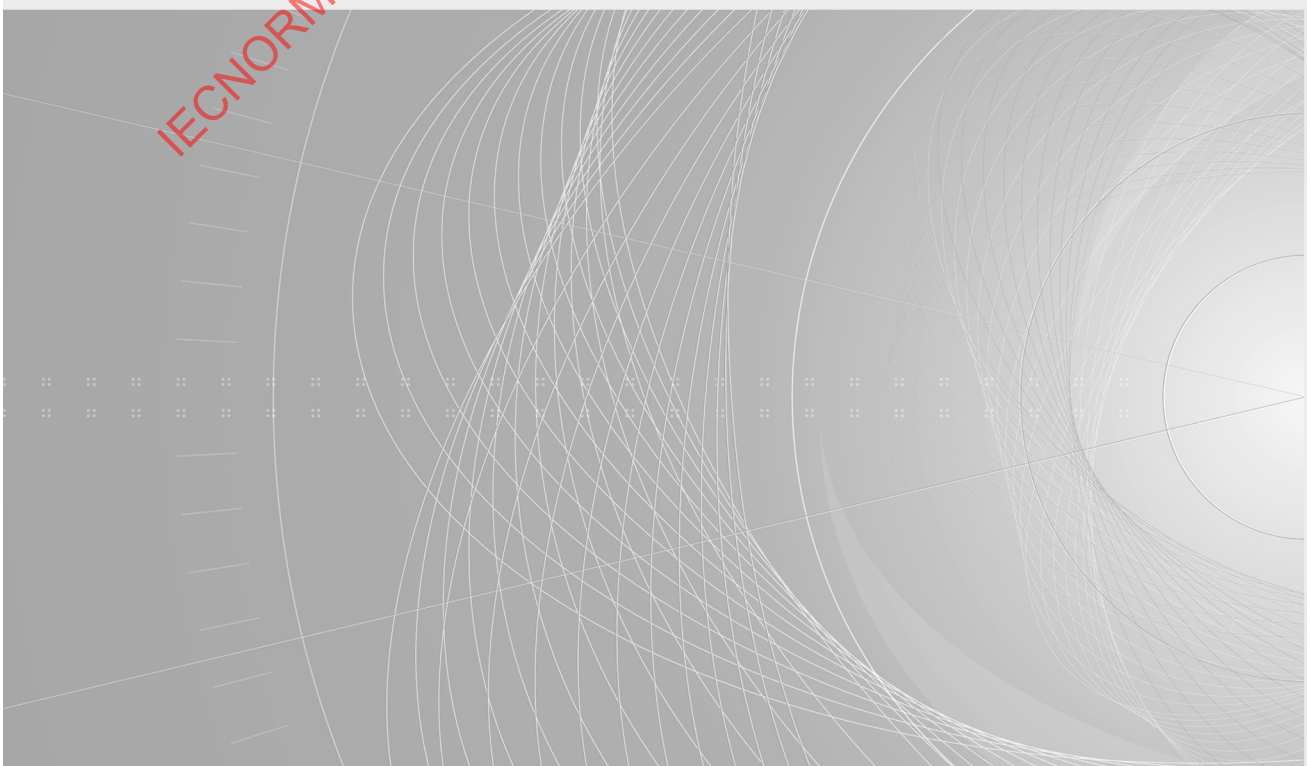
IEC TR 62987

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 It also gives information on projects, replaced and withdrawn publications.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

CONTENTS

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.

4.2.2 IEC 61513

IEC 61513:2011 identifies failure mode and effect analysis as one of several systematic analysis methods that may be used to determine the extent of preventive maintenance (in 6.3.8 System maintenance plan).

IEC 61513:2011, in 5.4.2.6, recommends an assessment of the possible failure modes and failure sequences, including their effects on components whose loading is independent of demand, and of components of the I&C systems performing category A functions whose loading is demand dependent.

4.2.3 IEC 61226

IEC 61226 recommends that FMEA analysis techniques are used to analyse systems and equipment which implement category A functions (7.3.2.1 of IEC 61226:2009).

4.3 Other standards

4.3.1 General

In addition to the IEC, a number of standards development organizations have discussed the use of FMEA in their nuclear power plant standards.

