PROCEEDINGS OF THE CSNI WGOE/SEGHOF WORKSHOP ON MODIFICATIONS AT NUCLEAR POWER PLANTS - OPERATING EXPERIENCE, SAFETY SIGNIFICANCE AND THE ROLE OF HUMAN FACTORS AND ORGANISATION

Organised by the OECD/NEA in cooperation with the Institut de Radioprotection et de Sûreté Nucléaire (IRSN)

Held at the OECD Headquarters, Château de la Muette, Paris, 6-8 October 2003

The complete version is only available in pdf format.
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996) and the Slovak Republic (14 December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full Member. NEA membership today consists of 28 OECD Member countries: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its Member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

© OECD 2004

Permission to reproduce a portion of this work for non-commercial purposes or classroom use should be obtained through the Centre français d'exploitation du droit de copie (CCF), 20, rue des Grands-Augustins, 75006 Paris, France, Tel. (33-1) 44 07 47 70, Fax (33-1) 46 34 67 19, for every country except the United States. In the United States permission should be obtained through the Copyright Clearance Center, Customer Service, (508)750-8400, 222 Rosewood Drive, Danvers, MA 01923, USA, or CCC Online: http://www.copyright.com/. All other applications for permission to reproduce or translate all or part of this book should be made to OECD Publications, 2, rue André-Pascal, 75775 Paris Cedex 16, France.
COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS

The Committee on the Safety of Nuclear Installations (CSNI) of the OECD Nuclear Energy Agency (NEA) is an international committee made up of senior scientists and engineers. It was set up in 1973 to develop, and co-ordinate the activities of the Nuclear Energy Agency concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international co-operation in nuclear safety among the OECD Member countries.

The CSNI constitutes a forum for the exchange of technical information and for collaboration between organisations, which can contribute, from their respective backgrounds in research, development, engineering or regulation, to these activities and to the definition of the programme of work. It also reviews the state of knowledge on selected topics on nuclear safety technology and safety assessment, including operating experience. It initiates and conducts programmes identified by these reviews and assessments in order to overcome discrepancies, develop improvements and reach international consensus on technical issues of common interest. It promotes the co-ordination of work in different Member countries including the establishment of co-operative research projects and assists in the feedback of the results to participating organisations. Full use is also made of traditional methods of co-operation, such as information exchanges, establishment of working groups, and organisation of conferences and specialist meetings.

The greater part of the CSNI's current programme is concerned with the technology of water reactors. The principal areas covered are operating experience and the human factor, reactor coolant system behaviour, various aspects of reactor component integrity, the phenomenology of radioactive releases in reactor accidents and their confinement, containment performance, risk assessment, and severe accidents. The Committee also studies the safety of the nuclear fuel cycle, conducts periodic surveys of the reactor safety research programmes and operates an international mechanism for exchanging reports on safety related nuclear power plant accidents.

In implementing its programme, the CSNI establishes co-operative mechanisms with NEA's Committee on Nuclear Regulatory Activities (CNRA), responsible for the activities of the Agency concerning the regulation, licensing and inspection of nuclear installations with regard to safety. It also cooperates with NEA's Committee on Radiation Protection and Public Health and NEA's Radioactive Waste Management Committee on matters of common interest.

The opinions expressed and the arguments employed in this document are the responsibility of the authors and do not necessarily represent those of the OECD.

Requests for additional copies of this report should be addressed to:

Nuclear Safety Division
OECD Nuclear Energy Agency
Le Seine St-Germain
12 blvd. des Iles
92130 Issy-les-Moulineaux
France
TABLE OF CONTENTS

EXECUTIVE SUMMARY ............................................................................................................. 5
CONCLUSIONS AND RECOMMENDATIONS ............................................................................... 7
PROGRAMME ............................................................................................................................. 11
PAPERS AND PRESENTATIONS ................................................................................................. 17
  • Welcome and Opening ........................................................................................................ 19
  • General plenary session (Monday October 6th) ................................................................. 19
  • Parallel Stream 1: Human Factor (October 7th) ............................................................. 141
  • Parallel Stream 2: Operating Experience (October 7th) ................................................. 141
  • Session 1: Human Factors, Methods and Tools (October 8th) ....................................... 215
  • Session 2: Operating Experience, Role of the Regulator (October 8th) ....................... 215

ANNEX 1 - SUMMARY OF SELECTED WORKSHOP DISCUSSIONS ...................................... 235
ANNEX 2 - LISTE OF PARTICIPANTS ......................................................................................... 257
ANNEX 3 - CALL FOR PAPERS ............................................................................................... 265
EXECUTIVE SUMMARY

Operating experience repeatedly shows that changes and modifications at nuclear power plants (NPPs) may lead to safety significant events. At the same time, modifications are necessary to ensure a safe and economic functioning of the NPPs. To ensure the continuing safety of NPPs it is important that processes for change and modification are given proper attention both by the NPPs and the regulators. The operability, maintainability and testability of every modification should be thoroughly assessed from different points of view to ensure that no safety problems are introduced.

The OECD/NEA Committee on Safety of Nuclear Installations (CSNI) addressed the issue of modifications at a "Workshop on Modifications at Nuclear Power Plants – Operating Experience, Safety Significance and Role of Human Factors" held at the OECD headquarters in Paris on October 6 to 8, 2003. This workshop was undertaken as a joint effort of the Working Group on Operating Experience (WGOE) and the Special Experts Group on Human and Organisational Factors (SEGHOF). During the workshop, WGOE focused on the theme of "Minor Modifications and their Safety Significance", while SEGHOF focused on the topic "Human and Organisational Factors in NPP Modifications".

The workshop was attended by 55 experts from the industry, regulators and technical support organizations in 15 countries. The workshop programme consisted of plenary and parallel sessions for presentations and discussions. One important part of the workshop was to discuss findings of the WGOE and SEGHOF surveys of utility and regulatory experience from modifications at the NPPs.

Modifications at the NPPs are controlled by written procedures. The process varies depending on the type of the modification. Large modifications generally lead to fewer problems, because the projects are given both a great deal of attention and resources. In contrast, minor modifications seem to represent a generic challenge because they are less likely to be recognised as safety significant. Similar kinds of challenges may be born during plant maintenance, when changes in the design or materials may be made without anyone recognising that the maintenance work has modified the function of plant equipment.

A modification process in which possible safety influences are assessed early can improve nuclear safety and, at the same time, reduce the overall costs. Screening of intended changes can be used to estimate design and analysis efforts required in the modification process. It should be observed that systems complexity sometimes may have unexpected impacts. Screening criteria should address both the safety significance of the systems and components modified and the impact of the changes on tasks performed by operators and maintainers. Major modification projects should always involve a comprehensive review, which includes both technical and human contributions to plant operability and maintainability.

It is important to create awareness and understanding of the potential safety impact of large and small modifications in NPPs. This awareness may be improved by collecting and disseminating information about modification-related events. There is evidence that good results can be achieved by integrating technical and human factors considerations in the safety assessment process for plant modifications. Regulators have an important role in ensuring that modification processes are acceptable and documented, and that the processes are followed. International agencies have a role in informing regulators and industry about the importance of using appropriate processes when modifications are planned, reviewed, designed, and implemented.
CONCLUSIONS AND RECOMMENDATIONS

The workshop

The OECD/NEA/CSNI addressed the issue of modifications at a "Workshop on Modifications at Nuclear Power Plants – Operating Experience, Safety Significance and Role of Human Factors". This workshop was undertaken as a joint effort of the Working Group on Operating Experience (WGOE) and the Special Experts Group on Human and Organisational Factors (SEGHOF). The workshop was preceded by a questionnaire to SEGHOF members to collect information on experience with integrating human factors into design changes and to WGOE members to collect information about modification processes and events with emphasis on minor modifications. The results from the questionnaires were shared with and discussed among workshop participants.

During the workshop WGOE placed an emphasis on the theme "Minor Modifications and their Safety Significance" and SEGHOF focused on the topic "Human and Organisational Factors in NPP Modifications". Organisational changes at the NPPs were excluded from the scope of the workshop, since they are covered by other SEGHOF activities. The main findings from the workshop presentations and discussions are summarised below.

The workshop was attended by 55 experts from the industry, regulators and technical support organizations in 15 countries. The workshop programme consisted of plenary and parallel sessions. The specific themes of WGOE and SEGHOF were discussed in parallel sessions, where the joint plenary sessions focused more generally on the modification process. A total of 16 presentations were given by the participants.

Modifications at NPPs

NPPs undergo many technical safety significant changes throughout their life-cycle. Modifications to plant equipment or documents may be generated by regulatory issues or by internally driven initiatives, such as replacing ageing equipment. These modifications can impact on the operation and/or maintenance of the installation. As a consequence they may present new challenges to plant personnel who are trained and experienced in using existing equipment and documents.

One good practice at the NPPs is to create a long term development plan for upcoming modifications to be made. Such plans have the benefit that better co-ordination between various changes and modifications can be achieved. A plan also makes it easier to ensure that the modifications introduced are consistent with the overall human-machine interaction philosophy of the plant. When the development plans are updated in the normal planning cycles of the NPP, it is also easier to identify the resources needed over time to avoid delays and other difficulties during the modification projects.

