. This Standard applies to all space vehicle systems (e.g., launch vehicles, upper stages, boosters, payloads, and related systems using electroexplosive devices).

DOD MIL1591

This document establishes uniform criteria for conducting trade studies to determine the optimal design for an on-aircraft fault diagnosis/isolation system. This document is applicable where a selection can be made between such alternatives as central computer controlled on-board centrally polled built-in test equipment (BITE), decentralized BITE, detached Aerospace Ground Equipment (AGE), etc., or combinations of the preceding. The fault diagnosis/isolation systems of interest are those used to diagnose/isolate faults at the flight line (organizational) level of maintenance. This document also provides a cost model and a maintainability labor power model.

DOD MIL1629A

This document shows how to perform a Failure Mode, Effects, and Criticality Analysis (FMECA). It establishes requirements and procedures for performing a FMECA to systematically evaluate and document, by item failure mode analysis, the potential impact of each functional or hardware failure on mission success, personnel and system safety, system performance, maintainability, and maintenance requirements. Each potential failure is ranked by the severity of its effect in order that

appropriate corrective actions may be taken to eliminate or control the high risk items. It details the functional block diagram modeling method, defines severity classification and criticality numbers. It provides sample formats for a FMEA, criticality analysis, FMEA and criticality analysis maintainability information sheet, and damage mode and effects analysis sheet. The document also provides several examples.

DOD MIL1701

This document establishes the general procedures, terms and conditions governing the preparation and completion of a hardware diagnostic test system.

DOD MIL1843

This document, which is based on the Airline/Manufacturer Maintenance Program Planning Document MSG-3, outlines the procedures for developing preventive maintenance requirements through the use of Reliability-Centered Maintenance Analysis (RCMA) for Air Force aircraft and engine systems, aircraft and engine structures and equipment, including peculiar and common Support Equipment (SE) Communications and Electronics (C-E) equipment, vehicles, weapons and other similar equipment items.

DOD MIL2074

This document establishes criteria for classification of failures occurring during reliability testing. This classification into relevant or nonrelevant categories allows the proper generation of MTBF reports. This document applies to any reliability test, including, but not limited to, tests performed in accordance with MIL-STD-781.

DOD MIL2084

This document covers the common maintainability design requirements to be used in military specifications for avionic and electronic systems and equipment.

DOD MIL2155

This document establishes uniform requirements and criteria for a Failure Reporting, Analysis, and Corrective Action System (FRACAS) to implement the FRACAS requirement of MIL-STD-785.

DOD MIL2164

This document defines the requirements for ESS of electronic equipment, including environmental test conditions, duration of exposure, procedures, equipment operation, actions taken upon detection of defects, and test documentation. The document provides for a uniform ESS to be utilized for effectively disclosing manufacturing defects in electronic equipment.

DOD MIL2165A

This document is intended to prescribe a systematic approach for establishing and conducting a testability program. It describes a uniform approach to testability program planning, establishment of diagnostic concepts and testability (including BIT) requirements, testability and test design and assessment, and requirements for conducting testability program reviews. Relevant tasks in this document are to be applied during the conceptual phase, demonstration and validation phases, full-scale development phase and production phase of the acquisition process.

DOD MIL2173

This document is used to provide procedures for a Reliability-Centered Maintenance analysis for naval aircraft, weapons systems, and support equipment. This document is used during development of new systems and equipment, and by analysts and auditors within the Naval Air Systems Command for determining preventive maintenance requirements and developing age exploration requirements. The document can also be used to update the initial reliability-centered maintenance analysis and analyze newly discovered failure modes.

EIA SEB6-A

Issuing agency: Industry association, Electronic Industries Association

Type: Guide

Level: Software

Size: 137 pages

Scope: Provides guidelines on how a system safety analysis and evaluation program should be conducted for systems which include computer-controlled or -monitored functions.

Applies to DoD weapon systems, and supplements Mil Std 882 (qv).

Principal topics:

System safety analysis tasks

Establishment of safety requirements

V&V planning

Considerations for safety analysis of system software

Life cycle activities

System software hazardous effects analysis

Technique

Format

Software safety analysis process flows and description

ESA-01-21

Issuing agency: Government, multinational, civilian, European Space Agency

Type: Standard

Level: Software

Size: 35 pages

Scope: Development and operation of software used in ESA space systems.

Principal topics:

SPA functions (note: I think this is the same as SQA in other standards)

SPA management

Organization

Planning

Reporting and control

Procedures

Metrics

Life cycle SPA activities

Requirements

Tracing

Planning

Monitoring

Reviews

Data collection

Architectural design (same breakdown)

Detailed design (same breakdown)

Installation and acceptance (same breakdown)

Operations and maintenance (same breakdown)

Comment: Doesn't seem to cover coding.

ESA-01-40

Issuing agency: Government, Civilian, European Space Agency

Type: Standard

Level: Application system

Size: 75 pages

Scope: Defines the system safety requirements which implement ESA safety policy. Applies to ESA space systems and associated equipment. Probably applies to any software in such systems.

