IEC TR 62987

Edition 1.0 2015-09

TECHNICAL REPORT

colour inside

Nuclear power plants – Instrumentation and control systems important to safety – Use of Failure Mode and Effects Analysis (FMEA) and related methods to support the justification of systems

IEC TR 62987:2015-09(en)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue
The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

IEC publications search - www.iec.ch/searchpub
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and also once a month by email.

Electropedia - www.electropedia.org
The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in 15 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
More than 60 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

IEC TR 62987

Edition 1.0 2015-09

TECHNICAL REPORT

colour inside

Nuclear power plants – Instrumentation and control systems important to safety – Use of Failure Mode and Effects Analysis (FMEA) and related methods to support the justification of systems

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 27.120.20

ISBN 978-2-8322-2886-9

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD 3
INTRODUCTION 5
1 Scope 7
2 Normative references 7
3 Terms and definitions 8
4 References to FMEA in published standards 8
4.1 General 8
4.2 IEC standards 8
4.2.1 IEC 60812 8
4.2.2 IEC 61513 9
4.2.3 IEC 61226 9
4.3 Other standards 9
4.3.1 General 9
4.3.2 IEEE Std 7-4.3.2-2003 9
4.3.3 ANSI/IEEE Std 352-1987 9
4.3.4 IEEE Std 577-2004 10
5 Scope of application of FMEA 10
5.1 Relationships to other methods 10
5.2 Analysis subjects 10
5.3 Common cause failure 10
6 Examples of applications 11
6.1 General 11
6.2 Replacement items 11
6.3 Survey results 12
7 Industry practice and regulatory relevance 12
7.1 General 12
7.2 France 12
7.2.1 Experience of practice for FMEA records authority (licensing) 12
7.2.2 Board-level FMEA 13
7.2.3 System-level FMEA 14
7.2.4 Subset-level FMEA 15
7.2.5 Tools to support FMEA 16
7.2.6 Current research 17
7.2.7 Dissemination of FMEA practice 17
7.3 United Kingdom 18
7.4 United States 18
8 Conclusions 19
Annex A (informative) Standardized form used in survey 20
Bibliography 21

Figure 1 – Safety case studies including FMEAs 13

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – USE OF FAILURE MODE AND EFFECTS ANALYSIS (FMEA) AND RELATED METHODS TO SUPPORT THE JUSTIFICATION OF SYSTEMS

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

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

IEC TR 62987, which is a technical report, has been prepared by subcommittee 45A: Instrumentation, control and electrical systems of nuclear facilities, of IEC technical committee 45: Nuclear instrumentation.

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

Enquiry draft	Report on voting
45A/1006/DTR	45A/1028/RVC

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

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

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

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

A bilingual version of this publication may be issued at a later date.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

a) Technical background, main issues and organisation of the Technical Report

Failure mode and effects analysis (FMEA) is a qualitative method of reliability analysis that may be applied to many different types of systems. It is an inductive method of performing system reliability or safety analysis from a low to a high level (IEC 60812).

There is a need to provide guidance on nuclear-specific issues, for example common cause failure and meeting the single failure criteria, when applying failure mode and effects analysis (FMEA) and related methods to instrumentation and control systems important to safety in nuclear power plants. The information gathered in the development of this technical report was used to determine if the topic can be standardised. If a positive conclusion was reached the intent was to produce a scope and a first draft CD of a standard. Such a standard would use IEC 60812 as its basis and provide guidance specific to the nuclear industry for implementing IEC 60812. The conclusion in this technical report is that the topic is not yet amenable to standardisation, however, additional development of the topic by the committee would be beneficial and could result in a standard at a later date.

This Technical Report identifies international standards applicable to nuclear power plant instrumentation and control systems that invoke FMEA as a method. It describes the contexts in which the standards invoke FMEA. The Technical Report describes how FMEA and associated methods have been applied to nuclear power plant instrumentation and control systems important to safety and to systems with similar attributes. The examples are followed by descriptions of the response of regulators to the use of FMEA and related methods in regulatory processes. The examples and regulatory experiences are based on a survey of and contributions by participating national committees. A bibliography is provided for further reference.

b) Situation of the current Technical Report in the structure of the IEC SC 45A standard series

IEC TR 62987 as a technical report is a fourth level IEC SC 45A document.

For more details on the structure of the IEC SC 45A standard series, see item d) of this introduction.

c) Recommendations and limitations regarding the application of the Technical Report

It is important to note that a technical report is entirely informative in nature. It gathers data collected from different origins and it establishes no requirements.

d) Description of the structure of the IEC SC 45A standard series and relationships with other IEC documents and other bodies documents (IAEA, ISO)

The top-level document of the IEC SC 45A standard series is IEC 61513. It provides general requirements for I&C systems and equipment that are used to perform functions important to safety in NPPs. IEC 61513 structures the IEC SC 45A standard series.