Modifications at the NPPs are typically controlled by written procedures, which divide the modification process into distinct phases. These phases may include writing a proposal for a modification; an assessment of the proposal; a decision to stop or continue; preparation of a detailed plan for implementing the modification; and finally the implementation phases: design, construction, procurement, installation, testing and documentation. Safety reviews with a varying scope and degree of detail are carried out after the completion of each major step in the process. A common practice is to do regular
quality audits of selected modification projects. It is a good practise to perform a general review of the modifications implemented at least on a 10 year interval. A well documented modification process and properly documented individual modification projects are important preconditions for the audits and reviews to be performed.

Operating experience

Operating experience has revealed that modifications may cause different problems if they are not properly attended to. For example minor changes in components, materials or spare parts may cause safety significant events. Such modifications were not initially recognised as being safety significant, but they nonetheless may present a challenge to the safety of NPPs. An investigation of events exhibiting minor modifications show that safety impacts were typically not expected or it was not even recognised that some action actually constituted a modification. Such situations may lead to unexpected functional behaviour in interaction with other components or systems in certain circumstances. Another example of problems connected to modifications is when they are introduced without a proper consideration of operability and maintainability aspects. In such cases human errors in operation or maintenance may have a negative influence on plant safety and availability.

According to experience presented at the workshop it seems that large modification projects bring in fewer problems, because they are generally well resourced, assessed and analysed by the utilities and the regulator. This finding illustrates the need to raise awareness that deficiencies in the modification process may contribute to events regardless of the size of the modification project or object.

Minor or non-identified modifications

An assessment of events related to minor or non-identified modifications (MiNIMs) demonstrate that they can reduce the availability and reliability of equipment that is important for safety. They may even generate common cause failures influencing multiple layers of safety barriers. For example, when standby components or systems are affected, such modifications may cause latent and common cause failures. Such failures may remain undetected, as operating experience shows, especially when the anomalies are difficult to identify by pre-operational or periodic tests. It is even possible that faults unknowingly are spread throughout the whole NPP by some common coupling mechanism. Such mechanisms are e.g. wrong lubricants or widely used spare parts.

Presentations and discussions at the workshop demonstrated clearly that the MiNIMs can be a topic of concern. Related events and incidents that have occurred in all the countries were presented at the workshop. The common difficulty seems to be connected to awareness and understanding that even minor modifications may be safety significant. Some events demonstrate that modifications are sometimes introduced unknowingly, when a new version of a system, component or part contains changes as compared to earlier versions. When this is the case, it is very important to subject changes such as in function, material, size and form to a proper identification, analysis and testing.

Human factors considerations

The presentations and discussions at the workshop clearly demonstrated the importance of integrating human factors considerations into the modification process. If human factors issues are not given a proper attention during the design and implementation of a modification, the consequence may be human errors when installing, testing, operating and maintaining of the changed systems or components. There are several safety significant events that can be attributed to deficiencies in the human-system interface of modified systems. During the workshop, several examples of good practices for incorporating human factors into the modification process were discussed.
Participants at the workshop agreed that all modifications do not need the same degree of a human factors analysis work. It is therefore important to screen all modifications regarding their potential to affect human performance. A good practice is to have all modifications screened, analysed and approved by a qualified multi-disciplinary team. The modification process should be documented clearly to ensure consistency and completeness in the modification projects.

The transfer from operating an existing system to the modified one should always be given proper attention. This includes the preparation of necessary documents such as installation instructions and testing programmes, operating procedures, and maintenance manuals as well as a proper training of personnel. Sometimes it may be necessary to prepare dedicated procedures and instructions when the existing and modified parts of the systems are to be operated in parallel.

An observation from the workshop is that plant operation and maintenance should follow all modifications closely and, in consultation with the safety department, initiate necessary assessments and reviews. The technical support at the NPPs is typically not in a good position to initiate such reviews, but they can utilise their own expertise to participate in the design and review teams.

Structuring the modification process

The NPP operators have full responsibility for the safety of the plants and correspondingly for the safety of all modifications. This responsibility for safety remains when the NPP contracts out a major part of the design and implementation of the modification. The division of responsibilities between the NPP and the contractor may vary depending on the project and the competency of the contractor. However, the verification that design requirements are fulfilled and the validation that the system fulfils its functions should always be the task of the NPP.

There was consensus at the workshop that modifications may take different routes depending on their target and scope. In assessing modifications, it is important to establish criteria for those potentially different routes. Discussions at the workshop showed however that it sometimes is difficult to set absolute criteria for all possible variations in scope, human factors impact and safety importance that may have an influence on the modification process. Some interesting practices of performing an analysis of potential risks within a PSA (Probabilistic Safety Assessment) were described at the workshop. Changes and modifications should be subject to a careful screening at an early point in the modification process. Screening should encompass both technical and human factors considerations in order to identify the appropriate form and level of scrutiny in the design and safety assessment process. This may help to minimise the need for costly changes to plant design and analysis in later stages of the modification process.

There are some areas related to modifications, which seem to be important to review in depth. One area is connected to spare parts, where it is important to assess their availability and different versions over a reasonable time frame. Spare parts may, according to several examples in operational experience, sometimes cause problems. One problem is that slight design changes in components and parts may create incompatibility between versions of components and spare parts. Another problem that may occur is that the spare parts have not been properly stored or handled at the NPPs. A remedy to these problems is to address the documentation and functionality of spare parts properly before closing a specific change or modification.

Temporary modifications are another class of modification that require added attention, because they are often not subjected to an in-depth safety analysis due their provisional status and they may become permanent without sufficient assessments. Temporary modifications also have the drawback of forcing operation and maintenance organisations to a loop of several rounds of modifications, which may be difficult to control. The temporary modifications should always be subjected to a technical review and, if
they are somehow safety related, also to a safety review. A good practice is to restrict any temporary modification to a maximum duration of, e.g. 6 months.

**Regulatory oversight**

It is impossible for the regulator and its technical support organisation to know all the modifications implemented either by the plant operator or by a manufacturer. Regulatory oversight should thus include auditing both the modification process itself and the results obtained. The regulator may require review and approval of larger and safety related modifications. In the periodic safety reviews, a special focus may be put on how modifications have been handled. The main role of the regulator is to ensure that operators have implemented an acceptable modification process and that this process is followed. It would be beneficial if regulators in different countries could create a harmonised view on requirements to be placed on acceptable modification processes.

To ensure a proper assessment of human factors issues in the design and implementation of modifications, it is a good practice to have a specialised experts’ group available for the NPP. Furthermore, it is important that regulators have the proper human factors expertise to assess both the adequacy of modification processes as the adequacy of individual modifications.

It is necessary to address personnel competency especially if it is to be expected that existing skills and knowledge will be replaced due to retirements. These issues should be addressed in a broader context to ensure that important knowledge connected to the plant design basis is not lost when people leave. The loss of knowledge on specifications and requirements for components that have not been properly documented can be critical for modifications later in plant life. Some NPPs have introduced competency surveys and documentation inventories to assess possible needs for actions to ensure that tacit knowledge is captured and documented.

**Further work**

Based on the experience of workshop participants, additional international work is required for addressing modifications at the NPPs. Already the discussions during the workshop brought up important insights, experiences and good practises. One good practise is for example to have all modifications analysed and approved by a qualified team, which is separated from the modification project. Another good practice is to audit modifications at regular intervals to ensure that instructions are followed and that the documentation is updated properly.

Further work should concentrate on creating awareness and understanding of the problems modifications could cause if they are not given a proper attention. Continued safety of the NPPs can be achieved only through a prudent approach to all changes and modifications. On the other hand it is equally important to understand that changes and modifications are an important component in a continuous quest for safety and efficiency. This finding should as applicable be brought into various documents, which are giving guidance on the handling of modifications at the NPPs.

National and international organisations should provide forums for utilities, suppliers and designers, and regulators to exchange experience from the design and implementation of modifications. This information could be used to update present guidance on the modification processes to ensure a safe and economic implementation of modifications at the NPPs. Further work in WGOE and SEGHOF could focus on collecting modifications experience from actual modification projects and from events following modifications to create better guidance for the nuclear utilities and regulators.
OECD Nuclear Energy Agency (NEA)
Committee on the Safety of Nuclear Installations (CSNI)
Working Group on Operating Experience (WGOE)
Special Expert Group on Human and Organizational Factors (SEGHOF)
International Atomic Energy Agency (IAEA)

Workshop on
Modifications at Nuclear Power Plants – Operating Experience, Safety Significance and Role of Human Factors

FINAL PROGRAMME

Hosted by OECD Nuclear Energy Agency (OECD/NEA)
In co-operation with the Institut de Radioprotection et de Sûreté Nucléaire (IRSN)

At OECD Headquarters, Château de la Muette,
Paris, France
6 – 8 October, 2003
Monday, October 6

9h00  † Welcome and Opening Addresses
      **CHAIRMEN: M. D. TASSET AND M. D. WATTRELOS**
      M. K. SHIMOMURA (NEA)
      M. F. NIEHAUS (IAEA)
      M. J.C. NIEL (IRSN, France)

9h50  † Logistics information
      M. P. PYY (NEA)

10h00  † Workshop objectives and related CSNI
      M. D. TASSET (IRSN, France)
      M. D. WATTRELOS (IRSN, France)

10h30  † Break*

11h00  † Organization and process concerning modifications of nuclear plants
      G. JEANTON (EdF/UNIPE, France)

11h30  † Identifying and addressing lessons from plant modernization programs
      J. O'HARA (BNL, USA), J. KRAMER, J. PERSENSKY (NRC, USA)