Principal topics:

Safety program requirements

Safety organization and management

Personnel access and authority

System safety program plan

Safety program tasks

Safety assurance

Safety analysis

Hazard tracking and acceptance

Unresolved residual hazards

Safety function and item identification and control

Safety validation and qualification testing

Progressive risk assessment

Hazardous operations control

Accident & incident reporting and investigation

Safety reviews
Documentation
Safety audits
System level technical requirements
General design requirements
Failure tolerant design
Failure propagation
Operational safety
Human error
Manned system safety requirements
Escape and rescue
Hazard detection annunciation and safing
Launcher systems
Unmanned missions
Manned missions
Payload safety requirements
Ground equipment and facilities

IEC0643

Issuing agency: Standards agency, International, IEC
Type: Technical report; guide
Level: Computer system
Size: 17 pages

Scope: Digital computer use in alarm, instrumentation, control, reporting and equipment protection systems in nuclear power plants. Does not cover reactor protection systems.

Principal topics:
Application classes
Four classes of computer systems
Potential applications of computers in nuclear power plants
Reliability requirements for each class
Application principles
Logging and recording
Plant monitoring
Display systems
Plant performance calculations
Plant control systems
Protection of equipment

IEC0671

Issuing agency: Standards agency, International, IEC
Type: Standard
Level: Application system
Size: 17 pages

Scope: Protection systems in nuclear power plants. Covers principles of testing protection systems during normal operations and shutdown. Applies to computers if such are used in protection systems.

Principal topics:

General requirements for periodic testing

Coverage

Design of protection systems to facilitate testing

Test data collection

Test intervals

Testing of safety monitoring assemblies

Testing equipment

Test signals

Operability of instruments

Calibration tests

Surveillance of safety monitoring assemblies

Periodic testing of electromechanical and mechanical equipment

Test interfaces

Functional tests

Test of solid-state safety logic assemblies

Testing signals

Test data to be displayed and recorded

Test equipment

IEC0706-1

The guide is intended to make recommendations for the standardization of maintainability practices, and to stimulate ideas in the maintainability field. Includes three sections of the guide on maintainability which concern with introduction to maintainability, maintainability requirements in specifications and contracts and maintainability programme.

IEC0706-3

This guide is intended to make recommendations for the standardization of maintainability practices and to stimulate ideas in the maintainability field. Describes the various aspects of verification necessary to ensure that the specified requirements have been met, and provides suitable procedures and test methods. While verification as such should be a mandatory part of any programme, each individual case requires appropriate methods to be carefully selected in order to ensure overall cost effectiveness.

IEC0706-4

The tasks described should be performed during the system acquisition phase in order to meet the availability objectives in the operational phase. The interfaces between reliability, maintainability and the maintenance support planning programme and their tasks are also described. Annexes A and B deal with maintenance planning analysis and maintenance support resources determination.

IEC0706-5

Provides guidance for the early consideration of testability aspects in design and development and assists in determining effective test procedures as an integral part of operation and maintenance. Is applicable to all categories of equipment in their concept and principles, although many of the techniques described are clearly more applicable to the electrical and electronic fields. For mechanical equipment, the traditional diagnostic techniques can still be used. Reference is made to condition monitoring.

IEC0706-6

Specifies techniques covering some quantitative aspects of maintainability engineering in various phases of the system life cycle. Is applicable to the tasks of maintainability allocation, maintainability demonstration and maintainability data evaluation (sections five, six and seven of IEC 706-2 and IEC 706-3). In the informative annexes A, B and C, mathematical methods and procedures for performing these tasks are presented in corresponding order. Is intended to serve as an addendum, for specific maintainability topics, to existing statistical textbooks.

IEC0709

Issuing agency: Standards agency, International, IEC

Type: Standard

Level: Application system

Size: 8 pages

Scope: Design of protection systems in nuclear power plants. Covers computer systems if such are included in the protection system.

Principal topics:

Categories of possible failure-initiating events

Design errors

Protection system failure events

Single random failures

Multiple failures from a single common cause

Plant failure events

Environmental conditions

Failure of plant equipment

Operator error

External failure events

Natural events

Man-made events

Basic rules for designing a protection system

Fire protection

Operation during and after an accident

Cabling separation principles

IEC0801-1

Deals with general considerations in the context of the complexity of electromagnetic compatibility and the problems with which manufacturers and users of industrial-process measurement and control equipment may be confronted. Provides background information necessary to understand the development of the different parts of the standard on electromagnetic compatibility.

IEC0801-2

Defines the immunity requirements and test methods for equipment which must withstand electrostatic discharges. Gives several severity levels which relate to different environmental and installation conditions.

IEC0801-4

Establishes a common and reproduceable basis for the evaluation the performance of electronic instrumentation when this is subjected to repetitive fast transients (bursts), on supply, signal or control lines. Includes severity levels and the required test procedures.

IEC0812

Describes the procedure and gives guidance as to how they may be applied to achieve various objectives by providing the procedural steps necessary to perform an analysis, by identifying appropriate terms, assumptions, criticality measures, failure modes, by determining basic principles, by providing examples of the necessary forms.

IEC0880

Issuing agency: Standards agency, International, IEC

Type: Standard

Level: Software

Size: 132 pages

Scope: Software contained in computer-based safety systems in nuclear power plants.

Principal topics:

Project structure

Software QA plan

Software requirements

Software development

Verification

Hardware/software integration

Computer system validation

Maintenance and modification

Operation

IEC0880/Supplement 1

Issuing agency: Standards agency, International, IEC

Type: Draft standard

Level: Software

Size: 60 pages

Scope: Software contained in computer-based systems important to safety in nuclear power plants.

