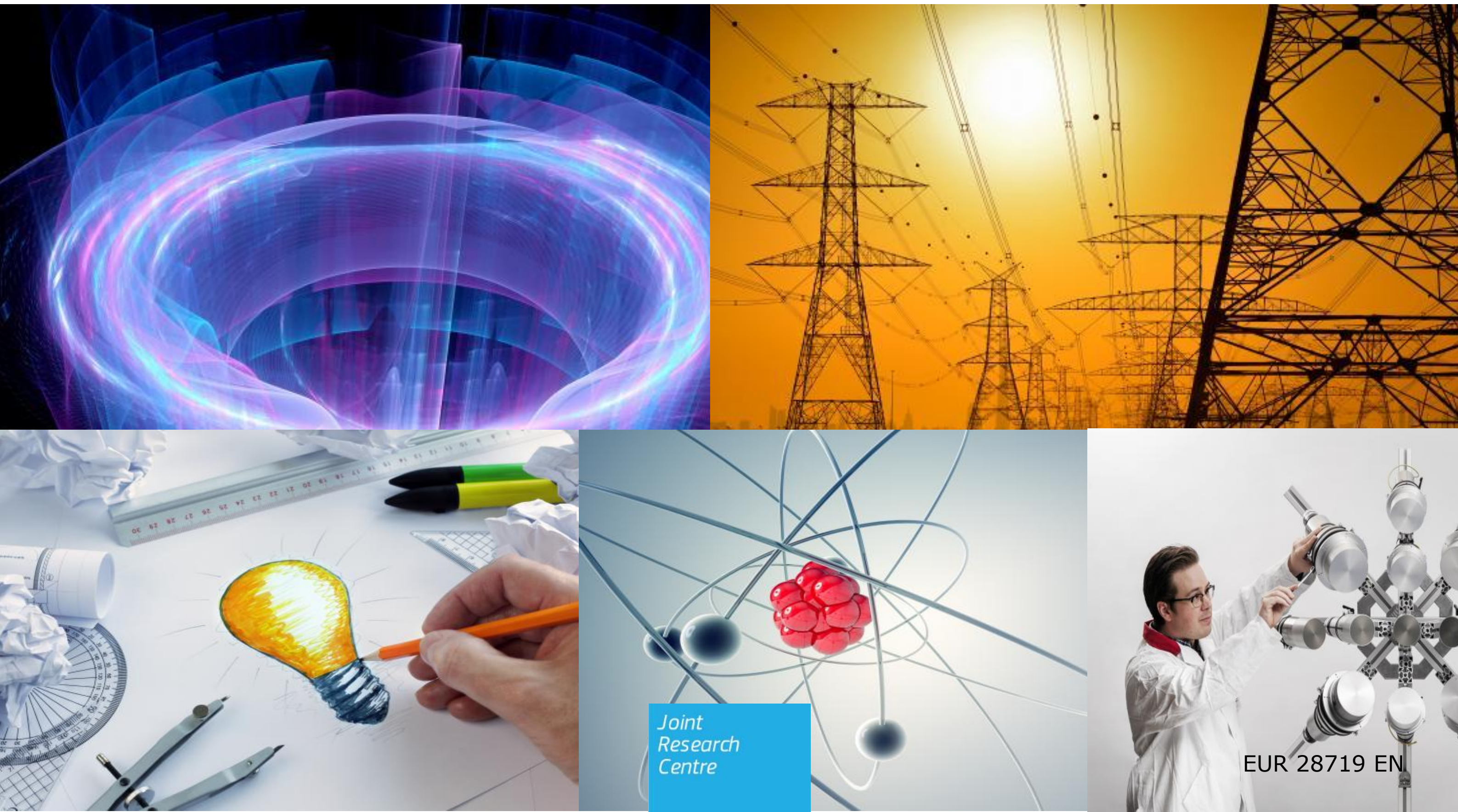
European Commission

# JRC TECHNICAL REPORTS

# Summary report of events related to design deficiency

Miodrag Stručić

2017



Joint Research Centre

EUR 28719 EN

This publication is a technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

**Contact information**
Name: Miodrag Stručić
Address: Westerduinweg 3, 1755 LE Petten, the Netherlands
Email: miodrag.strucic@ec.europa.eu
Tel.: +31 22456-5448