12h00  † Lunch Break*

14h00  † General Plenary Session

**CHAIRMEN: C. REIERSEN, Y. VAN DEN BERGHE, D. WATTRELOS**

† Evaluation of reported events in German nuclear power plants due to insufficient equipment labelling.
   V. WILD, M. STÜCK, M. MAQUA (GRS, Germany)

† Integration of human factors engineering into a refurbishment a multi unit CANDU station.
   A. KOZAK, (Bruce NPP Canada), J S. MALCOLM (AEC, Canada)

† Guidelines for control room modernization as part of Instrument and control modernization program.
   J. NASER, L. HANES (EPRI, USA), J. O'HARA (BNL, USA), R. FINK, D. HILL (MPR), G. MORRIS (DOE)

15h30  † Break*
A micro-macro human factors approach to improve team working after an incident
J.F. VAUTIER, M. TOSELLO, I. BARNABE, S. GARANDEL, V. PAULUS, B. PAPIN (CEA, France)

A classification of validation criteria for new operational design concept in nuclear process control
A.B. SKJERVE, G. SKRAANING (HRP, Norway)

End of the First day
Tuesday, October 7

Plenary Session:

| 9h00 | Outlines of and the briefing for the break-out sessions |

This day is divided into 2 parallel streams with an opening presentation as follows:

Parallel Stream 1: HUMAN FACTOR

| 9h30 | Presentation: Analysis of maintenance history for identification and prevention human CCFs originating from minor modifications and maintenance |
| K. LAAKSO (VTT, Finland) |
| 11h30 | Discussion in groups (incl. a potential break) |
| 12h30 | Lunch break* |

Theme: How to improve the consideration of potential impact of modification as soon as possible?

| 14h30 | Presentation: Taking into account of socio-organizational and human aspects into upgrade packages (technical or not) |
| L. QUENTIN, D. NIGER (EdF/UNIPE, France) |
| 16h30 | Synthesis of discussions |
| 17h30 | End |
| 20h00 | Social event in Paris, hosted by IRSN: a diner in “Atelier Renault” restaurant, 53, avenue Champs-Elysées - Paris |

* Lunch break
Parallel Stream 2: OPERATING EXPERIENCE

**CHAIRMEN: H. WERDINE, M. MAQUA**

*Theme: Is it possible to set a reference basis to define which modifications, considered as minor, have to be taken into account because of their potential impact on safety?*

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
</table>
| 9h30   | The Swiss modification process in NPP Regulatory Regime – Regulator/Operator process and experience related to events with safety impact  
        | H. DEUTSCHMANN (HSK, Switzerland)                                                        |
| 11h30  | General synthesis of discussions                                                            |
| 12h30  | Lunch Break*                                                                              |

**CHAIRMEN: K. LAAKSO, D. WATTRELOS**

*Theme: How to improve the national modification processes?*

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
</table>
| 14h30  | Presentation: Temporary modifications and minor changes: a threat for the safety of NPP’s  
        | H. WERDINE (IAEA)                                                                          |
| 16h30  | General synthesis of discussions                                                            |
| 17h30  | End                                                                                        |

20h00  | Social event in Paris, hosted by IRSN: a diner in “Atelier Renault” restaurant, 53, avenue Champs-Elysées - Paris |
Wednesday, October 8

The morning sessions are divided into 2 streams:

Session 1: HUMAN FACTORS, METHODS & TOOLS

Theme: Which tools and methods can be used for integrating human factor in the design process of a modification?

CHAIRMAN: T. TAYLOR, H. McROBBIE

9h00  Presentation: Providing ergonomics guidance to engineers when designing Human-Machine interfaces for nuclear plants installations

D. GREGSON, E. Marshall, A. GAIT, N. HICKLING (Synergy Consultant Ltd, UK)

Discussion in groups (incl. a potential break)

11h30  Synthesis of discussions

Session 2: OPERATING EXPERIENCE, ROLE OF THE REGULATOR

Theme: How can the regulator and his TSO help to improve detection of shortcomings due to modifications?

CHAIRMEN: H. DEUTSCHMANN, M. MAQUA

9h00  Presentation: Regulatory aspects of plant’s modifications

M. JUAN (DGSNR, France)

Discussion in groups (incl. a potential break)

11h30  Synthesis of discussions

12h30  Lunch Break*

14h30  CONCLUSIONS

Syntheses of the breakout discussions of the two streams in the plenary session

Perspectives, actions ...

Conclusions

16h30  End of the workshop

See also the tentative schedule of sessions on the next page

* Notice that the refurbishment of the La Muette site may cause some problems for the availability of services, which has been taken into account in the duration of the breaks. For instance, it is evident that the OECD cafeteria will be closed. The restaurants in the La Muette area are an alternative.
PAPERS AND PRESENTATIONS
Welcome and Opening Addresses
M. K. SHIMOMURA (NEA) .......................................................... 21
M. F. NIEHAUS (IAEA) .............................................................. 23

Organization and process concerning modifications of nuclear plants .......... 25
G. JEANTON (EdF/UNIPE, France)

Identifying and addressing lessons from plant modernization program .......... 45
J. O'HARA (BNL, USA), J. KRAMER, J. PERSENSKY (NRC, USA)

General Plenary Session
Evaluation of reported events in German nuclear power plants due to insufficient equipment labelling .......................................................... 63
V. WILD, M. STÜCK, M. MAQUA (GRS, Germany)

Integration of human factors engineering into a refurbishment a multi unit CANDU station ................................................................. 79
A. KOZAK, (Bruce NPP Canada), J S. MALCOLM (AEC, Canada)

Guidelines for control room modernization as part of Instrument and control modernization program ......................................................... 85
J. NASER, L. HANES (EPRI, USA), J. O'HARA (BNL, USA), R. FINK, D. HILL (MPR), G. MORRIS (DOE)

A micro-macro human factors approach to improve team working after an incident ................................................................. 107
J.F. VAUTIER, M. TOSELLO, I. BARNABE, S. GARANDEL, V. PAULUS, B. PAPIN (CEA, France)

A classification of validation criteria for new operational design concept in nuclear process control ......................................................... 117
A.B. SKJERVE, G. SKRAANING (HRP, Norway)
Good morning, Ladies and Gentlemen,

It is a great pleasure for me to welcome you to the NEA CSNI WGOE/SEGHOF Workshop on “Modifications at Nuclear Power Plants - Operating Experience, Safety Significance and the Role of Human Factors & Organisation” in co-operation with the International Atomic Energy Agency (IAEA) and the Institut de radioprotection et de sûreté nucléaire (IRSN) at the beautiful Château la Muette here in Paris. First of all, I would like to express my appreciation to the IAEA and IRSN for their co-operation and to you all for your participation.

The Committee on the Safety of Nuclear Installations (CSNI), which is the one of the NEA Standing Technical Committees, contributes to maintaining a high level of safety performance and safety competence by identifying emerging safety issues and establishing international research projects. The work is to be conducted by experts from member countries through Working Groups, Special Expert Groups, and Task Groups such as the Working Group on Operating Experience (WGOE) and the Special Expert Group on Human and Organisational Factors (SEGHOF).

This joint Workshop were proposed by the CSNI task forces: the WGOE “Minor Modifications and their Safety Significance” and the SEGHOF “Human and Organisational Factors in NPP Modifications”. The general objective of this Workshop is to exchange and dissemination information about the safety aspects of NPP modification, and to share and discuss good practices for regulators and licensees.

We are now in changing economic and social circumstances such as “Competition in electric markets, commonly referred to as economic deregulation”. The new technology is also available to replace ageing equipment and to make modifications. In this context, “Plant Modifications” are an important theme where aiming at the life-extension of operating Nuclear Power Plants. However, operating experience shows that modifications may lead to safety significant events. At the same time, modifications are necessary to ensure the economic and safe functioning of the NPPs. There are differences in approaches to regulating and managing plant modifications in different countries. I have heard that the Workshop will discuss examples of different types of modification process, their key elements and - both regulatory and licensee - guidelines dealing with modifications in the member countries.

This Workshop is covering several important topics in the programme, for instance, “Why and how human and organisational factors need to be considered in relation to modification process?”, “To be identified or proven good practices to deal with modifications in regulation and in safety management”. The special topic related to the important work of the WGOE will be also discussed as “Minor or Non-identified modifications may not be initially recognised, or communication about changes may be insufficient.

I am sure that the programme promises useful results which will assist member countries in managing and regulating modifications more effectively and efficiently.
Before closing my remarks, I would like to emphasise the importance of collaboration with the IAEA and competence organisations such as the IRSN to maximise the results of the Workshop. I would like to thank again the IAEA and the IRSN for co-sponsoring. Their representatives, Mr. Brockman and Mr. Niel will address you next.

Ladies and Gentlemen, I am looking forward to this interesting Workshop, to thought provoking presentations, to lively and fruitful discussions, and useful results.

Thank you very much for your attention.
Good morning Ladies and Gentlemen.

It is a great pleasure for me to welcome you on behalf of the IAEA to this Workshop.

I would like to apologize for the fact that our new DIR for the Division of Nuclear Installation Safety, Mr. Ken Brockman, is unfortunately not able to attend himself. He was looking forward to attend this meeting, but on Friday he was asked by the Director General to stay in Vienna for some urgent tasks this week.

Thus on short notice I was asked to address you here to underline that we consider the topic of the workshop to be of high importance also for the IAEA. It is a pleasure for me to do so. As the IAEA representative on CSNI I have followed the discussions leading to this workshop since its initiation. We are pleased to see that it is now taking place, we are glad that we are able to contribute and we are looking forward to the results.