4.3.2 IEEE Std 7-4.3.2-2003

This standard applies to the use of computer systems in the safety systems of nuclear power plants. It is endorsed by the US NRC (Nuclear Regulatory Commission) as providing acceptable methods for meeting regulatory requirements, with certain limitations, as identified in US NRC Regulatory Guide 1.152.

Annex D is an informative annex to IEEE Std 7-4.3.2 on the identification, evaluation, and resolution of hazards during the development of computer equipment for use in safety systems of nuclear power generating stations. Clause D.4.2.3.2 of Annex D discusses the use of FMEA as a way to elicit potential causes for evaluation against identified hazards. Annex D itself was not endorsed by the US NRC because the staff concluded that the guidance provided by Annex D was inadequate. Specific Annex D inadequacies are not identified in the applicable regulatory guide.

Annex D to IEEE Std 7-4.3.2-2003 states that IEEE Std 603-1998, which standardizes criteria for safety systems of nuclear power generating stations, suggests the use of FMEA for performing reliability analysis, as evidenced by a reference in IEEE Std 603-1998 to IEEE Std 352-1987, which provides guidance on the reliability analysis of nuclear power generating station safety systems.

4.3.3 ANSI/IEEE Std 352-1987

This standard is a guide for the designers and operators of nuclear power plant safety systems and the concerned regulatory groups that provides the essential methods and procedures of reliability engineering that are applicable to such systems.

Subclause 4.5 of this standard is titled “Extended Qualitative Analysis for Common-Cause Failures”. According to the standard, the section “describes an extended qualitative analysis procedure, based on the FMEA, that is designed to suggest to the analyst possible common-cause failure mechanisms not normally considered in an analysis of independent component failures.”

IEEE Std 352-1987 is identified by IEEE Std 577-2004 as the source of guidance on the application and use of the reliability techniques to which the standard refers.

4.3.4 IEEE Std 577-2004

The stated purpose of IEEE Std 577-2004 is “to provide uniform, minimum acceptable requirements for the performance of reliability analyses for safety-related systems found in nuclear facilities.” It defines f*ailure mode* as “all applicable, significant failure modes for each class of component, module, or device.”

IEEE Std 577-2004 identifies IEEE Std 352-1987 as the source of guidance on the application and use of the reliability techniques to which the standard refers.

5 Scope of application of FMEA

5.1 Relationships to other methods

FMEA is one of several methods used in failure (or hazards) analysis. Other methods are analysis of abnormal conditions and events (ACEs), fault tree analysis (FTA), hazards analysis, and software safety analysis.

5.2 Analysis subjects

The design details that are available and the point in the life cycle at which FMEA is to be applied are important factors in determining the scope of a FMEA. FMEA is a “bottom-up” method: For the method to be used, the “bottom” of the system (to the extent that it exists at the time of the analysis) shall be defined.

The selection of specific equipment for implementing safety systems is often intentionally deferred. (For example, as in the standardised reactor design approach in the United States under United States national regulation 10 CFR Part 52.) Even so, there is value in applying FMEA at the level of design detail that is available at early stages in system design. Information from a high-level FMEA may be used to guide instrumentation and control equipment selections. Detail-level FMEA can be used on the equipment itself once equipment candidates have been identified. Failure modes from the high-level analysis will correspond to failure effects in the equipment. (See Figure 2 of IEC 60812:2006.)

FMEA may be applied at the lowest possible level of detail during the development of pre-qualified safety system platforms, instruments, and other such items. Very specific failure modes may be identified in these cases. However, failure effects will remain highly specific to the item being developed since plant- and application-specific failure effects will not be known during a generic qualification. The FMEA of a generic item should support future development of a system based on that item. Guidance has been developed by the nuclear industry to support this approach.

5.3 Common cause failure

IEC 60812 indicates that the FMEA method is not applicable to situations with multiple or dependent failures. Even so, as described below, failure modes identified through a FMEA process can have causal relationships to other failures within the analysed system, or to failures outside of the scope of the relevant analysis. See IEEE Std 352-1987 for examples.

FMEA may be useful during the performance of the confirmatory assessment of a common cause failure (CCF) evaluation (IAEA Nuclear Energy Series publication No. NP-T-1.5). The basis of such a confirmatory assessment is the conceptual nuclear power plant design after obvious CCF vulnerabilities have been removed. In the context of the confirmatory assessment, FMEA is an analytical method that may be useful in developing reasonable assurance that required safety functions will be performed in the presence of concurrent design basis event (DBE) and CCF.