Principal topics:

Defenses against software common mode failure (SCMF)

Analysis for possible SCMF effects

Use of diverse features against SCMF

Specification, development, verification and management approaches against SCMF

Formal specification and design methods

Rationale for using formal methods

V&V using formal methods

Requirements for use and selection for formal methods

Automated tools for software development

Rationale for using automated tools

Selection and qualification of tools

Recommendations for specific tools

Use of pre-existing software products

Rationale for use of pre-existing software products

Criteria for evaluation and acceptance

Quality assurance

Contractual requirements

Safety-related application requirements

Project structure

Software requirements

Use of pre-existing software products

IEC0960

Issuing agency: Standards agency, International, IEC

Type: Standard

Level: Application system

Size: 11 pages

Scope: Design criteria for a safety parameter display system (SPDS) which provides information to aid reactor personnel, particularly under abnormal conditions. Assumes the SPDS is computer-controlled, so applies indirectly to the software in such computers.

Principal topics:

General performance requirements

Functional design criteria

Functional testing

Design criteria for the instrumentation system inputs to SPDS

Training and procedures

List of critical safety function measurements

IEC0987

Issuing agency: Standards agency, International, IEC

Type: Standard

Level: Computer system

Size: 24 pages

Scope: Computer hardware used in systems important to safety in nuclear reactors. Does not directly apply to software.

Principal topics:

Project management

Project organization and structure

Life cycle

Quality assurance

Hardware requirements

Functional and performance requirements

Reliability requirements

Environmental requirements

Documentation requirements

Design and development

Design activities

Reliability criteria

Interfaces

Documentation

Design description

V&V

Planning

Independence

Methods

Documentation

Installation and commissioning

Maintenance

Maintenance requirements

Failure data

Documentation

Modifications

Operation

IEC1025

Contains principles, identification rules, and symbols. Describes the steps to carry out an analysis, identifies appropriate assumptions, events, and failure modes.

IEC1160

Makes recommendations for the implementation of design review procedures as a means of stimulating product and for process improvement. Includes guidelines for planning and conducting design reviews and specific details concerning contributions by reliability, maintenance, maintenance support and availability specialists. Also includes subclauses on

contributions by other specialists dealing with subjects such as quality, environment, safety (product and user), human factors, and legal matters.

IEC1226

Issuing agency: Standards agency, International, IEC

Type: Standard

Level: Application system

Size: 21 pages

Scope: Creates a classification scheme for functions, systems and equipment (FSE) required in nuclear power plants.

Principal topics:

Classification

Three categories of FSE

Criteria for classifying FSE into the three categories

Classification procedures

Identification of design basis

Identification and categorization of FSE

Determination of requirements for ensuring the adequacy of FSE designs

Ensuring functionality

Ensuring reliability

Ensuring performance

Ensuring environmental durability

Quality assurance and quality control

IEC1609

Issuing agency: Standards agency, International, IEC

Type: Recommended practice

Level: Application system

This is a proposed series of eight parts. All are in draft form. The work is under TC56.

Part	Title
1	General considerations and methodology
2	Assessment of methodology
3	Assessment of system functionality
4	Assessment of system performance
5	Assessment of system dependability
6	Assessment of system operability
7	Assessment of system safety
8	Assessment of non-task-related system properties

Part 5

Principal topics:

Dependability properties

Dependability, availability, reliability, maintainability, credibility, security, integrity
Review of the system requirements document
Review of the system specification document
Assessment procedure
Analysis of system requirements and specifications
Designing an assessment program
Evaluation techniques
Qualitative techniques
Quantitative techniques

IEEE C37.1

Scope: The standard applies to systems used for monitoring, switching, and controlling electric apparatus in unattended or attended substations, generating stations, and power utilisation and conversion facilities. The standard does not apply to electromechanical or static, protective-relaying equipment.

Principal topics:

Definitions,
functional characteristics,
interfaces,
environmental conditions,
characteristics concerning:
 reliability,
 maintainability,
 availability,
 security and expandability,
 tests and inspections,
 documentation.

Keywords: Supervisory control, automatic control and data acquisition in electric power systems, functional characteristics, reliability, maintainability, availability, security, expandability, changeability, tests and inspections, documentation.

IEEE/SE

This standard collection contains some 25 standards on best practice of software engineering.

IEEE0308

Issuing agency: Professional society, IEEE Power Engineering Society

Type: Standard

Level: Application system

Size: 18 pages

Scope: Applies to the electrical systems of nuclear power plants specifically related to protection of the public. Applies only indirectly to software, if at all.

Principal topics:

Principal design criteria
Design basis event effects
Power quality
Location of indicators and controls
Equipment qualification
Single failure criterion
Circuits which penetrate containment
Supplementary design criteria
Power systems
Alternating and direct current systems
Instrumentation and control power systems
Protective action system
Surveillance and test requirements
Surveillance methods
Equipment tests and inspections

IEEE0338

Issuing agency: Professional society, IEEE Power Engineering Society
Type: Standard
Level: Application system
Size: 18 pages

Scope: Supplements IEEE 603 (qv) and IEEE 308 (qv) for the performance of periodic surveillance testing programs for safety systems in nuclear power plants. Would probably apply to software in such systems.