The workshop is a joint effort between SEGHOF and WGOE. As you might know the IAEA is co-operating with NEA in both of these groups: The IRS for NPPs has been operated jointly for many years and we are just now in the process of launching the joint operation of FINAS, the Incident Reporting System for Fuel Cycle facilities. We had also many other joint activities, or activities carried out in co-operation such as organizing workshops and drafting technical reports.

We want to emphasize that we would like to continue and, where possible, improve our co-operation with the NEA in the future.

We are thus pleased with this workshop. Our high interest in the topic of “modifications” is demonstrated by the fact, that within our series of safety standards documents we have specifically addressed this issue in a safety guide. I noticed that you have referenced this guide in the list of guidance documents which is included in the background material prepared for this workshop. I will briefly come back to this later.

The topic of human factors is also high on our Agenda though it is not easy to address. Our safety standards refer to them in many places. Also, Article 12 of the Nuclear Safety Convention requests that “the capabilities and limitations of human performance are taken into account throughout the life of a nuclear installation”. Additional guidance on how to address human factors is welcome.

A principal aim is to share and discuss good practices for regulators and licensees. In particular the role of the regulator in the softer aspects of nuclear safety, i.e. human factors, organizational aspects and safety culture needs clarification and higher attention in the future.

It is expected that the results will also aid participants to manage and regulate modifications more effectively in their own countries. But it is our specific interest as an international organization to receive advice as to the technical work we can usefully pursue in the future. We would like to learn from your experience: what are the main issues, what could eventually be achieved, how to proceed, and where to focus our efforts, i.e. the workshop
results will be used to steer international developments in the area of NPP modification safety.

Finally, I would like to come back to our work at the IAEA to revise and prepare safety standards. This part of our programme is receiving high priority. There is a strong international commitment that the new or revised standards should better reflect international best practices.

I have earlier referred to our safety guide on “Modifications to Nuclear Power Plants” published in 2001. It addresses many aspects including the safety significance of modifications and learning from operating experience. Related to human factors, however, the guidance is limited to aspects of quality assurance, testing and related training efforts. It is hoped that this workshop and the resulting future work will provide more detailed guidance on how to include human factor considerations into the design and implementation of modifications. Eventually this guidance will be reflected in future revisions of the standard.

At the present time the IAEA is also preparing a new set of safety standards in the area of “Management Systems” to include quality assurance, human and organizational factors and safety culture. We anticipate that this workshop will also provide insights, which are important in drafting these documents.

Last not least we have several programmes in the area of operational safety, operational safety feedback, safety culture, and safety assessment, including the safety services in each of these areas, which can benefit from the results of this workshop. Some of them will be referred to during the workshop by the participants from the IAEA.

In conclusion I would like to emphasize that we look forward to the results of this workshop. This is with the expectation that it will provide us with guidance on where to focus our efforts in this area in the future, in good, and where possible, in improved co-ordination and co-operation with the NEA/OECD.

Thank you for your attention and I wish you a successful workshop.
ELECTRICITE DE FRANCE
ORGANIZATION AND PROCESS
CONCERNING MODIFICATIONS OF NUCLEAR PLANTS

Gérard JEANTON – Safety Mission
Electricité de France / Unité Nationale de l'Ingénierie du Parc en Exploitation *

* UNIPE is a national engineering unit which implements the decision taken in the national engineering field to increase safety and performance of the plant pool. To provide operating reference base upgrades under optimal conditions, UNIPE offers products and services (modifications implementation, documentation upgrading, fuel management,...) to the nuclear power plants, with preparation, delivery and guidance tailored to the particular situation of each site.
1. **ABSTRACT**

Because of the importance of French nuclear power plants with 58 standardized reactors, "Electricité De France" groups modifications, as much as possible in batches.

A batch of modifications contents:

- modifications which keep or increase safety level of nuclear units (1st group),
- modifications which increase availability or production performance of nuclear plants (2nd group).

In its processes, "Electricité de France" distinguishes modifications concerning important safety equipment (all the modifications of the first group, some modifications of the second group). National units of engineering investigate the development of these modifications.

A particular organization specifies:

- A safety analysis,
- Foreseen qualification or validation tests results,
- Impact on operating documentation,
- Operational feedback of experience (when possible)

Nevertheless some errors are still existing:

- Failure of controlled valves of emergency diesel generators
- Failure of fire-proof valves...

2. **GENERAL PROCESS**

Because of the importance of French nuclear power plants with 58 standardized reactors, general process is based on:

- Decision-making process
  
  An order-giver (committee) decides to initiate a strategic study.

  A strategic phase conducted by a strategic leader takes into account experience feedback, Safety Authority requirements and operations targets. It leads to a technico-economic assessment file.

  A technical operation and maintenance committee, on the basis of the technico-economic assessment file, decides to implement the modifications. It also judges its urgency and its integration process (batch or individual treatment).
The implementation phase begins. It is conducted by an implementation leader (UNIPE). This phase consists of:

- a Study phase intrusted by a national unit of engineering (DIN),
- a programme of integration.

- Constitution of batches and project mode management

"Electricité de France" groups the modifications, as much as possible in batches in order to:

- integrate modifications without affecting physical and documentary consistence,
- take into account nuclear safety reviews and durability of components jointly with 10-yearly inspections,
- minimize the impact on units operability.

A project type management is set up in order to master the implementation technically and financially.

The overall strategy can be broken down into:

- definition of a target: expressions of expectations, needs, dosimetry, mastering costs, outage duration
- implementation on a "pilot unit" and gathering of experience feedback,
- generalization of implementation on other units.

- Documentation

The documentation, the users need to operate, is provided to the plants with the implementation of the modifications:

- Engineering documentation: installation drawings, basic system files, constructor/contractor documents, etc. . . .
- Operating and Maintenance documentation: Operating technical specifications, periodic test documents, basic preventive maintenance programmes, particular rules, etc . . .

- Control tools

The main control tools are:

- A study programme which includes key-points of this phase (diffusion of study-notes, safety Authority information, diffusion of implementation files, end of batch preparation, . . .)
- The implementation programme
- The typical implementation planning with its milestones.
3. MODIFICATIONS CONCERNING IMPORTANT SAFETY EQUIPMENT

Batches content two types of modifications:

- modifications which keep or increase safety level of nuclear units (1st group),
- modifications which increase availability or production performance of nuclear plants (2nd group).

Most of the modifications of the first group and some of those of the second group concern important safety equipment, they are called IPS modifications.

"Electricité de France" distinguishes in its processes modifications concerning important safety equipment.

These modifications:

- need necessarily a national decision
- are entrusted by a national unit of engineering,

"Electricité de France" informs Safety Authority before the implementation sending:

- safety objectives,
- description of the modification,
- description of validation tests.

Safety Authority makes an evaluation. It can agree or veto the implementation.

A particular organization specifies:

- A safety analysis,
  It consists of:
  - definition of the safety goal,
  - compliance with safety requirement basis,
  - analysis of the implementation conditions in regard of the respect of Operating Technical Specifications,
  - dosimetry impact (if necessary),
  - definition of requalification criteria
  - impact on the users (modifications of practise).
- Foreseen qualification or validation tests results,
  Definition of qualification tests when the modification concern equipment qualified to accident conditions
- Impact on operating documentation,
  Analysis of the impact of the modification on:
• general operating guideline (Operating Technical Specifications, State oriented approach emergency procedures, periodic testing programme)
• normal operation guidelines,
• particular operation guidelines
• preventive maintenance base programmes
• Operational feedback of experience
  The organization requires evaluating:
  • implementation conditions,
  • effectiveness of the modification (when possible),

4. CONCLUSION

"Electricité de France" specifies a particular organization to intrust and implement modifications concerning important safety equipment (cf §3).

The key factors of this organization are:
- anticipation of processing time,
- a clear decision process,
- integrating the experience feedback,
- guidance and assistance of users.

Thanks to this organization, Electricité de France which implements about 350 modifications each year declared:
- 1 significant safety-related event in 1999,
- 1 significant safety-related event and 1 safety-related event in 2000,
- 1 significant safety-related event and 1 safety-related event in 2001,
- 1 significant safety-related event and 2 safety-related events in 2000,
due to modifications.

Two significant safety-related events of modifications which impacted safety are:
- *Modification of CONTROLLED VALVES OF EMERGENCY DIESEL GENERATORS*
  During periodic tests at full power, some diesel generators tripped due to the action of a protection device.
  The result of investigations was that the valve controlling the coolant temperature was defective.
The origin of this defection was a modification implemented to correct malfunctions observed on the originally installed valves. This modification made the valve less reliable.

The cause of the failure was a design defect which was not detected.

Nevertheless the specifications of development had been respected and requalification tests results were successful.

A modification of design of the valves had been necessary to keep them reliable.

- **Modification of FIRE-PROOF VALVES**

  During periodic tests some fire-proof valves didn’t turn off.

  The origin was a modification of design made to upgrade fight against fire.

  Investigations revealed that a spring on electric controls was defective.

  This defection was not detected. Nevertheless the specifications of development had been respected and requalification tests results were successful.

  Investigations also revealed that users didn’t know the modifications of practice due to the new material.