**JRC Science Hub**
https://ec.europa.eu/jrc

JRC107453

EUR 28719 EN

| PDF | ISBN 978-92-79-71480-1 | ISSN 1831-9424 | doi: 10.2760/006508 |
|---|---|---|---|

Luxembourg: Publications Office of the European Union, 2017



How to cite this report: Miodrag Stručić, *Summary Report of Events related to Design Deficiency*, EUR 28719 EN, Publications Office of the European Union, Luxemburg, 2017, ISBN 978-92-79-71480-1, doi 10.2760/006508, PUBSY No 107453

# Contents

## Acknowledgements

This report has been prepared by the European Clearinghouse on nuclear power plant operating experience feedback at the European Commission's Joint Research Centre (JRC) with the support of the Institut de Radioprotection et de Sûreté Nucléaire (IRSN), France, and Gesellschaft für Anlagen und Reaktorsicherheit mbH (GRS), Germany.

The author would like to thank Miguel Peinador Veira, Benoit Zerger and Diego Escrig Forano for their contribution in the comprehensive study behind this summary report.



***Author***

Miodrag Stručić

## Abstract

This summary report presents the results of a comprehensive study described in the topical study 'Events related to design deficiency'. The study has been conducted to review the recent worldwide operating experience and to draw from it the lessons learned and recommendations to improve the safety performance of nuclear power plants (NPPs). The work covers all kinds of commercial power reactors currently or recently in operation and all off-power modes of operation. The sources of operating experience for the study are the international reporting system for operating experience (IRS) database, the licensee event reports (LERs) of the United States Nuclear Regulatory Commission (US NRC), the French operational experience database Sapide and the German operational experience database VERA. Thousands of event reports were screened to select those more relevant for the objectives of the study. This resulted in a list of 774 event reports.

After different approaches applied in examining pre-defined categories and families of events, it was concluded that six common major issues could be defined to present the areas of concern in the best way. Accordingly, the 29 recommendations from this study are distributed under these topics: unanalysed conditions, instrumentation and control, robustness of design, ageing, internal and external hazards, and quality of documentation.

These recommendations are expected to help the licensees and the regulatory authorities to recognise latent weaknesses dating from the design phases of the NPPs, before the start of NPP operation, and perform adequate measures to prevent the occurrence of events similar to those described in this report. The report can also be used as a good reference for new NPP construction projects.

# 1. Introduction

The European network on operating experience feedback (OEF) for NPPs, or 'European Clearinghouse', was established by European nuclear safety regulators to promote the regional sharing of operating experience, the dissemination of lessons learned from NPP operation, and the understanding of the role of OEF systems in the safe and reliable operation of existing and new-build NPPs. The centralised office of the European Clearinghouse is operated by the Joint Research Centre (JRC) of the European Commission.

One of the technical tasks of the European Clearinghouse consists in performing in-depth analysis of families of events ('topical studies') in order to identify the main recurring causes, contributing factors and lessons learned and to disseminate and promote recommendations aiming to reduce the reoccurrence of similar events in the future.

Requested by European Clearinghouse members, this topical study provides an analysis of the event reports in which design deficiency played the main or contributing role in the development of an event. This report was prepared in cooperation with the Institut de Radioprotection et de Sûreté Nucléaire (IRSN), France, and Gesellschaft für Anlagen und Reaktorsicherheit mbH (GRS), Germany. These two institutions analysed information from their respective databases, i.e. France and Germany, while the JRC processed information from the IRS and US NRC licensee event reports. At the latest stage, JRC staff combined all results in the present study.