Principal topics:
Safety system design requirements for testability
Testing program requirements
General considerations
Types of tests
Test methods
Test intervals
Documentation

IEEE0379

Issuing agency: Professional society, IEEE Power Engineering Society
Type: Standard
Level: Application system
Size: 11 pages

Scope: Supplements IEEE 603 (qv) to interpret the 'single-failure criterion' included there as applied to electrical systems. Probably does not apply directly to software, though the principles certainly apply.

Principal topics:
Statement of the Single-Failure Criterion
Requirements for applying the single-failure criterion

Independence and redundancy
Nondetectable failures
Cascaded failures
Design base events and single failures
Common-cause failures
Shared systems
Design analysis to determine violations of the single-failure criterion
Procedures
Analysis of portions of systems
Channels and interconnections
System logic
Actuation devices
Electrical power supplies
Auxiliary supporting features

IEEE0384

Issuing agency: Professional society, IEEE Power Engineering Society
Type: Standard
Level: Application system
Size: 19 pages

Scope: Provides criteria and requirements for establishing and maintaining the independence of safety systems equipment by physical and electrical isolation in nuclear power plants. Probably does not apply directly to software, but probably does apply to the hardware in computer systems.

Principal topics:
General independence criteria
Requirements for independence
Methods of achieving independence
Electrical independence
Specific separation criteria
Cables and raceways
Standby power supplies
Power distribution system
Control switchboards
Instrumentation cabinets
Specific electrical isolation criteria
Power circuits
Instrumentation and control circuits
Shutdown circuits and equipment
Postulated exposure fires
Separation criteria

IEEE0493

Scope: The fundamentals of reliability analysis as it applies to the planning and design of industrial and commercial electric power distribution systems are presented. The

presentation is self-contained and should enable trad-off studies during the design of industrial and commercial power systems.

Principal topics:

Basic concepts of reliability analysis by probability methods

fundamentals of electric power systems

reliability evaluation

economic evaluation of reliability

cost of power outage data

equipment reliability data

evaluation and improving the reliability of an existing plant

preventive maintenance

emergency and standby power

examples of reliability analysis and cost evaluation.

Keywords: Designing reliable industrial and commercial power systems, equipment reliability data, industrial and commercial power systems reliability analysis, reliability analysis.

IEEE0494

Issuing agency: Professional society, IEEE Power Engineering Society

Type: Standard

Level: Application system

Size: 11 pages

Scope: Provides uniform criteria for the identification of documents relating to safety systems in nuclear power plants. Probably applies to documentation of software in such systems.

Principal topics:

Document identification - requires the use of the label 'nuclear safety related' on the document

Comment: This is a very short standard - the heart of the standard is less than one page, and can be summarized by one sentence (as above).

IEEE0497

Issuing agency: Professional society, IEEE Power Engineering Society

Type: Standard

Level: Application system

Size: 14 pages

Scope: Establishes minimum design criteria for accident monitoring instrumentation for nuclear power plants. Would apply to any software contained in such systems.

Principal topics:

Basis for the design

Design criteria

System design criteria

Failure criteria

Integrity

Rate and trend analysis
Channel identification
Power source
Equipment qualification
Information display channel design criteria
Classification of equipment
Isolation
Capability for test and calibration
Test methods
Instrument characteristics
Display requirements
Installation

IEEE0603

Issuing agency: Professional society, IEEE Power Engineering Society

Type: Standard

Level: Application system

Size: 32 pages

Scope: Establishes minimum functional design criteria for the power, instrumentation and control portions of nuclear power plant safety systems.

Applies to any software in such systems.

Principal topics:

Safety system criteria

Single-failure criterion

Completion of protective action

Quality of components

Equipment qualification

System integrity

Independence - several different types

Capability for test and calibration

Information displays

Human factors considerations

Reliability

Functional and design requirements for sense and command features

Automatic and Manual control

Interactions with other systems

Capability for test and calibration

Operating and maintenance bypasses

Setpoints

Functional and design requirements for executive features

Automatic and manual control

Completion of protective actions

Operating and maintenance bypasses

Power source requirements

Electrical power sources

Non-electrical power sources

Comment: This is the basic standard for nuclear power plant safety systems; quite a few other standards rely on IEEE 603. In particular, see IEEE 7-4.3.2.

IEEE0610

This standard contains definitions for more than 1000 terms, establishing the basic vocabulary of software engineering. Building on a foundation of American National Standards Institute (ANSI) and International Organization for Standardization (ISO) terms, it promotes clarity and consistency in the vocabulary of software engineering and associated fields.

IEEE0627

Issuing agency: Professional society, IEEE Power Engineering Society

Type: Standard

Level: Application system

Size: 14 pages

Scope: General standard for qualification of all types of safety systems equipment in nuclear power plants. This includes mechanical, instrumentation and electrical equipment. Probably doesn't apply directly to software.

Principal topics:

Qualification principles

Qualification requirements

Approaches to qualification

Specification criteria

Equipment safety function

Equipment description and boundaries

Interfaces

Design codes and standards

Service conditions

Aging mechanisms

Acceptance criteria

Qualification program

Program formulation

Selection of qualification methods

Interfaces

Documentation

IEEE0730

This standard has legal liability as its basic rationale. It is directed toward the development and maintenance of critical software, that is, where failure could impact safety or cause large financial or social losses. The orientation is toward delineating all of the planned and systematic actions on a particular project that would provide adequate confidence that the software product conforms to established technical requirements.