  The implementation leader:

  • built an implementation program to replace defective springs,

  • intensified guidance and assistance of users.
Technical modification management

- General process for the implementation of modifications
  - Classification of modifications
  - General process
  - Batches of modifications
- Concrete examples
  - Controlled valves of emergency diesels generators
  - Fire-proof valves
**General process**

- Decision-making process (strategic processing phase, decision, implementation phase)

- Constitution of batches and the project mode management

- Documentation

- Control tools

**Classification of modifications**

- Two groups of modifications

  » Modifications which concern important safety equipment (IPS)

  » Modifications which don't concern important safety equipment
IFS Modifications

- National decision
- Development entrusted to a national center
- Implementation phase conducted by an implementation leader

Strategic processing phase

- Conducted by a strategic leader
- It takes into account
  - Experience feedback,
  - Safety Authority requirements
  - Operation targets
- It leads to a technico-economic assessment file
**Decision to implement**

- Taken by a Technical Operation & Maintenance Committee on the basis of the technico-economic assessment file
- The Committee includes representatives of the National Engineering entity, of Nuclear Power Plants and of Corporate Branches of the Nuclear Power Division
- It may veto the modification for technical or cost reasons.
- It judges its urgency and its integration process (batches or individual treatment)

**Implementation phase: Studies and implementation files**

- The study phase includes several steps: diffusion of study notes, Safety Authorities information notes and the Implementation Files
- The Implementation File gathers all the documents necessary for modification integration on the unit
- The study phase is miles-stoned by key points (end of study, end of batch preparation and before generalization key points)
- A fine-tuning scheduling of the modification is prepared during this phase
**IFS Modifications**

- A particular organization specifies
  - A safety analysis,
  - Qualification for qualified equipment,
  - Foreseen qualification or validation tests results,
  - Impact on operating documentation,
  - Operational feedback of experience

---

**Batches Objectives and Interest**

- The need to integrate modifications without affecting physical and documentary consistence has led to modifications being grouped into batches
- They limit to the strict minimum the "progressive" arrival of modifications on a nuclear unit
- The implementation of a batch jointly with a 10-yearly inspection outage makes it possible to take into account the nuclear safety review and the durability of the components
- This makes it possible to show an overall strategy with regards to the Safety Authority
**Batches content**

- Batches content
  - Modifications which keep or increase safety level (modifications IFS)
  - Modifications which increase availability or production performance

**Individual treatment**

- In the individual topics we find:
  - Urgent topics without consequences on the process
  - Topics belonging to specific fields such as industrial data processing, hoisting equipment, etc.
**Project setting up**

- A "project" type management is setting up in order to master the implementation of batches and the associated individual topics
- The overall project strategy can be broken down into:
  - Defining a target: expression of expectations, needs, dosimetry, mastering costs, outage duration,
  - Implementing on a "pilot unit" and drawing experience feedback from it
  - Generalising implementation on next units

**Documentation**

- In coherence with the implementation of the modifications, all of the documentation is provided to the plant:
  - Engineering documentation: installation drawings, basic system files, constructors/contractors documents, etc...
  - Operating & Maintenance documentation: Operating technical specifications, periodic test documents, basic preventive maintenance programmes, particular rules, etc...
## Implementation control tools

- The long-range planning engineering programme lists all the activities entrusted to DIN
- The implementation programme, established by UNIPE, programmes each modification on all units
- The UNIPE/DIN Plant technical scheduling group prepares the integration of the batch at the plant
- The typical implementation programme with its milestones (hold points)

## Process description

<table>
<thead>
<tr>
<th>Time scale</th>
<th>Steps of the Process</th>
<th>Persons/Entities Involved</th>
</tr>
</thead>
<tbody>
<tr>
<td>C0</td>
<td>Strategic processing</td>
<td>Strategic leader</td>
</tr>
<tr>
<td>(C0+2 to 4 months)</td>
<td>decision</td>
<td>Branch Energy</td>
</tr>
<tr>
<td>(C0+4 to 6 months)</td>
<td>Writing of set of specifications</td>
<td>Implementation leader</td>
</tr>
<tr>
<td>(C0+4 to 6 months)</td>
<td>Contractual form (proposal)</td>
<td>Project management</td>
</tr>
<tr>
<td>D0 – 6 months</td>
<td>Studies – Establishment of DI</td>
<td>Project management</td>
</tr>
<tr>
<td>D0</td>
<td>« Pilot Unit » implementation</td>
<td>Project management</td>
</tr>
<tr>
<td></td>
<td>Experience feedback</td>
<td>Implementation leader</td>
</tr>
<tr>
<td>(D0 + 6 to 10 months)</td>
<td>Generalisation</td>
<td>DPN</td>
</tr>
<tr>
<td></td>
<td>Modification report</td>
<td>Implementation leader</td>
</tr>
</tbody>
</table>
Controlled valves of emergency diesel generators (1/3)

- During tests at full power some diesel generators tripped due to the action of a protection device.

- The result of investigations revealed that the valve controlling the coolant temperature was defective.

Controlled valves of emergency diesel generators (2/3)

- The origin was a modification made to correct malfunctions observed on the originally installed valves.

- Validation tests results were successful but the modification made the valves less reliable.
Controlled valves of emergency diesel generators (3/3)

- The cause of the failure was a design defect which was not detected during validation tests.

Fire-proof valves (1/3)

- During periodic tests some fire-proof valves didn’t turn off.
- The origin was a modification made to upgrade fight against fire.
Fire-proof valves (2/3)

- Investigations revealed that:
  
  » A spring of electric controls was defective

  » Users didn’t know modifications of practise due to new materials

Fire-proof valves (3/3)

- The implementation leader:
  
  » Built an implementation program to replace defective springs

  » Intensified guidance and assistance of users
Conclusion (1/2)

- a particular organization to intrust and implement modifications concerning important safety equipment
- The key factors of this organization are:
  - anticipation of processing time
  - A clear decision process
  - Integrating the experience feedback
  - Guidance and assistance of users

Conclusion (2/2)

- Thanks to this organization, Electricité de France which implements about 350 modifications each year declared:
  - 1 significant safety-related event in 1999,
  - 1 significant safety-related event and 1 safety-related event in 2000,
  - 1 significant safety-related event and 1 safety-related event in 2001,
  - 1 significant safety-related event and 2 safety-related events in 2000, due to modifications.
Identifying and Addressing Lessons Learned from Plant Modification Programs

John O'Hara
Brookhaven National Laboratory
and
Joel Kramer & J Persensky
U. S. Nuclear Regulatory Commission

NEA/CSNI Workshop on Modifications at Nuclear Power Plants
Paris, France
6-9 October 2003

Topics

- Introduction
- Lessons Learned
- Addressing Lessons Learned
- Conclusions
Introduction

Utilities are Modifying Plant Systems and Control Rooms

- Need for equipment replacement due to high maintenance cost or lack of vendor support for existing equipment
- Enhancement of plant performance and reliability
  - power uprates
  - digital instrumentation and control systems
- Enhancement of personnel performance and reliability
  - improved human-system interfaces (HSIs) and procedures
- License renewal
- Extent of modifications can range significantly
  - replacement "in-kind" of a single components
  - multiple, "independent," small-scale modifications
  - extensive plant modifications
Impact on Human Factors
Aspects of the Plant

- Broad impact on organization/management, operations, maintenance, and engineering
- Changes to personnel roles, tasks, training, and qualifications
- Changes to HSIs
  - new HSIs are introduced using advanced digital technologies
  - hybrid HSIs result - a mixture of analog and digital technology

NRC Research on Modifications

- We have been studying plant modification and modernization programs to identify safety significant human performance impacts on facility personnel
  - nuclear plants and process control facilities in other industries
- In addition to human performance impacts, other consistent observations emerged
- Summarized in 10 lessons learned divided into two categories
  - Impact on Individual and Team Performance
  - Organizational and Programmatic Considerations
- Lesson have implications for both plant safety and production missions
- Learning the lessons and how to address them can ensure that the benefits of plant modifications are achieved
Lessons Learned

Overview of Lessons Learned

- Impact on Individual and Team Performance
  1. Impact of modifications on personnel performance is not always obvious
  2. Plant personnel come to favor new technology, but may not at first
  3. Even new technology can be poorly designed from a human factors standpoint
  4. New technology has unanticipated consequences
  5. Personnel do not use HSIs in the way designers expect

- Organizational and Programmatic Considerations
  6. Knowledge gaps early in a modification project can be problematic
  7. Involvement of plant personnel increases over time and is usually more than what's expected
  8. End-point vision is often not achieved.
  9. Computer-based systems may change staffing, training, and procedure requirements
  10. Coordination of plant modification with training and operational requirements is difficult
Impact on Performance

1. Impact of modifications on personnel performance is not always obvious.
   - New tasks
     - an action that was not previously performed by personnel such as when an action formerly performed by automation is allocated to the operators
   - Modified tasks
     - a change to the way actions were previously performed, such as through the introduction of new task steps
     - introduction of new HSIs for performing the action
   - Modified task demands
     - e.g., the amount of time available or the overall performance environment
   - Combinations of all of the above

Impact on Performance

2. Plant personnel come to favor new technology, but may not at first.
   - Greater change can lead to greater resistance
   - Issue of acceptance
   - Crews initially prefer older technology when under high workload
   - Over time most would not want to return to old technology
   - Personnel involvement, training, and familiarization are keys
Impact on Performance