This report summarises the main findings and recommendations from the topical study *Events related to design deficiency* [1]. The main objective of the topical study is to draw the generic and case-specific lessons learned from the events contained in the databases, and to provide recommendations to the members of the European Clearinghouse on operational experience for NPPs. More specifically, the study aims to reveal latent weaknesses dating from the design phases, i.e. before the start of NPP operation. These weaknesses could be discovered not only during the operation of the plant when they trigger actual events, but, in many cases, they could also be discovered through other related activities (e.g. regular plant assessments) or even unrelated activities (e.g. walkdowns). Moreover, the study should provide useful lessons to those who are in a position to initiate adequate changes in their area of work to improve the safety of nuclear power plants.

Relevant references for assessing design deficiencies can be found in two International Atomic Energy Agency (IAEA) documents. The first, IAEA SSR-2/1, *Safety of nuclear power plants: Design* [2] gives requirements for the design of nuclear power plants. The other one, IAEA GS-G-3.5, *The management system for nuclear installations* [3], provides recommendations and guidance for developing the design process or processes.

As in most studies of this type, the discovered deficiencies are, in fact, causes or potential causes of undesirable events. It should be emphasised that regardless of its importance for a particular event, each cause is worth treating adequately in accordance with its potential risk for nuclear safety. Sometimes it is not easy to estimate the risk and that is why we should treat them equally, regardless of whether they produced or just contributed to the event.

In 2011, the European Clearinghouse issued the topical report *Analysis of nuclear power plants modifications events* [4]. It covered NPP events related to modifications to structures, systems and components, to process software, to operational limits and conditions, to operating procedures and to management systems. The present study does not overlap excessively with this report. The main difference between these two studies should be in events of concern. Design deficiencies in the 'modifications' study mostly come from a deficiency in the modification process, and deficiencies in the 'design deficiency' study come from NPP design phases which often resulted in design-change requirements.

# 2. Methodology

## 2.1. Description of the databases

This study used data from four NPP reported events databases.

The IRS is an international system jointly operated by the International Atomic Energy Agency (IAEA) and the Nuclear Energy Agency of the Organisation for Economic Cooperation and Development (OECD/NEA). The fundamental objective of the IRS is to contribute to improving the safety of commercial NPPs which are operated worldwide. The IRS database contains more than 4000 event reports with detailed descriptions and analyses of the events' causes that may be relevant to other plants.

United States commercial nuclear reactor licensees are required to report certain events according to US NRC Regulation 10CFR50.73. These LERs are available to the public on the NRC's website, which contains LERs from 1980 onwards. More than 50 000 events are currently available. This database is searchable using a variety of criteria, including name, date, reactor type and vendor or text search in the title, abstract or full report.

The IRSN database, called Sapide, is managed by the IRSN department in charge of analysing the OEF. The database contains events in French NPPs reported since 1973, but it has been improved over the years. A significant improvement was implemented in 1996 and the information contained in the database has been more detailed since that upgrade.

The German database VERA is a GRS database which contains reportable events occurring at German NPPs. This database, used for the systematic evaluation of operating experience, includes over 6 300 events, which have been reported in detail since 1975. In this study, all reported events that occurred at German NPPs between 1992 and 2011 were examined.

## 2.2. Screening of events

In order to retrieve the relevant events, it was necessary to carry out a screening of the information sources used for the study. Each database used is structured in a different way and features different searching capabilities. For these reasons, the screening criteria were database-specific. Since not all events are fully applicable for the study, all selected reports were examined and only those with the most valuable lessons were selected for in-depth analysis.

IRS events from 1990 or later were retrieved and a total of 581 events were obtained. All these were then checked to determine whether they met the scope of the study. After screening, a total of 297 event reports were retained for detailed analysis.

In the US NRC LER database, identification of events relevant for the study resulted in 341 events for the whole database time period. After further analysis, it was decided to use events from 1990, and 156 events were found interesting for study.

Similarly, from the French database Sapide, 103 events were selected for study, and from the German database VERA, the number of events selected for further study was 218.

In total, 774 events were chosen for in-depth analysis.

## 2.3. Classification of events

All event reports selected for full analysis were classified into categories and families according to a number of criteria. To complete the categorisation of the events, specific sets of families were defined and specific assumptions used. That way, the events with similar characteristics were grouped.