During evaluation of the I&C system, once the assumptions about the CCF susceptibility of blocks are known, CCFs are postulated, and the effect on safety functions is determined. For

each set of blocks susceptible to the same CCF, the failure in the most adverse way should be postulated and the effect on plant safety functions (when they are needed to mitigate postulated accidents or transients) determined. (IAEA Nuclear Energy Series publication No. NP-T-1.5)

FMEA is often used in assessments of an I&C architecture's susceptibility to CCFs. Failures to be considered are developed from detailed analyses of functional units and the integrated architecture. These analyses can be performed after a representation of the decomposed I&C architecture is available. (IAEA Nuclear Energy Series publication No. NP-T-1.5)

Subclause 4.5 of IEEE Std 352-1987 describes an extended qualitative analysis procedure, based on FMEA, that is designed to suggest possible common-cause failure mechanisms not normally considered in an analysis of independent component failures.

6 Examples of applications

6.1 General

This clause discusses examples of the application or use of FMEA in nuclear power plant safety analysis.

Data collection for this Technical Report included a survey of member national committees regarding examples of the use of FMEA for the purposes of nuclear power plant design and licensing. The survey requested information including:

Confirmation of the scope of use of FMEA techniques for example for:

- Analogue devices - circuits, cards / boards or devices (e.g. power supplies)
- Discrete component (op amps, logic gates) - circuits, cards / boards or devices
- Complex / 'programmable' device (PLDs, microprocessors, FPGAs, ASICs) – circuits, cards / boards or devices
- Modules, e.g. made up of – racks, power supplies and/or cards/boards
- Systems, e.g. made up of – modules

Description of examples of use of the techniques:

- A description of context in which FMEA was applied,
- Description of the scale of the equipment,
- A listing of tools that were used, including support tools (software, templates, etc.),
- The specific type of FMEA used (FMEDA, FMECA, or other variations),
- How outputs were documented (content, format),
- Who were the intended users of results (e.g. to whom documentation was delivered),
- A description of the degree of effort (total number of person-hours, etc.),
- The overall time span of the effort (start/finish of analysis),
- The team composition (number, roles, types and degrees of experience), and
- Perceived benefits of the exercise (determination of reliability, proof test intervals, redesign to eliminate unrevealed failures, etc.).

6.2 Replacement items

Specific guidance on the use of FMEA in the process for evaluating replacement items not originally designed and manufactured to nuclear power quality standards is given in Electric Power Research Institute (EPRI) report number 1008256. In this guidance, the FMEA is used to identify an item's credible failure modes and to identify the effects of the failure modes on

the systems affected by the item. The guidance on the analysis stipulates the assumptions that maintenance procedures have been properly followed and that all parts of an item are present. For FMEA to be useful in context of safety assurance, the safety functions of the item shall be known.

The EPRI report includes an appendix that lists typical failure mechanisms and modes and could therefore be useful in the process of identifying failure modes. Two important parts of the process are distinguishing between credible and non-credible failure mechanisms and documenting the bases of the determinations. The guidance identifies the following inputs as useful to the failure effects evaluation:

- Piping and instrumentation diagrams
- Isometrics
- Electrical schematics
- Electrical one-line diagrams
- Electrical elementary drawings
- Instrument loop descriptions
- Technical specifications
- Supplier drawings
- Supplier instruction manuals
- System descriptions
- Safety analysis report (with accident descriptions)

6.3 Survey results

The proprietary nature of much of the information requested for the survey placed severe limitations on the information that could be returned by the national committees. The information that was provided is presented in the sections below. The form used in the survey is reproduced in Annex A.

7 Industry practice and regulatory relevance

7.1 General

Historical and current uses of FMEA in national environments are described in this clause.

Examples of the use of FMEA are described for several nations.

7.2 France

7.2.1 Experience of practice for FMEA records authority (licensing)

Even before the publication of the IEC 60812 standard, FMEA method was used to validate technical solutions for safety control and associated monitoring systems. The analysis of failure modes and of their effects (FMEA) was performed on safety systems as early as the 90's for French 1 300 MWe pressurized water reactors (PWR) and later on for 1 450 MWe PWR.