3. Even new technology can be poorly designed from a human factors standpoint.
   - Examples
     - Data Overload
       - Too much data and too many alarms
       - Some tasks are more difficult because of information organization
     - Interface Management Demands
       - Greater cognitive workload and time required to work with and manage the HSIs
       - Not enough display area to look at information simultaneously (too few monitors)
       - Serial access to HSIs, navigation requirements, and HSI flexibility
     - Computer Complexity
       - Computer-based systems add to overall complexity
       - Difficulty understanding what the computer system is doing - not sufficiently observable and the communication facilities are inadequate
       - Computerized operator support systems make mistakes

Impact on Performance

4. New technology has unanticipated consequences.
   - Teamwork affected by changes to the work environment
   - Computerization can change the roles and responsibilities of crewmembers
     - HSIs perform tasks or task elements accomplished by crew members
     - the basis for crew interaction can be altered
   - Computer-based control room designs can create obstacles to effective teamwork
     - limiting awareness of other crewmember actions
     - Inhibiting communicating
     - reducing opportunities for collaboration
Impact on Performance

5. Personnel do not use HSIs in the way designers expect.
   • Paradox of Design vs. Use
   • Designers expectations
     – provide lots of information in a flexible workstation with limited viewing area
     – operators will use flexibility to configure HSIs to best meet task demands
   • Operators do not use HSIs in ways designers expect
     – workload management strategy
     – create workarounds that correct for design limitations
     – constrain design flexibility

Organizational and Programmatic Considerations

6. Knowledge gaps early in a modification project can be problematic.
   • There is a learning curve for utilities embarking on large modification programs with new technology
   • The gap between utility and vendor personnel can lead to misunderstandings and changing utility expectations
   • End-point vision change over the course of the project
     – end-point vision is the design the utility wishes to have once modifications are completed
Organizational and Programmatic Considerations

7. Involvement of plant personnel increases over time and is usually more than what is expected.
   - Utilities often expect "turn-key" operation with little need to involve significant personnel time
   - Eventually utilities need to assign personnel to the project to ensure the final design meets their needs

Organizational and Programmatic Considerations

8. End-point vision is often not achieved.
   - Modification projects often extend over many years
   - For budgetary and other reasons, it is often not possible to achieve the endpoint vision
   - It is important to have a migration plan that provides acceptable "stop points" if needed
Organizational and Programmatic Considerations

9. Computer-based systems may change staffing, training, and procedure requirements.
   • Changing systems
   • Changing personnel roles and responsibilities
   • More to know, so less training on any one topic
   • Inadequate training on HSI use (functions and interaction strategies) is frequent personnel complaint

10. Coordination of plant modifications with training and operational requirements is difficult.
    • Modifications are made while the demands of training and operations are ongoing
    • It is difficult to make modifications to the simulator to reflect plant changes while meeting ongoing training commitments at the same time
    • Especially difficult for multiunit plants
Addressing the Lessons Learned

General Considerations

• To achieve safety and operational benefits of plant modifications user needs must be addressed

• A clear process has to be in place to identify impacts on personnel performance and to engage in appropriate human factors engineering activities to address them

• Human factors engineering program is a key
  – user-centered design
  – participatory ergonomics
Characteristics of Effective Human Factors Engineering Programs

- Human factors program should be follow a top-down model
  - functions to tasks to detailed design
  - ensures all performance shaping factors and human reliability considered

- Human factors should be considered a life-cycle process
  - concept planning
  - design
  - verification and validation
  - performance monitoring after modifications are in place

- A graded approach should be used
  - need to consider what aspects of a human factors program are needed to ensure the human performance considerations have been appropriately addressed

NRC Regulatory Approach

- US NRC design review process reflects these characteristics

- Review process is designed to correlate with and track the design process

- Flexible, graded, risk-informed application
  - sets clear expectations for the use of human factors engineering as part of the project
  - is not prescriptive about how expectations are met
  - accommodates individual design processes of vendors and utilities
  - grade the review to focus on safety important aspects of the modification
Key Documents

- NUREG-0800 - Standard Review Plan*, Chapter 18, Human Factors Engineering
- NUREG-0711, Rev. 2 - Human Factors Engineering Program Review Model
- NUREG-0700, Rev. 2 - Human-System Interface Design Review Guidelines

HFE Review Model

<table>
<thead>
<tr>
<th>Planning and Analysis</th>
<th>Design</th>
<th>Verification and Validation</th>
<th>Implementation and Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>HFE Program Management</td>
<td></td>
<td>Human-System Interface Design</td>
<td>Design Implementation</td>
</tr>
<tr>
<td>Operating Experience</td>
<td></td>
<td>Procedure Development</td>
<td>Performance Monitoring</td>
</tr>
<tr>
<td>Function Analysis &amp;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allocation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Task Analysis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Staffing &amp; Qualification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Human Reliability</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analysis</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Addressing Lessons

- Impact of modifications on personnel performance is not always obvious
  - function and task analysis
  - tests and evaluation
  - verification and validation

- Plant personnel come to favor new technology, but may not at first
  - user involvement in design
  - adequate and timely training

- Even new technology can be poorly designed from a human factors standpoint
  - HSI design using guidelines and tests and evaluations
  - verification and validation

Addressing Lessons

- New technology has unanticipated consequences
  - user involvement
  - HSI tests and evaluations
  - verification and validation
  - performance monitoring

- Personnel do not use HSIs in the way designers expect
  - user involvement
  - HSI guidelines and tests and evaluations

- Knowledge gaps early in a modification project can be problematic
  - HFE program planning and endpoint vision definition
Addressing Lessons

- Changing utility involvement
  - HFE program management and planning
- End-point vision is often not achieved
  - HFE program management and planning
  - migration strategy planning
- Computer-based systems change staffing, training, and procedure requirements
  - HFE program inputs to modifications of these areas
  - plan for changes in training program scope
- Coordination of plant modification with training and operational requirements is difficult
  - HFE program management and planning
  - define unique training approaches and opportunities
  - engineering simulation and part-task trainers

Conclusions
Conclusions

• Modification programs have provided valuable lessons learned
• These lessons illustrate the importance of addressing personnel needs
• Lessons have been used to better define human factors program requirements
• Incorporation of improved HFE programs by design and regulatory organizations will help ensure that safety and operational benefits of modification programs are achieved

Appendix
Characterizing Modifications
### General HSI Trends

<table>
<thead>
<tr>
<th></th>
<th>Centralization of HSI into compact workstations and overview displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Large expansive control rooms</td>
<td>Interaction through computer systems</td>
</tr>
<tr>
<td>Crew interaction with plant systems and components</td>
<td>Virtual HSI</td>
</tr>
<tr>
<td>Physical HSI</td>
<td>Serial access to HSI through view ports (keyholes)</td>
</tr>
<tr>
<td>Parallel access to HSI</td>
<td>Flexible HSI</td>
</tr>
<tr>
<td>Fixed HSI</td>
<td>Expanding functionality of HSI</td>
</tr>
<tr>
<td>Limited functionality</td>
<td></td>
</tr>
</tbody>
</table>

### General Trends

![Image of control room]
HSI Trends

- Alarm reduction processing and management
- More data and information integration
- Greater automation
- Soft controls
- Computerized procedures
- Limited use of computerized operator support systems (COSSs)

HSIs Trends
Procedure Trends

Trends in Functionality

- Integration of HSI Resources
- Processing
- Decision Support
- Flexibility
- Portability
- Automation
Reported events in German nuclear power plants due to insufficient equipment labelling

V. Wild
Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH
Paris, October 06, 2003

Situation of the plants

- Long period since initial start-up of German nuclear power plants
- Increasing amount of preventive and corrective maintenance work (parts reach the end of their life time, defects, etc.)
  - Replacement by identical parts or by modernized different parts
  - Immense effort in documentation and labelling as well as in in-depth analysis before an replacement
Approach:

- Evaluation of reported events from German nuclear power plants
- Selection of reported events due to insufficient equipment labelling
- Classification of the selected reported events
- Search for common root causes

Recommendations for German nuclear power plants

Selection of reported events due to insufficient equipment labelling

- Focus was on events due to insufficient equipment labelling
- Several similar events with failures during the replacement we did not select (lacks in quality assurance of the manufacturer, common failures in maintenance work, etc.)
- Additionally: Problems by replacement with new technology
Classification of events

- Modifications by manufacturers unknown to the plant
- Modifications by the plant without adequate documentation
- Maintenance failures due to insufficient quality assurance after replacement
- Maintenance failures due to differences seeming to be unimportant

Additionally:
- Replacement by new different parts

Modifications by manufacturers unknown to the plant

- Changes of spare parts by the manufacturer in the course of time
- Changes seem to be unimportant, therefore no necessity to inform the plant
- Unexpected effects by interaction of the new parts with the plant component
- Example: plug-in module with different length of mass contact pin
Modifications by the licensee without adequate documentation

- Several minor modifications of serial parts by the licensee during construction
- Insufficient documentation of the modifications of the parts in use and the spare parts depending on their possible application
- Example: Modifications of electronic plug-in modules to suit them for special purposes

Maintenance failures due to insufficient quality assurance after replacement

- Simple failures during installation because of unclear labelling of components
- Quality assurance after maintenance also failed because distinctive features are too small
- Example: wrong fuses in two different power supplies because the labelling of the power supply module was missing
Maintenance failures due to differences seeming to be unimportant

- Evaluation showed a lot of differences compared to the documented specification of a system
- Maintenance personnel did not follow existing procedures
- Differences had low safety significance
- Example: wrong screws in safety-related valves

Replacement by new different parts

- Increasing need to exchange parts by modern or total different parts
- Performance of in-depth analysis, regulatory body has to confirm
- Nevertheless some events occurred in operational experience
- Example: Exchange of relays with a too long triggering time

- In future: Ongoing modernisation, for example use of digital instrumentation and control system
**Statistics**

- Rate less than 1% of all events
- 6 German information notices with recommendations for other nuclear power plants
- Existing efforts assure this small rate of events
- Nevertheless there will always be some events due to insufficient equipment labelling

**Lessons learned**

Already known but still important!