This grouping of the events was done with a double aim: understanding the phenomenology of the events observed and helping in the extraction of valuable lessons and recommendations. Furthermore, after careful analysis of events reported in all four databases, it was found that lessons are more efficiently presented when events are grouped as discussed in the lessons learned section of the main report.

'General plant design characteristic/principle affected' is the one of the main categories defined based on IAEA SSR-2/1, *Safety of nuclear power plants: Design* [2]. This document gives general plant requirements for design basis, design for safe operation over the lifetime of the plant, human factors, other design considerations and safety analysis.

The 'design phase concerned' category originates from IAEA GS-G-3.5, *The management system for nuclear installations* [3] which gives recommendations and guidance for requirements set mainly in reference [2]. Examples of families in this category are 'design initiation', 'specification of scope and planning', 'work control and planning of design activities', 'configuration management', etc.

Other important categories include: 'specific plant systems affected'; 'affected components'; 'detection mode'; 'impact on safety' and 'corrective measures'.

## 2.4. Analysis

The categorisation of events reveals a phenomenological description of the event types' distribution. It is a simple way to identify dominant events. Events grouped around a common topic frequently reveal a general issue. These events, depending on impact on safety, can provide the most valuable lesson to stakeholders.

Thus, for example, grouping events under the most dominant families of the 'general plant design characteristic/principle affected' category can point to the design requirements that are too often breached or challenged.

Dominant families in the 'design phase concerned' category may extract critical phases in the designing process that should be better managed.

The 'specific plant systems affected' category groups events around systems that may need more attention. Accordingly, the 'affected components' category's dominant families point to critical components.

The most common modes of detection from the 'detection mode' category show how the failure is discovered and their trend could have an important influence on some NPPs' strategies for discovering deficiencies.

The 'impact on safety' category simply shows whether the events resulted in degraded safety features, which is helpful in understanding the risk of a specific event, and could also give a general perception of risk in the concrete area of concern — in this case, design deficiency.

To reveal the areas where most of the corrective actions are aimed, the 'corrective measures' category is used. The measures could also influence the NPP's strategy for areas (families) which are more affected.

Finally, one additional technique was employed to extract the most important topics of concern in the area of NPPs' design deficiencies. For this technique, the problem statement of each event was defined. All the problem statements were examined and distributed to the appropriate groups, which became a set of common major issues which were analysed separately. General recommendations based on events under that topic were defined.

# 3. Results of analysis and recommendations

Due to the high dispersion of results between four databases and seven main categories, as well as some obvious deficiencies which could not be satisfactorily categorised in the pre-defined categories, it was concluded that six common major issues categories properly summarise most of the concerns related to design. Accordingly, the 29 recommendations from this study are distributed under these six issues categories:

- Unanalysed condition;
- Instrumentation and control (I&C);
- Robustness of design;
- Ageing;
- Internal and external hazards; and
- Quality of documentation.

The distribution of these issues is presented as a graph in Figure 1: Common major issues.