The design of these systems include self-test and watchdog functions to locally limit the effects of hypothetical malfunctions or failures that could lead to unwanted behavior at the system level. The FMEA method is used primarily for determining that the frequency of periodic testing is adapted regarding hardware failure modes and may be used as input in probabilistic safety assessment (PSA level 1).

The FMEA technique has been applied in France to systems including no software as well as for systems using software. In the latter case, the analysis has not been done on the software itself but the hardware and software together by assuming conformance of software regarding its specification.

Requirements for safety classified systems stipulate that the FMEA methodology applied takes into account failure modes including blocking failures and spurious failures. This analysis should show that under any circumstances the hardware fault to occur is detected either by online tests or by periodic testing and leads to a predefined behaviour of the system.

The safety assessment of 1 300 MWe PWR included the FMEA of the protection and safeguard system. This system is composed of analogue and digital inputs processing units, units running protection algorithms, and units implementing voting logics. The system includes functions for the protection of the reactor and the launch of safeguard systems when necessary. FMEA was part of the assessment of each system. See Figure 1.

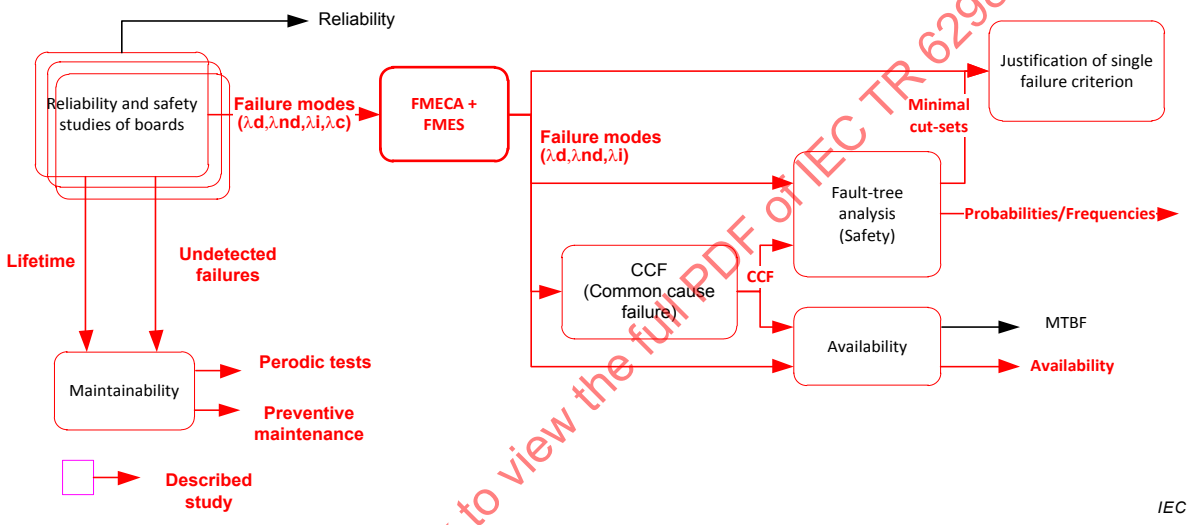


Figure 1 – Safety case studies including FMEAs

7.2.2 Board-level FMEA

Studies of reliability and safety of individual boards (e.g. circuit cards) define the different failures states of each board with their occurrences and types of failure. These studies provide also a summary. The information obtained at this level are the failure modes and constitutes the input data used for the FMEA of the higher level (sub-system or system).

The effects are then propagated on the higher-level (sub-) system, taking into account the different types of monitoring means of the studied (sub-) system existing for detecting or mitigating their consequences.

Synthesis (FMES) of this FMEA can then be used to:

- assess the availability of the (sub-) system;
- build fault tree(s) and compute the probability and occurrence frequencies of postulated events previously identified;
- verify that no hardware single failure could cause the loss of the safety function (complemented by the minimal cut (the order) provided by fault trees).

Outputs of FMEA on boards include the list of failures non-detected by the self-test that shall be covered by periodic tests and the board lifetime that leads to recommendation on preventive maintenance.