- Comprehensive labelling and documentation including exact installation location and application of spare parts
- Communication between licensee and manufacturer about all modifications and the boundary conditions for the application
- Comprehensive functional tests after maintenance work to assess implications of different characteristics
Possible additional problems in future

- Loss of undocumented knowledge by retiring of personnel
- New problems by the use of technology with extended functionality
Evaluation of reported events in German nuclear power plants due to insufficient equipment labelling

1 Introduction

As a result of the long period since initial start-up of German nuclear power plants the amount of preventive and corrective maintenance work has increased and will increase in future. This maintenance work comprises besides other work the preventive replacement of parts of equipment due to reaching end of life time or corrective replacement because of defects. Preventive work can be well prepared and the potential consequences of an application of new equipment can be analyzed. There are two fundamental different ways to replace designated parts. A part can be either replaced by an identical part or by a part of a modernized or different type.

Considering the replacement by identical spare parts no in-depth analysis has to be performed before the replacement. Main requirement for a successful replacement is a comprehensive documentation and labelling of parts and mounting locations. Even though lots of efforts have been performed by German nuclear power plants the operating experience still reveals some deficiencies in practical experience. GRS has analyzed several events reported by German nuclear power plants that gave example of those deficiencies. This paper discusses general findings gained by the evaluation and reports some striking events. The focus of the evaluation comprised all types of components, nevertheless most of the examples are from the area of electrical engineering.

The amount of in-depth analysis performed by the operating organization and independent experts is much higher if parts are replaced by a different type or equipment of a different manufacturer. At first the new part has to provide all functions of the old part. But also the interaction between the affected component, the related system and the new part has to be analyzed. The documentation has to be adapted. Usually, the operating organization performs this analysis following regulatory procedures. Nevertheless failures have occurred during this process and resulted in several reported events. After such an event an in-depth analyses usually identifies unexpected functional behaviour of the new parts interacting with the component and system.
2 Classification of events

The reported events caused by replacement of components are categorized to reveal underlying root causes. Generally, the following categories have been distinguished for our analysis.

- Modifications by manufacturers unknown to the plant
- Modifications by the plant without adequate documentation
- Maintenance failures due to insufficient quality assurance after replacement
- Maintenance failures due to differences seeming to be unimportant

Besides, there are further events which resulted of an unexpected behaviour by the replaced parts of a new or modern type. Events caused by these reasons are discussed in a separate category:

- Replacement by new different parts

The correlation of the events to only one category is not always clearly possible. The root cause analysis of complex events often reveals aspects of more than one of these categories.

Modifications by manufacturers unknown to the plant

Evaluating operating experience of German nuclear power plants GRS analysed several reported events resulting from different design features of so-called identical spare parts. Main reasons for the different design of spare parts are changes by the manufacturer in the course of time. These changes seemed to be not very important in most cases, so that the manufacturer had no necessity to inform the plant about these modifications. Sometimes the modifications are considered to be just a kind of follow-up development than as a new model or type of a part with a new functional design. However by the interaction of the new part with the component some unexpected effects occurred. GRS noticed from the reported events that the licensee was always not aware of the changes or differences in the technical specifications and thus no preventive measures have been established to assure that the compatibility of the new parts is analyzed. The manufacturer failed to inform the plant because he did not know all
applications and operational boundary conditions of the part. So the most important lesson to be learned from this category of events is the importance of communication between operating organisation and manufacturer or supplier and vice versa. The organisations involved are aware about the significance of communication and there are already existing networks to prevent lack of communication.

Apart from this generic aspect GRS also informed German nuclear power plants about the specific problems of significant reported events by its German information notices.

One example is the use of different electronic plug-in modules with different length of the mass contact pin. The mass contact pin of one module type was a little bit shorter than that of the other type. The replacement of a plug-in module by one with a short mass pin led to wrong signals in the reactor protection system due to non-specific voltage ratios. The event resulted in the opening of one safety and relief valve in the affected BWR.

**Modifications by the licensee without adequate documentation**

Especially during the construction of the different German plants several minor modifications of serial parts by the licensee have become necessary. These modifications include for example electronic plug-in modules that have been suited for special purposes. Even though an immense effort concerning documentation was and is practised, there are still examples that reveal deficits in these efforts. The analysis of operational experiences has shown that besides labelling and documentation of the parts in use also the labelling of spare parts depending on their possible application has to be guaranteed. Further on, general lessons about quality assurance and documentation can be learned from the reported events. The concrete aspects of the events from this category are always very specific for the affected plant, so that GRS never wrote a German information notices. Nevertheless the failures which occurred are the focus of generic evaluations and will be continuously evaluated. The main focus hereby will be whether the amount of these events is increasing. One contributing problem may be that more and more personnel already working during plant commissioning will leave and thus a lot of undocumented knowledge could be lost.

**Maintenance failures due to insufficient quality assurance after replacement**
This class comprises simple failures during the installation or the purchase of spare parts. These failures could have been avoided by the existing quality assurance but the distinctive features have been too small to inhibit a mix-up. A good example to illustrate the character of this category occurred in the over-current protection. In a safety related switch gear two different fuses - one of 6 A and the other of 63 A - for two different power supplies have been mixed-up. The amperage was only written on the fuses but a labelling of the power supply module was missing. The two fuses have been mixed up during maintenance works when both fuses have been removed. The maintenance work is normally finished by a functional test that should be able to reveal such a failure. The recommendation of the related German information notices had two intentions. On the one hand similar deficits should be eliminated by a clear and comprehensive labelling. In consequence this led to a labelling of similar power supplies with the amperage of the fuse. These simple measures make it easier for the maintenance staff to confirm the correct status without any documentation sheet which they have to refer to. On the other hand the recommendations of several information notices aimed to improve the final quality assurance after maintenance work.

**Maintenance failures due to differences seeming to be unimportant**

Especially in the last years GRS observed several events in German nuclear power plants which showed differences of the actual status of a system compared to its documented specification. Several licensees recognized that at some valves wrong screws have been installed for example screws of different strength or material. The safety significance of these events has always been very low and calculations showed that the integrity of the different systems was not in doubt for all cases. Nevertheless these differences revealed that the existing measures of quality assurance were not sufficient. A specific problem seemed to be the parallel work at different components during outages. Thereby the working staff decided to use screws that seem to fit and did not check the existing documentation because it looked as if it would be unnecessary. In-depth analyses due to a German information notice uncovered similar situations and behaviour of the maintenance staff in several plants. The discrepancies in these plants have also been of very low safety significance. The recommendations by GRS aimed to improve the documentation of the affected systems and to modify steps in the maintenance work process. Further on, the amount of the revealed discrepancies also touched the field of safety culture and safety management. Some persons of the maintenance staff may have not been aware of the importance of existing procedures.
Concerning these aspects, these events will be part of further evaluation of operation experience.

Replacement by new different parts

Besides replacement by identical parts there is an increasing need to exchange parts by modern or total different parts. This can be caused by ordering spare parts because the production of one series has ended. If such a replacement is necessary, usually an in-depth analysis to appraise the consequences has to be performed. Besides the licensee and the manufacturer also independent experts and regulatory bodies are involved in such a replacement procedure. Even though an immense effort has to be performed before regulatory body confirms such a replacement in safety relevant systems, some events occurred that revealed failures in the investigations.

One example for these failures is the replacement of some relays in a German BWR. These relays give an alarm if a short circuit appears in the related switch gear. The new relay type that was explicitly recommended by the manufacturer had a too long triggering time and therefore it did not send an alarm to the control room on demand. The failure was not noticed for several years, even though plenty of short circuit triggerings had occurred during this time. An adequate communication between licensee and manufacturer especially about the boundary conditions for the use of the relay could have avoided the event. Further on, the operational experience feedback analysis showed once again the importance of final functional tests after replacement by new equipment.

Most of the reported events described above could have been avoided by these functional tests. In some instances these tests have not been sufficiently comprehensive and thus the hidden failure was not found. But there are also examples that results of the tests have been ignored or misinterpreted.

Modernising of nuclear power plants will become more and more important due to the plant ageing. So not only particular parts but also complete system functions will be replaced by new technologies. One major example is the installation of digital instrumentation and control systems that already has begun in several plants. We already have observed some events that belong to this category of failures. Concerning the ongoing modernisation of the plants we expect an increasing amount of events that result from the interaction of the old and the new technology of the instrumentation and
control system and the extended range of functions of the new digital systems. Furthermore there may appear an increase of reported events because of an insufficient operational experience of these systems up to now. GRS has already written some German information notices about the problems leading to such events. One important recommendation was that the maintenance staff have to be thoroughly advised about the consequences of potential failures and the necessary quality assurance during maintenance of the new technologies.

3 Summary

Generally, the rate of events due to insufficient labelling and the resulting replacement with wrong spare parts is low compared to all reported events of German nuclear power plants. Even taking account some events with root causes not fully revealed, the rate of events is less than one per cent of all reported events. Altogether, GRS has written six German information notices concerning these problems. The amount of information notices makes obvious that there are events with an importance for all German nuclear power plants. Besides the recommendations that referred to the concrete event some lessons of a general character were derived.