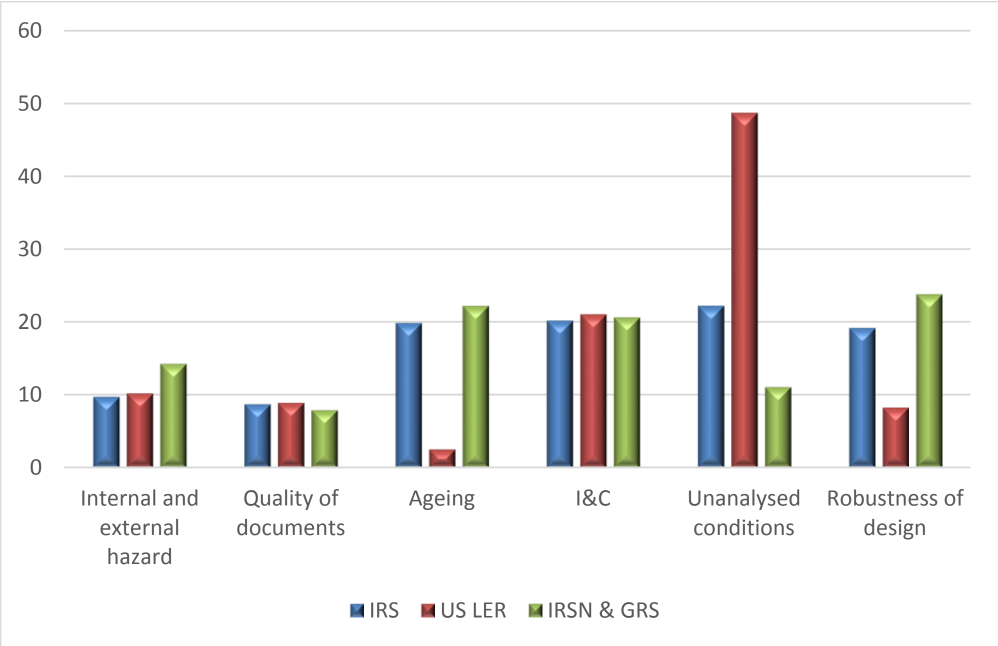



**Figure 1**: Common major issues [1]

It can be noted that almost half of United States LERs are grouped under the 'unanalysed condition' issue. The reason for this could lie in different reporting criteria, which may be more rigorous regarding unanalysed or not-predicted conditions, but also because of a stronger review process in the United States (more than half are detected by review process). The other three databases show a fairly similar distribution

## 3.1. Unanalysed conditions

The group of events under the 'unanalysed conditions' category presents a very dominant common major issue. Not recognising potential safety problems was directly related to this topic, since many different kinds of analyses and controls missed the opportunity to detect them. Most events in this category have in common that the design failed to appropriately identify either the initiators or contributors of design-basis accidents, or the failure modes of safety systems during accident conditions.

[1] The values are presented as a percentage of the total number of selected events in each database.

The following recommendations have been derived from the events reviewed in the study, and highlight some of the safety analysis issues experienced by nuclear power plants in the past 20-30 years.

- Operational limits and conditions should be well defined, and operating procedures should take unambiguous steps to prevent the operation of the reactor beyond the specified limits.
- The design of safety-related gate valves should properly address the risk of pressure locking and thermal binding during all scenarios, including test conditions.
- During the cold shutdown mode of operation, it is essential that the hydrogen concentration in the coolant and in the void spaces in the primary circuit be monitored systematically and that potential areas of hydrogen accumulation be ventilated permanently.
- Ventilation systems' design should adequately account for all emergency situations. An unanticipated interaction may occur when an exhaust system is not well balanced with a supply system, or would not trip if the diesel generator sequencer were actuated. All possible design-basis accident scenarios should be evaluated in order to verify if ventilation systems would work as designed.
- The thermal study of premises containing equipment important to safety should be comprehensive, in order to prove that ambient temperature increase will not render safety equipment inoperable when ventilation is not available.
- The design of the component cooling water system should take into account temperature transients experienced during accident conditions by portions of the system located inside the containment. All possible scenarios in accordance with emergency procedures should be analysed. Special attention should be paid to component cooling water system pump restart after isolation during some design-basis accidents.
- The design of oil-cooled large power transformers should include protective measures to contain oil spills. All possible leak paths should be analysed.
- Safe shutdown analyses should be reviewed to verify the capability to isolate the reactor coolant pump seal leak offline, in case of loss of cooling to the seals after fire or Station black-out events.

## 3.2. Instrumentation and control

The group under this category presents the events where instrumentation and control deficiencies were detected and the roots of problems are closely connected with design phases.

According to IAEA requirements [2] regarding design-basis accidents (requirement 19): 'design basis accidents shall be used to define the design bases, including performance criteria, for safety systems and for other items important to safety that are necessary to control design basis accident conditions, with the objective of returning the plant to a safe state and mitigating the consequences of any accident'. Unfortunately, some events showed that some I&C components important in case of design-basis accidents are vulnerable under those conditions.

The following recommendations can help in the prevention of these I&C vulnerabilities.

- Regular simulator usage (e.g. training, plant changes) should be used to identify potential I&C deficiencies in safety-related systems. In particular, different combinations of events paired with maintenance and single failures should be taken into account.
- Operating experience should be collected during the construction of new plants, in particular regarding design deficiencies in I&C systems.