System FMEA feeds different objectives. Its primary purpose is to summarize all the effects that the board (sub-system) failure modes can generate and provide monitoring test coverage. The types of failures and the system effects are used in upper level studies according to their relevance. This study also allows taking into account the fall-back positions, degradation, inhibitions and optional self-tests at the system level in order to build the rationale using fault trees and availability studies with regards to the system safety requirements.

7.2.3 System-level FMEA

The system level FMEA, which has been implemented for PWRs in France, followed the following steps:

- Determination of safety objectives of the protection system from reactor design requirements
- Description of the functional architecture of the system
- Statement of undesirable events of the system
- Identification of the critical paths[1]
- FMEA: description of the principles used for the analysis, definition of information and data used to carry out FMEA, identification of means of detection (with location) for the effects of postulated failures
- Summary of FMEA.

At that level, hypotheses have to be assumed for describing the limits of that study in terms of:

- Analysis method:
  - A single failure at a time is analysed (multiple failures are analysed by other types of studies).
  - Human errors are excluded.
  - Manual operations are excluded.
  - Mechanical and electrical interfaces are assumed to be reliable (brackets, screws, nuts, cables, etc.), consequences of their degradation are thus not taken into account.
  - Programmable systems have a deterministic behaviour (outputs depend on a finite set of observable input parameters and of a non-degraded state of the system hardware components).
  - Catalectic failure is excluded (failure that causes an unexpected, full stop).
  - Non-explicit failures are assumed undetected.
- Input data: those coming from studies of reliability and safety of the boards that will be used as failure modes of the (sub-) system FMEA.

The FMEA conducted typically encompasses:

- A Functional Analysis, which contains:
  - a description of the functional architecture of the system,
  - a description of the critical paths to understand at first the nominal operation of the system and better infer the effects of failures (dysfunctional aspects). A critical path highlights the elements/components directly affecting the safety of the system, and therefore the parts that are particularly important for the analysis.
- A Dysfunctional Analysis which contains:

[1] All necessary components directly related to the fulfilment of the safety function carried out.

  - a description of the methodology: description of the principles adopted for that FMEA (for example: analysis of all board failure modes identifying for each the effect on equipment and the system with respect to monitoring still existing at each level),
  - a definition of degraded modes if inhibition or in case of a failure detection causing degradation in the voting logics (for example).
- A system(s) FMEA that includes:
  - identification of the means of detection implemented (or to be implemented if necessary) which can be used in that FMEA (location, type, frequency, triggered action). The description of the action upon detection allows for identification and determination of the system behaviour due to self-test triggering and also the maximum detection time,
  - an overview of the format of the FMEA (table columns, etc.),
  - the features taken into account (function fall-back positions).

A summary of the FMEA is produced indicating the sum of the failure rates of all failure modes which contribute to the same final effect ("stuck off output") considering output validity and detection of hardware fault or internal misbehaviour.

The remaining undetected hardware faults are identified. The related hardware needs to be tested during periodic tests in order to detect the possible undetected latent faults within the system and, if detected, to repair the faulty component. These tests permit limiting the persistence of those faults which directly and significantly impact the safety and availability of the system and thus increase the risk of multiple failures within the system. Predictive failure rates of that hardware have to be confirmed as sufficiently conservative regarding operating experience collected on equivalent equipment/components used in similar contexts (i.e., environmental stresses, embedded functions, etc.). Test periodicities then have to be justified based on board failure rates.

Once confirmed, failure rates and test periodicities can be used in probabilistic safety assessment (see Figure 1).

7.2.4 Subset-level FMEA

Each equipment subset (electronic board, board rack, rack cabinet with power supply) used in the protection system has been subjected to an analysis.

For an electronic board for instance, the methodology includes:

- The general description and the identification of inputs and outputs of the board, its operating environment, the block diagram with a description of each function block.
- The reliability study of the board with the definition of “life profile”, the operating parameters of the components, the distribution of failure modes, the study of aging sensitive components (life span), and the determination of the function block reliability.
- Construction of dependability from the safety objectives, the definition of postulated events and the expected effects. This approach allows the identification of self-tests required to achieve the assigned safety objectives. These self-tests are defined and described to indicate the type of self-test, frequency and action taken upon detection of an internal failure.
- The dysfunctional analysis with a description of the principles used in the analysis, the format of the FMEA presentation, the results obtained after the application of the failure modes.
- The synthesis results showing:
  - the types of faults to be covered by periodic testing,
  - the types of faults covered by internal detection mechanisms (during operation),
  - the overall rate of failure by effect and by type of failure,

  - the critical components, if any.
- The summary of the reliability and safety data of the subset.