The standard establishes a required format and a set of minimum contents for software quality assurance plans. The description of each of the required elements is sparse, thus

providing a template for development of further standards, each expanding on a specific section of this document.

IEEE0828

This standard is similar in format to IEEE Std 730, but deals with the more limited subject of software configuration management. The standard identifies requirements for configuration identification, configuration control, configuration status accounting and reporting, and configuration audits and reviews. The implementation of those requirements provides a means by which the evolution of the software product items are recorded, communicated, and controlled. This provides assurance of the integrity and continuity of the software product items as they evolve through the software development and maintenance life cycle.

IEEE0829

This standard defines the content and format of eight documents that cover the entire testing process. The test plan prescribes the scope, approach, resources, and schedule of the testing activities. It identifies the items to be tested, the testing tasks to be performed, the personnel responsible for each task, and the risks associated with the plan. Test specification is covered by three document types, while test reporting is covered by four document types. The standard shows the relationships of these documents to one another as they are developed, and to the test process they document.

IEEE0830

The content and qualities of a good software requirements specification (SRS) are described and several sample SRS outlines are presented. This recommended practice is aimed at specifying requirements of software to be developed but also can be applied to assist in the selection of in-house and commercial software products.

IEEE0982.1

This standard provides definitions of selected measures. The measures are intended for use throughout the software development life cycle in order to produce reliable software. The standard does not specify the use of any of the measures. Its intent is to describe the individual measures and their use.

IEEE0982.2

IEEE Std 982.2 is a companion to IEEE Std 982.1 and provides guidance in the use of the measures in IEEE Std 982.1. It provides information needed by industry to make the best use of IEEE Std 982.1.

IEEE0990

This recommended practice provides recommendations reflecting state-of-the-art and alternate approaches to good practice for characteristics of Program Design Languages

(PDLs) based on the syntax and semantics of the Ada Programming Language. In this document, these are referred to as Ada PDLs.

IEEE1002

This standard describes the form and content of a software engineering standards taxonomy. It explains the various types of software engineering standards, their functional and external relationships, and the role of various functions participating in the software life cycle. The taxonomy may be used as a method for planning the development or evaluation of standards for an organization. It could also serve as a basis for classifying a set of standards or for organizing a standards manual.

IEEE1008

Software unit testing is a process that includes the performance of test planning, the development of a test set, and the measurement of a test unit against its environment. Measuring entails the use of sample data to exercise the unit and the comparison of the unit's actual behavior with its required behavior as specified in the unit's requirements documentation.

This standard defines an integrated approach to systematic and documented unit testing. The approach uses unit design and unit implementation information, in addition to unit requirements, to determine the completeness of the testing. The standard describes a testing process composed of a hierarchy of phases, activities, and tasks. Further, it defines a minimum set of tasks for each activity, although additional tasks may be added to any activity.

IEEE1012

This standard has a threefold purpose:

- a) To provide, for both critical and noncritical software, uniform and minimum requirements for the format and content of Software Verification and Validation Plans (SVVPs).
- b) To define, for critical software, specific minimum Verification and Validation (V&V) tasks and their required inputs and outputs that shall be included in the SVVPs.
- c) To suggest optional V&V tasks to be used to tailor SVVPs as appropriate for the particular V&V effort.

IEEE1028

Software reviews and audits are a basic part of the ongoing evaluation of software products as they pass along the software development life cycle. This standard provides direction to the reviewer or auditor on the conduct of evaluations. Included are processes applicable to both critical and noncritical software and the procedures required for the execution of reviews and audits.

IEEE1042

The purpose of this guide is to provide guidance in planning Software Configuration Management (SCM) practices that are compatible with IEEE Std 828. The guide focuses on

the process of SCM planning and provides a broad perspective for the understanding of software configuration management.

IEEE1044

This standard defines a process for classifying and establishing categories of anomalies relating to software products and providing related data and information. The standard provides a standard set of categories and classifications for relating software anomalies. Classified anomalies help in project management, product correction, and process improvement.

IEEE1046

Issuing agency: Professional society, IEEE Power Engineering Society

Type: Guide

Level: Computer system

Size: 105 pages

Scope: Use of digital computers in power plants other than nuclear power plants. Only the specific control aspects of fossil-fuel power plants have been included; apparently also excludes hydroelectric power plants. This guide presents alternative solutions, with comments on them.

Principal topics:

Objectives of distributed control and monitoring systems

Dependability

Plant efficiency

Improved response time

Extended equipment life

Improved operation

Improved operator interface

Accessibility of plant data

Cost-related factors

System application issues

Integrated versus segregated systems

Functional and geographic distribution

Hierarchical architecture and automation

Control and protection functions

Input and output systems

Environmental considerations

Documentation

Data communications structure

Data communications functions

Data communications structures

Control data communication requirements

Architectural view

Remote intelligence in distributed control systems

Single linear network topology

Special features of proprietary control networks

Hierarchical network architecture's

Data acquisition and monitoring
Man/process and man/ system interfaces
Reporting functions
Monitoring functions
Operating functions
Diagnosing functions
Plant performance functions
Optimization
Processing
Reliability, availability and fault tolerance of distributed systems
Reliability
Software/ hardware/ human reliability
Partitioning, redundancy and fault tolerance
Reliability and availability in distributed control systems

IEEE1059

The purpose of this guide is to provide guidance in preparing Software Verification and Validation Plans (SVVP) that comply with IEEE Std 1012-1987. Software Verification and Validation (V&V) is a disciplined approach to assessing software products throughout the product life cycle. A V&V effort strives to ensure that quality is built into the software and that software satisfies the user requirements.