- It should be ensured that I&C equipment specifications include all necessary electrical parameters, so that these parameters may be confirmed during the equipment qualification.
- Special attention should be paid to protection circuit applications. Tests should be carried out during commissioning to ensure that short-circuit protections do not falsely respond on the activation of safety-significant motors.
- The I&C of operational functions should be independent of safety functions I&C.
- Instrumentation piping should be carefully designed and tested to prevent pressure build-up or any other phenomena that could affect instrument response, erroneous readings and subsequent spurious actuation of protections of safety systems.
- The results of Probabilistic safety assessment studies should be considered as a valuable source to detect inadvertent dependencies among systems propagated through poorly designed I&C systems, for instance instrument air and essential power systems.
- The design of I&C used to measure water levels during mid-loop and draindown operations should be carefully reviewed to detect any common cause of failure mode in its design.

## 3.3. Robustness of design

Some of the reported events contain examples of equipment or components with a design lacking the necessary robustness, rendering safety systems vulnerable to minor deviations from normal operating conditions. Presented events could have been prevented if the design process had been performed in accordance with standards and proven practice. Requirement 18, 'Engineering design rules', of IAEA SSR-2/1 [2] simply states: 'Methods to ensure a robust design shall be applied, and proven engineering practices shall be adhered to in the design of a nuclear power plant to ensure that the fundamental safety functions are achieved for all operational states and for all accident conditions'[2].

None of the issues in this category (debris in containment during a LOCA, pipes and conduits fretting, power switches too sensitive to vibrations and valves stuck by dirt/corrosion) have been sufficiently considered by the relevant engineering discipline.

- Licensees and/or regulators should perform studies on possible reactor containment building sump filters clogging during the recirculation phase following a Loss of coolant accident. Subject to the results of these studies, modifications or replacement of the recirculation filters could be considered.
- Design of piping and tubing at particular locations like the feeder cabinet in heavy water reactors should take into account the risk of damage to piping/tubing/cables caused by fretting.
- Safety equipment power switch design should be sufficiently robust, so as not to be spuriously triggered by mechanical loads (e.g. vibrations).
- A preventive and surveillance maintenance programme should be set up to detect valves stuck by corrosion or dirt in those applications where the valves are not frequently operated. A complete list of such valves should be established and checks should be carried out on those installed in the systems important to safety.

## 3.4. Ageing

The group under this category presents the events related to inappropriate ageing management defined in design phases. Requirement 31 of IAEA SSR-2/1 [2] states: 'The design for a nuclear power plant shall take due account of ageing and wear out effects in

---

[2] 'Safety of nuclear power plants: Design', IAEA SSR-2/1, January 2012, IAEA, Vienna, 2012, p. 22.

all operational states for which a component is credited, including testing, maintenance, maintenance outages, plant states during a postulated initiating event and plant states following a postulated initiating event'[3].

Corrosion in primary circuits, engineering safety features pump vibrations, subsidence of piping, different types of corrosion, pollution effects and many other issues addressed under these topics caused, contributed or could cause the serious failures of safety systems.

- The design of piping in auxiliary systems physically connected to the reactor coolant system should account for a number of thermal-hydraulic phenomena observed in existing reactors that may lead to piping corrosion or fatigue damage, with the potential for a loss-of-coolant accident.
- Enhanced monitoring methods should be used to detect the development of deposits at the steam generators' upper support plates.
- The design of safety equipment subject to environmental conditions should accurately take into account all requirements resulting from loading cases, and the qualification tests should be sufficiently representative of real conditions during an accident.

## 3.5. Internal and external hazards

Requirement 17 of IAEA SSR-2/1 [2] states that 'all foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered for determination of the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant[4]…'

- The safety case for seismic risk should be carefully reviewed to assess the consequences of fire and floods induced by earthquakes.
- The cooling water intake structure should be reviewed, where applicable, to detect potential vulnerabilities related to frazil ice accumulation.
- Where applicable, the design of the plant should consider extreme cold weather as an external event with the potential to cause common cause failures modes related to safety. The impact of a loss of offsite power (caused by the cold weather) on electrical heating systems used to protect equipment from freezing conditions should be addressed.
- The effects of an outdoor fire on the ventilation system of safety-relevant buildings should be thoroughly assessed. The possible ingress of smoke into the respective buildings and the resulting potentially safety-related consequences should be considered in particular.