Test coverage ratio is often computed by summing internal failure rates detected by self- test and dividing it by the sum of component failure rates. It is thus very important to indicate on which basis individual failure rates have been estimated to avoid bias of estimation through giving greater importance to failure rates of components that are frequently tested.

7.2.5 Tools to support FMEA

The FMEA applied to systems represents a major effort to get the results, given the number of sub-assemblies and components therein.

The generalization of these analyses would encourage companies to develop tools that enable iterations necessary to fulfil the required reliability figures of safety classified systems.

For several years, the systems engineering profession has established tools that support the achievement of FMEA.

The current complexity of systems leads to a representation in several layers where each layer contains a higher level of details. Thus, the first main goal of new tools is to offer modeling capabilities taking into account different granularity levels and to propose reusable libraries of sub-assemblies, by increasing common knowledge on existing design.

Some available tools like Windchill Quality Solution© (previously named RELEX), ItemToolKit©, ReliaSoft©, Isograph©,[2] etc., are already able to build their own or a user's library of sub-assemblies with their associated, previously performed reliability and FMECA analyses.

Even if some of them are able to suggest final effects of a global modeled system (set of sub-assemblies) with a predefined set of self-tests and set of final effects, the outputs of these semi-automated methods need to be validated by the safety engineer mainly because of a remaining low reliability of these tools and methods.

Functional representation of different blocks could help to perform this task. Tools, such as SIMFIA©[3] or Safety Architect©[4,5], are constantly integrating greater capacity to ease model validation by system engineers (mechanical, electrical and I&C). These are mainly based on representing systems using widespread engineering methods (SADT, SART, sub sets of UML[6] formalism) with the possibility of importing models coming from development life cycle phases and to verify that the representation of the system by its model is sufficient to perform the FMEA. They provide the possibility to include several constraints sets such as task allocation, interfaces or some basic functional constraints. This type of tool permits increases in the traceability between different levels of details and in-depth verification throughout the system life cycle.

---

[2] Trade names or Trademarks of products are examples of suitable products available commercially. This information is given for the convenience of users of this technical report and does not constitute an endorsement by IEC of these products.

[3] See Apsys http://www.apsys.eads.net/fr/17/Nos-Progiciels.

[4] See All4tec http://all4tec.net/index.php/en/model-based-safety-analysis/25-safety-architect-a-mbsa-tool.

[5] Trade names or Trademarks of products are examples of suitable products available commercially. This information is given for the convenience of users of this technical report and does not constitute an endorsement by IEC of these products.

[6] The Unified Modeling Language, standardized by the Object Management Group. See http://www.omg.org/uml.

Some tools are capable of generating fault tree models of sub-systems by considering equivalent electronic circuits and by propagating the effect of a limited set of well characterized failure modes. Nevertheless combinatory explosion of model complexity typically requires model simplification, which may lead to a less comprehensive representation for a final user. As usual, the most important thing for engineers remains to understand how the tool is proceeding in order to limit inappropriate use of its functionalities. That is why each tool's processing principles shall be well documented and thoroughly and correctly explained by vendors.

All assumptions made during local analysis and results of the global analysis have to be documented as well as the impact on results of the shortcuts made to conduct the analysis.

7.2.6 Current research

Today, FMEA asks questions that are the subject of research.

A recent report[7] published jointly by the IRSN and the US NRC (NUREG/IA-0254 June 2011) shows that, to date, there is no effective use of FMEAs that demonstrate the quality of software in complex logic systems[8]. The limits today are mainly:

- the impossibility of characterizing internal complex logic malfunctions in a sufficiently representative and limited number of failure modes,
- the difficulty of characterizing the consequences of failure modes, for example depending on the time of occurrence of the fault, constraints of schedules, variability of delay in relation to the allocation of unit processes, considering that some of which are also correlated.

These limitations are in addition to:

- the impossibility of modelling unknown specific faults introduced during the design and unidentified at successive test campaigns;
- time shrinking for electronic cards of these systems (obsolescence).