This guide recommends approaches to verification and validation planning.

IEEE1061

This standard provides a methodology for establishing quality requirements and identifying, implementing, analyzing, and validating the process and product of software quality metrics. This standard does not prescribe specific metrics. It does include examples of metrics together with a complete example of the standard's use.

IEEE1062

A set of useful quality practices that can be selected and applied during one or more steps in a software acquisition process is described. This recommended practice can be applied to any software, but is more suited for use on modified-off-the-shelf software and fully developed software. This recommended practice defines a nine step process starting with planning the acquisition, carrying out the execution to accepting and using the software. A set of checklists are provided for use by individuals or organizations.

IEEE1074

This standard defines the set of activities that constitute the processes that are mandatory for the development and maintenance of software. The management and support processes that continue throughout the entire life cycle, as well as all aspects of the software life cycle from concept exploration through retirement, are covered. Associated input and output information is also provided. Utilization of

the processes and their component activities maximizes the benefits to the user when the use of this standard is initiated early in the software life cycle. This standard requires definition of a user's software life cycle and shows its mapping into typical software life cycles. It is not intended to define or imply a software life cycle of its own.

IEEE1219

This standard describes the process for performing the maintenance of software. It prescribes requirements for process, control, and management of the planning, execution, and documentation of the software maintenance activities.

IEEE1228

This standard describes the minimum acceptable requirements for the content of a Software Safety Plan. It addresses the processes and activities intended for development, procurement, maintenance, and retirement of safety-critical software. Safety-critical software are those software products whose failure could cause loss of life, serious harm, or have widespread negative social impact. The standard does not contain special provisions required for software used in distributed systems or in parallel processors.

IEEE1298

This is Australian Standard AS 3563.1-1991. This standard establishes requirements for a software developer's quality management system. It identifies each of the elements of a quality management system to be design, developed, and maintained by the developer with the objective of ensuring that the software will meet the requirements of a contract, purchase order, or other agreement.

IEEE7-4.3.2.

Issuing agency: Professional society, IEEE Power Engineering Society

Type: Standard

Level: Computer system

Size: 39 pages

Scope: Supplements IEEE 603 (qv) with additional computer-specific requirements. The combination of IEEE 603 and IEEE 7-4.3.2 establish minimum functional and design requirements for computers used as components of safety systems in nuclear power plants.

Principal topics:

Safety system criteria

Quality of components

Software development

Qualification of existing commercial computers

Software tools

V&V

SCM

Equipment qualification

System integrity

Design for computer integrity

Design for test and calibration
Independence
Reliability

Comments: This standard is organized in the same manner as IEEE 603, with additional requirements for some topics. Topics are omitted above when there are no additional criteria.

ISA SP84.01

Issuing agency: Professional society, Instrument Society of America (ISA)

Type: Standard

Level: Computer system

Size: 107 pages

Scope: Use of computer systems in safety related applications in the process industries, excluding nuclear reactors.

Principal topics:

Personnel competency

Safety management and planning

Safety life cycle requirements

Hazard and risk analysis

Safety integrity level selection

System design process

System implementation requirements

Installation validation and commissioning

Safety system validation

Operation and maintenance

Decommissioning

ISO2382/11

Is intended to support international communication in information processing. Providers selected English and French terms and their definitions especially in the field of processing units and arithmetic and logic units as well as registers and converters.

ISO2382/14

Is meant for the international communication in information processing. Provides selected English and French terms and their definitions of special concepts relevant to the field of data processing and identifies relationships between the entries.

ISO2382/2

Facilitates the international communication in information processing. Provides selected English and French terms and their definitions in the field of mathematics and logic. The terms relating to numeric values are dealt with under the aspect of computing techniques as for arithmetic and logical operations.

ISO6527

Identifies the typical parameters of a component that permit it to be characterized unequivocally and to allow the corresponding reliability data to be associated with those of other components having equivalent typical parameters. Parameters refer to technical characteristics including the physical principle of operation and quality level and to actual operating conditions and maintenance and test intervals. Data may be represented both in a historical and in a statistical form.

ISO7385

The output of a data collection system is strongly dependent on the quality of the information collected. Before starting such a system, it is necessary to clearly define the following items: the overall goal, the suppliers of field data, the users of processed data, the terms and expressions used, the means used to collect data and to treat them, the questions to be answered by field data, field data needed. The standard gives a comprehensive guidance to ensure quality of availability and reliability data collected in nuclear power plants.

ISO8402

Defines the basic terms relating to quality concepts as they apply to products and services, for the preparation and use of quality standards and for mutual understanding in international communications.

ISO8807

Defines the syntax and semantics of the Formal Description Technique LOTOS used for the formal description of distributed, concurrent information processing systems. LOTOS can be used to describe formally the service definitions and protocol specifications of the layers of Open Systems Interconnection (OSI) architecture described in ISO 7498, and related standards, and conformance tests for implementations of OSI protocols and/or OSI functions. It can also be applied for the formal description of other distributed systems, such as telephone switching networks. References: ISO 7498; CCITT Recommendation Z. 100, SDL.