IEC 61513 refers directly to other IEC SC 45A standards for general topics related to categorization of functions and classification of systems, qualification, separation of systems, defence against common cause failure, software aspects of computer-based systems, hardware aspects of computer-based systems, and control room design. The standards referenced directly at this second level should be considered together with IEC 61513 as a consistent document set.

At a third level, IEC SC 45A standards not directly referenced by IEC 61513 are standards related to specific equipment, technical methods, or specific activities. Usually these documents, which make reference to second-level documents for general topics, can be used on their own.

A fourth level extending the IEC SC 45A standard series, corresponds to the Technical Reports which are not normative.

IEC 61513 has adopted a presentation format similar to the basic safety publication IEC 61508 with an overall safety life-cycle framework and a system life-cycle framework. Regarding nuclear safety, it provides the interpretation of the general requirements of IEC 61508-1, IEC 61508-2 and IEC 61508-4, for the nuclear application sector, regarding

nuclear safety. In this framework IEC 60880 and IEC 62138 correspond to IEC 61508-3 for the nuclear application sector. IEC 61513 refers to ISO as well as to IAEA GS-R-3 and IAEA GS-G-3.1 and IAEA GS-G-3.5 for topics related to quality assurance (QA).

The IEC SC 45A standards series consistently implements and details the principles and basic safety aspects provided in the IAEA code on the safety of NPPs and in the IAEA safety series, in particular the Requirements SSR-2/1, establishing safety requirements related to the design of Nuclear Power Plants, and the Safety Guide IAEA NS-G-1.3 dealing with instrumentation and control systems important to safety in Nuclear Power Plants. The terminology and definitions used by SC 45A standards are consistent with those used by the IAEA.

NOTE It is assumed that for the design of I&C systems in NPPs that implement conventional safety functions (e.g. to address worker safety, asset protection, chemical hazards, process energy hazards) international or national standards would be applied, that are based on the requirements of a standard such as IEC 61508.

NUCLEAR POWER PLANTS – INSTRUMENTATION AND CONTROL SYSTEMS IMPORTANT TO SAFETY – USE OF FAILURE MODE AND EFFECTS ANALYSIS (FMEA) AND RELATED METHODS TO SUPPORT THE JUSTIFICATION OF SYSTEMS

1 Scope

This Technical Report provides guidance on nuclear-specific issues when applying Failure Mode and Effects Analysis (FMEA) and related methods to instrumentation and control systems important to safety in nuclear power plants. The information in this Technical Report complements, for nuclear power plant applications, the procedure for FMEA in IEC 60812.

This Technical Report attempts to provide information, in the context of applications to nuclear power plant instrumentation and control systems important to safety, on:

- terminology used in FMEA processes,
- benefits of using FMEA,
- shortcomings and limitations of FMEA methods,
- anticipated outcomes of and claims to be made from application of FMEA,
- relationships to other analysis methods used in establishing the safety / reliability of nuclear power plant designs,
- typical FMEA process inputs,
- typical FMEA process outputs,
- typical initiators of FMEA processes,
- most prevalent uses of FMEA processes,
- recommended uses of FMEA processes,
- discouraged uses of FMEA processes,
- FMEA work product contents and characteristics,
- FMEA work product configuration management practices,
- good practices,
- supporting tools,
- specific examples of FMEA use for nuclear power plant licensing, and
- FMEA references.

2 Normative references

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

IEC 60812:2006, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 61226:2009, *Nuclear power plants – Instrumentation and control important to safety – Classification of instrumentation and control functions*

IEC 61513:2011, *Nuclear power plants – Instrumentation and control for systems important for safety – General requirements for systems*

ANSI/IEEE Std 352-1987, *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems*

IEEE Std 577-2004, *IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Facilities*

IEEE Std 603-1998, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*

IEEE Std 7-4.3.2-2003, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*

IAEA Nuclear Energy Series publication No. NP-T-1.5:2009, *Protecting Against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
common cause failure
CCF
failure of two or more structures, systems or components due to a single event or cause

Note 1 to entry: Common causes may be internal or external to an I&C system.

Note 2 to entry: The IAEA definition differs from the IEC definition in two points:

a) The term “specific” was deleted because otherwise the definition of CCF is not consistent with the definition of CMF “Common mode failure”. Furthermore, this additional word is not necessary in order to understand the definition.

b) The word “and” was replaced by “or” because IEC/SC 45A experts thought it was a typing fault. In the online IAEA dictionary (NUSAFE) this correction was already made.

[SOURCE: IAEA Safety Glossary 2007 Edition, modified]

4 References to FMEA in published standards

4.1 General

This clause identifies and discusses international and national standards that discuss the use of FMEA in their application and which may have applicability to nuclear power plants.

4.2 IEC standards

4.2.1 IEC 60812

IEC 60812 is one of a number of standards on analysis techniques for system reliability. It defines a procedure for applying FMEA in the pursuit of reliable designs and processes. While IEC 60812 focuses on reliability assurance, it does recognize that FMEA may be and often is used in support of achieving system safety objectives. IEC 60812 is not specific to nuclear safety applications and does not provide guidance specific to such applications.