## 3.6. Quality of documentation

A very important phase in the design process is the detailed design and production of design documentation. IAEA GS-G-3.5, *The management system for nuclear installations* [3] states that 'calculations, analyses and studies should be documented in sufficient detail and should be controlled in such a manner that subsequent users of the design, in the various stages of the lifetime of the installation, can understand the design and make informed decisions. Inputs, assumptions, modelling, test and development work and

[3] 'Safety of nuclear power plants: Design', IAEA No SSR-2/1, January 2012, IAEA, Vienna, 2012, p. 29.
[4] 'Safety of nuclear power plants: Design', IAEA No SSR-2/1, January 2012, IAEA, Vienna, 2012, p. 20.

results, safe operating parameters and envelopes, key acceptance criteria and parameters for commissioning tests, for example, should all be documented.

Design activities should ensure that specified requirements are correctly translated into design outputs, such as: Basic design of the installation; Design computer codes; Design specifications; and Functional specifications[5].'

Since modern computer technologies offer many new solutions and possibilities to interlink all NPP drawings, records and all other dependent documents, and provide smart interconnections and fast access through user-friendly interfaces (e.g. plant information models), it is expected that this topic will have less issues compared to the past.

- Design documentation should translate the requirement to maintain safety systems such as emergency core cooling, decay heat removal, and containment spray systems full of water into drawings, specifications, procedures, and instructions. The design should identify potential gas source accumulation locations and symptoms of gas leakage from potential sources.

- The identification of equipment in drawings should accurately match the actual labelling displayed on the equipment.

## 3.7. Additional findings

Because of the dominance of the 'actual consequences' family of events and since the IRS collects events from NPPs from all over the world, this was considered important for further examination. A trend graph was created (Figure 2: Trend graph of detection modes of design deficiency in IRS). The graph shows that the number of events with actual consequences is increasing and gives a signal that some other detection approaches should be further employed or improved. The sudden drop in the number of events that are detected by surveillance and reviews may indicate obsolete or inadequate deficiency detection methods.

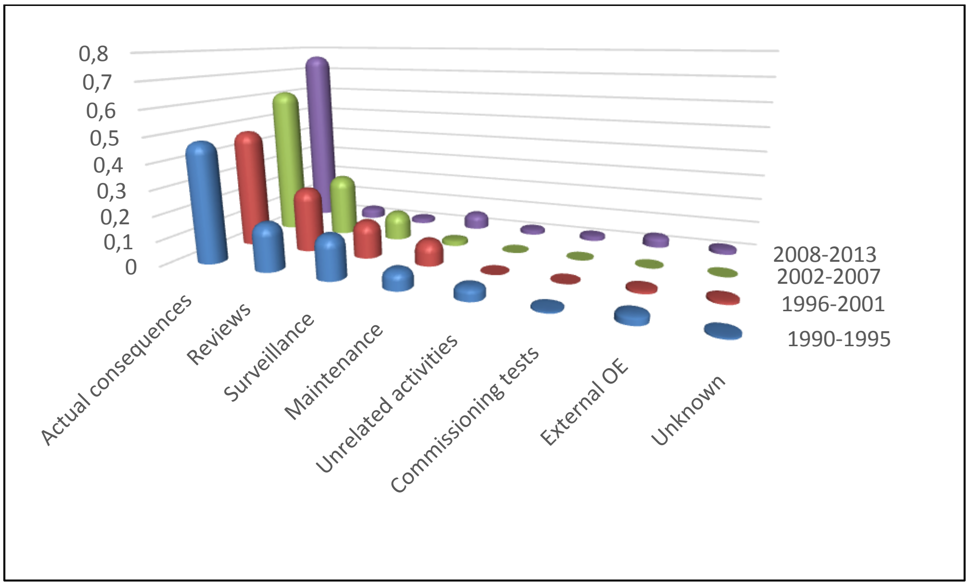



**Figure 2:** Trend graph of detection modes of design deficiency in IRS[6]

---

5 'The management system for nuclear installations', IAEA No GS-G-3.5, September 2009, IAEA, Vienna, 2009, p. 64.