ISO8930

Fixes the equivalence of the principal terms used in the field of reliability of structures, in different languages (English, French, Russian and German). An annex contains approximate but simple definitions of, and commentary on, the terms listed, gives indications about their use and quotes the corresponding symbols and subscripts.

ISO9074

Provides the semantics and syntax of the Formal Description Technique Estelle generally used for the formal description of distributed, concurrent information processing systems. Estelle is used formally to describe service definitions and protocol specifications of the

layers of Open Systems Interconnection described in ISO 7498. References: ISO 7185; 7498; 646.

JEAC4609

Issuing agency: Industry association, Japanese Electric Association

Type: Guide

Level: Computer systems

Size: 37 pages

Scope: Use of digital computers in the safety systems of nuclear power plants.

Principal topics:

Requirements for computers in safety systems

V&V

Alteration control and maintenance

JIS8115

This standard specifies the terms and their definitions used mainly in reliability.

MOD00-55

Issuing agency: Government, Military, United Kingdom

Type: Interim Standard

Level: Software

Size: 92 pages

Scope: Software used in UK defence equipment.

Principal topics:

Safety management

Organization and responsibility

Safety planning

Documentation

CM

Staff qualifications

Certification and acceptance

Software engineering practices

Hazard analysis

Safety integrity analysis

Life cycle activities

Specification

Design and design reviews

Implementation

Unacceptable practices

V&V

Static code analysis

Testing

Tool support

Product life cycle

Concept formulation
Feasibility
Project definition
Full development
Production
In-service
Disposal

MOD00-56

Issuing agency: Government, Military, United Kingdom
Type: Interim Standard
Level: Application system and software
Size: 64 pages

Scope: Requirements for hazard analysis in defence systems, with particular comments about the software in such systems.

Principal topics:

Management of hazard analysis
Project plan
Management structure and organization
Reduction of risks
Classification schemes
Categories of accidents
Classification of risks
Acceptability of risks
Safety critical features
Classification of functions and components
Hazard analysis activities
Preliminary hazard identification
Preliminary hazard analysis
System hazard analysis
System risk analysis
Software hazard analysis
Software classification
Software functional analysis
System change hazard analysis
Safety review
Independent safety assessment
Documentation
Requirements
Configuration control
Disaster protection
Hazard analysis techniques
Fault tree analysis
Failure modes, effects and criticality analysis

MU8004

Deutsche Bundesbahn has issued, complementary to VDE831, recommendations specifying the way to ascertain operativeness and the safe functioning in case of failure of an electronic system, in order to grant approval for use by the railway administration.

NASA NSS740.13

Issuing agency: Government, civilian, US, NASA

Type: Standard

Level: Software

Size: 28 pages

Scope: Software acquired or developed by NASA that is used as a part of a system that possesses the potential for harm to people or property.

Principal topics:

Life cycle topics

Software safety planning

Software requirements specification

Software architectural design

Software detailed design

Software implementation

Software integration and acceptance testing

Software operations and maintenance

Phase independent tasks

Safety requirements traceability

Discrepancy reporting and tracking

Software change control

Safety program reviews

Software safety analysis

Software safety requirements analysis

Software safety architectural design analysis

Software safety detailed design analysis

Software safety code analysis

Software safety test analysis

Software safety change analysis

Quality assurance

NATO STANAG 4404

Issuing agency: Government, multinational, military, NATO

Type: Seems to be a combination of standard and guide

Level: Software

Size: 26 pages

Scope: Use of computers in munitions systems by NATO member countries.

Principal topics:

Computer system design requirements

Software detailed design

Coding

Operator interface
V&V (some)
CM (minimal)

Comment: Not well organized; perhaps it's an early draft. Concentrates on low level design and coding issues.

NEN10319

This standard is intended to provide guidance for presenting data necessary to distinguish the reliability characteristics of a component. The data may be that relating to failures and failure rates or it may be data on changes (or drift) of characteristics. Such factual information should be available to the circuit and equipment designer to enable him to correctly assess the reliability of his circuits and units.

This information will be obtained from reliability test made on the electronic components in laboratories and should be presented as indicated herein.

NEN10671

To lay down principles for testing such systems during normal power operation and shutdown, so as to check complete availability especially with regard to the detection of unsafe faults. It covers the possibility of testing at short intervals or continuous surveillance, as well as periodic testing at longer intervals. To establish basic rules for the design application of the test equipment and its interface with the protection system. Further, the effect of any test equipment on the reliability of the reactor protection is considered.

NEN11069-1

This part of IEC 1069 outlines the general considerations in the assessment of industrial process measurement and control systems, hereafter referred to as "system(s)". This part, together with subsequent parts, is intended for the users and manufacturers of systems, and also for those who are responsible for carrying out assessments as an independent party.

NEN264

The flows of liquid fuels shall be capable of being interrupted by means of safety shut-off devices, which, for example, are designed as automatic valves or fast closing devices. Their reliability shall be proven by type tests according to this standard. Other test methods may be allowed where necessary. This standard comprises safety requirements and test methods for safety shut-off devices in combustion plants, which on opening release, with or without delay, the flow of the fuels mentioned below and shut off without delay on closing. This standard applies to the use of fuel oils. For other liquid fuels the test methods may be agreed between the manufacturer and the test institute. This standard also applies to safety shut-off devices forming part of devices having other functions, i.e. oil pumps. In this case the test methods apply to those parts or components of the device forming the safety shut-off device, i.e. those parts which are necessary for the closing function.