The obvious interest of using FMEAs in the broader framework of probabilistic safety assessment has led the OECD NEA / CSNI to form a working group to get taxonomies of failure modes of the different levels encountered in systems combining hardware and software. This research is conducted at the international level to identify and make homogeneous such taxonomies that would allow for FMEAs models to be integrated into the probabilistic assessments. Apart from this, efforts have already been performed in France for two decades in several research groups, including leading companies in aeronautics (e.g., EADS, APSYS, Dassault) and industry (e.g., TOTAL, CEA).

Regarding results of these international or nationwide research groups, these efforts have not yet led to significant progress in terms of classification. The increase of complexity of programmable electronics has led to a wider set of failure modes, which increases the difficulty of such researches to converge on this topic.

7.2.7 Dissemination of FMEA practice

Several schools of higher education and universities contribute to the dissemination of best practices in the field of FMEAs applied to nuclear safety systems. These courses are at Masters level and usually last 32 h per year.

---

7 Suitability of fault modes and effects analysis for Regulatory Assurance of Complex logic in Digital Instrumentation et Control Systems Luis Betancourt (US-NRC), Sushil Birla (US-NRC), Jean Gassino (IRSN), Pascal Régnier (IRSN), NUREG/IA-0254, June 2011.

8 Logic system for which it is not practicable to ensure the correctness of all behaviors through verification alone.

The purposes of these courses are:

- to show the necessary coupling between Design and FMEA/FTA techniques;
- to illustrate the resulting structure of the control-command adopted for the 1 450 MWe French PWR;
- to demonstrate built-in capability of a design based on deterministic multitask framework to control the consequences of a postulated fault in a hardware system that runs software.

Examples of FMEAs/FTAs are examined to show the need of combined techniques at all steps for safety related systems.

A complete list of tools for semi-automated generation of FMEA is not given by literature. Nevertheless it is possible to find most of them by using web search and identifying research laboratories working on this subject. Today, wide-spread tools are commonly used by electronics industry (e.g. companies like Intel or Siemens have developed their own tools that stay strongly under IP-control), defence, aeronautic, aerospace and nuclear domains.

7.3 United Kingdom

FMEA techniques are used to analyse I&C systems and equipment of all technologies (analogue, discrete and more complex electronic components). The FMEA for discrete component circuits have traditionally been carried out at a component level against postulated component faults. FMEA for systems containing integrated circuits have been undertaken for postulated faults at a pin level for low levels of integration. FMEA may be carried out at a functional level (e.g. during a concept design) and also later in the development phase in order for design weaknesses to be identified and design amendments to be introduced at an early stage. The FMEA of the final design will usually be used as part of the design and safety justification of the I&C systems.

FMEA techniques are routinely used to generate evidence that is used within the design and safety justification. Regulatory requirements imply that such techniques shall be used to demonstrate that systems will function as intended under all predicted operational conditions. In the UK, FMEA techniques are also used in conjunction with fault tree analysis techniques as part of the quantitative demonstration of reliability.

FMEA techniques are used to support the design process, for example, to identify system behaviour in the presence of a postulated fault. Knowledge of the behaviour in the presence of a fault can be used to introduce design features, i.e. self-monitoring, that reveal the fault. FMEA techniques are used to support the evaluation of the reliability and availability, for example to establish the fraction of ‘safe’ and ‘dangerous’ failures of the system. FMEA techniques are used to support the safety demonstration of components and systems, for example showing that faults and the subsequent failure of the system can be tolerated and its outcome does not cause the plant to move out of its safety envelope. FMEA techniques are used to support the demonstration that a system meets Regulatory expectations, for example in respect of revealing faults and system behaviour on failure.

7.4 United States

US NRC Inspection Procedure 43004 (10/03/2007) provides guidance to NRC inspectors on the inspection of commercial-grade dedication programmes. This guidance states that a dedicating entity should require the performance of a FMEA to identify the credible failure mechanisms of the item to be dedicated. The guidance states that a FMEA should address the specific application under consideration.

FMEA of plant-specific applications are sometimes required for generically approved safety system platforms. In one example, the US NRC determined that a plant-specific FMEA is required for any implementation of a computer-based safety system platform. (US NRC Safety Evaluation Report dated February 7, 2013, ADAMS Accession No. ML13022A011)