6 Values in the graph present the relative portion of each parameter during each observed period.

The other databases show a much higher proportion of deficiencies identified through reviews, maintenance, etc. Thus, the United States, France and Germany are considered to have a more adequate approach to detecting reported deficiencies.

# 4. Conclusions

This topical study was conducted to review the worldwide operating experience from events where design deficiencies have been addressed and to extract valuable lessons and recommendations to improve the safety performance of nuclear plants. The work covered all kinds of commercial power reactors in operation.

The sources of operating experience for the study were the IRS database, LERs from the US NRC, the French operational experience database Sapide and the German operational experience database VERA. Thousands of event reports were screened to select those most relevant to the objectives of the study. This resulted in a list of 774 event reports, listed in the annexes, which was judged to be sufficient to derive sound and representative lessons learned and recommendations.

A detailed examination of selected events was conducted, classifying them according to different defined criteria, in order to gain good insight into the nature of the design deficiency problems. The main part of the review was, however, the qualitative assessment of the events, with emphasis on lessons learned and recommendations that have been derived from them.

The analysis of how design deficiencies are detected by licensees identified that, for the IRS database, design issues are most often revealed only by an event with actual consequences, rather than, as would be desirable, by engineering reviews, inspections or surveillance activities. Furthermore, the trend for this type of detection mode is to increase over time. Therefore, design reviews and other methods to detect design deficiencies might need to be encouraged in some countries. Unlike the IRS database, the other databases show a much higher proportion of deficiencies identified through reviews, maintenance, etc.

It was concluded that six common major issues categories could be defined to properly summarise most of the concerns related to design. Accordingly, the 29 recommendations from this study are distributed under these six topics:

- Unanalysed conditions;
- Instrumentation and control;
- Robustness of design;
- Ageing;
- Internal and external hazards; and
- Quality of documentation.

Considering that many of the events reviewed in the topical study occurred a long time ago, licensees were probably already informed about them through different OEF communication channels and implemented appropriate actions to prevent reoccurrence on their sites. Therefore, in the first place, recommendations from described reports should be used to check if those applicable have been adequately implemented in affected NPPs. If not, further assessment should be performed and adequate priority for necessary changes should be given to each of them.

Recommendations from the topical study presented in this summary report are more general and they are expected to help licensees and regulatory authorities to perform adequate measures to prevent the occurrence of events similar to those described in this report. It would also be highly desirable to discuss all recommendations with senior managers of NPPs.

Nevertheless, it should be emphasised that design process management flaws are evident in all the events on which the main recommendations are based. Therefore, a successful management should establish high level of safety and strong culture of safety. To establish effective safety strategy necessary for preventing accidents and mitigating the consequences, management should integrate good design and engineering features by providing adequate safety margins, diversity and redundancy [5].

# References


[1] Stručić, M., *European Clearinghouse topical report: Events related to design deficiency*, European Commission 2016, JRC 105232.

[2] 'Safety of nuclear power plants: Design', *International Atomic Energy Agency (IAEA) Specific Safety Requirements* No SSR-2/1, January 2012, IAEA, Vienna, 2012.

[3] 'The management system for nuclear installations', *International Atomic Energy Agency (IAEA) Safety Guide* No GS-G-3.5, September 2009, IAEA, Vienna, 2009.

[4] Zerger, B., *European Clearinghouse topical report: Analysis of nuclear power plants modifications events*, European Commission 2011.

[5] 'Fundamental Safety Principles', *International Atomic Energy Agency (IAEA) Safety Standard* No SF-1, November 2006, IAEA, Vienna, 2006.

KJ-NA-28719-EN-N

## JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.



doi 10.2760/006508

ISBN 978-92-79-71480-1