OH CE-1001

Issuing agency: Company, Canada, Ontario Hydro

Type: Standard

Level: Software

Size: 77 pages

Scope: Software engineering of safety critical software used in real-time protection systems for nuclear power plants.

Principal topics:

Software development

Requirements

Design

Coding

Verification

Requirements verification

Design verification

Code verification

Hazards analysis

Testing

Reliability qualification

Support

Planning

SCM

Training

Documentation

Comments: Internal company standard, which cannot be distributed without the permission of the company.

PEO

Issuing agency: Professional society, Canada, Prof. Eng. of Ontario

Type: Guide

Level: Software

Size: 19 pages

Scope: Responsibilities of professional engineers in using software in safety-related applications.

Principal topics:

Software engineering model (standard topics)

Legal considerations of engineering software development

Software quality framework

RAC NPRD

This document provides failure rate and failure mode information for mechanical, electromechanical, electrical, pneumatic, hydraulic, and rotating parts. The assumption that the failures of nonelectronic parts follow the exponential distribution has been made because of the virtual absence of data containing individual times or cycles to failure.

Generic failure rate tables include environment; application (military or commercial); failure rate; number of records; number failed; and operating hours. A 60 percent confidence interval is used.

RIA23

The RIA 23 specification applies the IEC65A procedures to railway signalling. It is based on three prime concepts: integrity levels, lifecycle models and roles/responsibilities of individuals and organisations.

RTCA DO178b

Issuing agency: Industry association, RTCA

Type: Guide

Level: Software

Size: 89 pages

Scope: Provides guidance on determining that software in aircraft meets the safety requirements of the aircraft.

Principal topics:

System aspects of software development

Information flow between system & software life cycle processes

System architecture considerations

System requirements considerations

Software planning

Software development

Requirements, design, coding, integration

Software verification

Reviews and analyses

Testing

Software configuration management

Software quality assurance

Certification of aircraft and engines

Software life cycle data

Use of previously developed software

Tool qualification

UIC738R

Conclusions and recommendations for the specification, design, validation, use and modification of safety related information processing and transmission systems. It contains the general philosophy for fail-safe programmable electronic systems and identifies five methods of processing information in a fail-safe way.

VDE0831

The standard includes extensive definition of railway signalling terms, together with quantitative data for electrical parameters and a description of the philosophy to be applied when designing vital signalling systems.

8.5 List of Standards Organisations

AFS	Department of the Air Force, Air Force Systems Command
AIChE	American Institute of Chemical Engineers
ALLIANZ	Allianz Versicherungs AG
AMJ	Joint Airworthiness Authority (Advisory Material Joint)
ANS	American Nuclear Society
AS	Australian Standards Institute
ASME	American Society of Mechanical Engineers
BCS	British Computer Society
BS and BSI	British Standards Institute
BSI	Bundesamt fuer Sicherheit in der Informationstechnik
BfA	Bundesanstalt fuer Arbeitsschutz
CAA	Civil Aviation Authority, Civil Aviation Airworthiness Publications
CE	Candu Computer Systems Engineering Centre of Excellence
CEN and CENELEC	European Union Standards Organisations
CFR	Code of Federal Regulations, USA
CNS	Canadian Nuclear Society
CSA	Canadian Standards Association
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DIN	Deutsches Institut fuer Normung
DOD	Department of Defence, USA
EIA	Electronics Industry Association
EN and prEN	European Union Standards
EPRI	Electric Power Research Institute, USA
ERRI	European Rail Research Institute
ESA	European Space Agency
EURO	European Standards
HSE	Health and Safety Executive, UK
IAEA	International Atomic Energy Agency
IChE	Institute of Chemical Engineers, UK
IEC	International Electrotechnical Commission
IEE	Institute of Electrical Engineers, UK
IEEE	Institute of Electrical and Electronics Engineers, USA
ISA	Instrument Society of America
ISO	International Organisation for Standardisation
ITSEC	Information Technology Security Evaluation Criteria
JEAC	Japanese Atomic Energy Commission
JIS	Japanese National Standards Institute
JTC1	ISO/IEC Joint Technical Committee No. 1
KTA	Kerntechnischer Ausschuss Geschäftsstelle
MOD	Ministry of Defence, UK
MU	Deutsche Bundesbahn, Munich
NASA	National Aeronautics and Space Administration
NATO	North American Treaty Organisation
NAVORD	Navall Ordinance
NEN	Nederlands Normalisatie Instituut
NF	French National Standard

NUREG	Nuclear Regulatory Guide
Oe	Austrian National Standard
OH	Ontario Hydro A& Atomic Energy of Canada Limited
PN	Polish National Standard
RIA	Railway Industry Association, UK
RTCA	Radio Technical Commission for Aviation
TCSEC	Trusted Computer Systems Evaluation Criteria. DOD, USA
TS	Turkish National Standard
TUEV	Technischer Überwachungsverein
UL	Underwriters' Laboratories
VDE	Verein Deutscher Elektrotechniker