Labelling and documentation of spare parts has to be comprehensive. This includes for example the description of the exact installation location and of the application of these parts.

The second lesson learned was the importance of communication between licensee and manufacturer. The plant has to be informed about all modifications of spare parts even if they seem to be negligible. The manufacturer has to be informed about the boundary conditions for the applications of his parts.

The third lesson learned deals with the importance of functional tests after maintenance works. This comprises also the tests after replacement by new equipment in order to asses implications of different characteristics.

Taking a closer look at these recommendations it can be recognized that they are not restricted to the problems categorized above but have general safety significance. A lot of effort has already been performed and will be performed in future to implement these recommendations. However, operation experience will show that there will still occur
some events caused by deficits in the implementation of these recommendations. Additionally, the installation of new technology with extended functionality as well as the loss of knowledge because parts of the personnel reach the retiring age will lead to new different root causes that have to be faced.
Bruce A Restart

Integration of Human Factors Engineering into the Refurbishment of a Multi-Unit CANDU Station

Background

- Bruce A has four 750 MW units which were laid up in 1998
- Units 3 and 4 are being brought back to service
- Approximately 200 modifications have been done to the station
Basis for Program

- Human Factors Engineering Program Plan was prepared specific to Restart
- Key standards for program development
  - NUREG 0711 Human Factors Engineering Program Review Model
  - CNSC regulatory guidelines
    - C-276 Requirements for Human Factors Program Plans
    - C-278 Requirements for Verification and Validation Plans
**HFE Process**

<table>
<thead>
<tr>
<th>HF Class</th>
<th>Criteria</th>
<th>#</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>No impact on tasks</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>Minor</td>
<td>&lt; 5 HSI Elements and Guidelines available</td>
<td>19</td>
<td>Review completed by Design Engineer</td>
</tr>
<tr>
<td>Major</td>
<td>&gt; 5 HSI Elements or Guidelines not available</td>
<td>109</td>
<td>90 – Human Factors specialist input following NUREG-00711 10 element model – effort can be small</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>29 – ‘Major Mtce’ – only impact on mtce – COMS process used – design review with users</td>
</tr>
</tbody>
</table>
Main Control Room Impacts

- Key element of the program was monitoring impact in the control room
  - Control room redesign was not part of Restart scope
  - OPEX shows numerous small changes can have a significant cumulative impact in MCR
- Program monitored panel impacts
- Alarm tone monitoring was not put in place - with a negative unintended impact on Unit 0

Elements Impacting HF Effort

- Stage of the design process
  - The HF work began late in design process
  - Ability to influence design was better earlier in the design process
- Complexity of the design
  - Less complex designs - fewer recommendations.
- Design Staff Knowledge of Human Factors
  - Throughout the project, training was given to engineers
  - HF effort became easier over course of project
  - Less likely to modify design without consultation
- Legislative Framework
Design Process Changes

- Single HFEPP with customized project plans
  - Facilitates consistency of effort
- Risk element added to the classification process to better focus the ‘Major’ effort
- Minor process reworded for ease of use by designers
- Plant modification process changed to initiate HF Effort at the scoping phase

In the future

- HF Classification used to screen the Training Needs Analysis effort for projects
- Systematic monitoring of the design process to ensure correct classification
- Company wide HRA program analyzing the risk associated with tasks, performance modes and barriers to loss
  - Impact on the modification process:
    - initiate/prioritize modifications
    - strengthen the OPEX element
    - trained staff in HRA - strengthen ability to assess modifications
Key Lessons

- HF Screening process is essential to focus effort
- Systematic review of control room changes is needed to monitor cumulative effects
- Specific guidance on HF design outputs is required
- Monitoring through to in-service needed to minimize deviations from agreements

Summary

- Restart efforts were successful in the following:
  - Influenced the design
  - Increased awareness of human factors
  - Streamlined the training process
  - Mitigated regulatory risk
- Indicators of success
  - Changes to HF Design Management program
  - Higher HF staffing levels
  - HF specialists involved in non-design issues
  - Becoming easier to implement HF reviews in design
Guidelines for Control Room Modernization as Part of Instrument and Control Modernization Programs

Joseph Naser and Lewis Hanes (EPRI), John O’Hara (BNL), Robert Fink and Douglas Hill (MPR), Glenn Morris (DOE)

EPRI
3412 Hillview Avenue
P. O. Box 10412
Palo Alto, California USA
Tel: +1 650 855 2107
Fax: +1 650 855 2090
Email: jnaser@epri.com

Abstract

Several nuclear power plants are starting instrumentation and control (I&C) modernization programs using digital equipment to address obsolescence issues and to improve plant performance while maintaining high levels of safety. As an integral part of the I&C modernization program, the control room and other human-system interfaces (HSIs) will also be modernized. To support safe and effective operation, it is critical to design, implement, operate, maintain, and train for the control room and HSI changes to take advantage of human cognitive processing abilities.

A project, jointly funded by the Electric Power Research Institute (EPRI) and United States Department of Energy (DOE), is developing guidance, and the technical bases for this guidance, for specifying and designing digital components and systems, and their incorporation into hybrid (analog/digital) control rooms, remote shut-down panels, etc. Three types of guidance will be developed. The first is strategic planning guidance to help a utility develop its plant-specific control room operating concepts, endpoint vision for the control room, migration path to achieve that endpoint vision, and regulatory, licensing, and human performance program plans. The second is guidance for general HSI principles, for analysis, design, and verification and validation processes, and for training, simulation, and performance monitoring. The third type of guidance is for the detailed design of specific types of HSIs. Although the guidance is intended for immediate application to digital I&C replacements, it also applies to design and implementation of new plant systems and interfaces.

The guidance is being developed for application by utilities and by designers and suppliers of digital I&C replacements for power plants and will facilitate the specification, design, implementation, operations, maintenance, training, and procedure development activities. This guidance will be used to reduce the likelihood of human errors, reduce licensing risk, and increase human and overall plant performance.
1. Introduction

The majority of instrumentation and control (I&C) equipment in nuclear power plants in the United States was designed at least 25 to 45 years ago with analog and relay components, and in some cases rudimentary digital technology. Today, most of these plants continue to operate with a substantial amount of this original I&C equipment that is or soon will be obsolete. Much of this equipment is approaching or exceeding its life expectancy, resulting in increasing maintenance efforts to sustain acceptable system performance. Decreasing availability of replacement parts, and the accelerating deterioration of the infrastructure of manufacturers that support analog technology, accentuate the obsolescence problems and cause operation and maintenance (O&M) cost increases. In addition, the older technology limits the possibilities for adding new beneficial capabilities to the plant systems and interfaces.

Modernization of I&C systems and components, using digital equipment to address these obsolescence issues and the need to improve plant performance (e.g., increase power output capacity, reliability, and availability) while maintaining high levels of safety, is a current major issue for nuclear power plants in the United States and throughout the world. A number of nuclear power plant owners/operators are committing to major modernization programs. The need for this modernization will accelerate as plants age, as more plants receive their license renewals, and as features that digital technology offers are needed to increase cost-effective electricity production. As an integral part of the I&C modernization program at a nuclear power plant, the control room and other human-system interfaces (HSIs) will also be modernized. To support safe and effective operation, it is critical to specify, design, implement, operate, and maintain, as well as train for, the control room and HSI changes to take advantage of human cognitive processing abilities. This consideration of the human should be done to increase performance and to reduce the likelihood of human errors. This is essential in order to obtain maximum benefits of the new technology.

In most cases, modernized control rooms will be the result of incremental modernization steps of equipment and HSIs over several fuel cycle outages. The resulting control room and HSIs at each of the incremental modernization steps will be a hybrid control room. That is, it will be a combination of analog and digital technology. After each modernization step, the amount of analog technology will decrease and the amount of digital technology will increase. This means that the relationship between the human and the control room technology will keep changing until the complete modernization program is completed. Depending on how far the plant wants to go with its modernization program, the final configuration of the control room may still be a hybrid configuration. It should also be noted that even if the plant decides to do its entire modernization at once, the resultant control room could still be hybrid if that is the desired final state.
Concern exists by the plant owners/operators that if new digital equipment and the resulting control rooms and HSIs are not specified, designed, implemented, operated, and maintained correctly from a human factors perspective, the potential for human errors will increase and benefits of the new technology will not be achieved. It is important that a vision of the final configuration of the control room is established at the beginning of the modernization program and that current human factors knowledge and guidance is used in reaching that configuration. It is also important that the human factors knowledge and guidance is applied to each modernization step of the control room and HSIs as well as to the final configuration of the control room and HSIs. It is also important that the control room and interfaces are totally capable of controlling the plant under all conditions, and potentially for the rest of the life of the plant. This last is essential in case funding or other conditions occur that eliminate or significantly delay future modernization steps.

Examples of some of the major control room questions being asked by the plants are the following:

- What changes to our concept of operations should we consider?
- What new functional and HSI capabilities should we consider?
- How should we incorporate human factors engineering concepts?
- How do we reduce the likelihood of human errors?
- How do we achieve the full benefits from the new digital technology?
- How do we train operators during the ongoing changes in the control room?
- When, where, and to what extent should we use automation, computerized procedures, computerized support systems, etc.?
- What are the best types of displays available for various applications?
- What are the required licensing and regulatory activities and how do we ensure regulatory acceptance?

Although numerous human factors guidelines have been published, specific guidance needed both to satisfy safety requirements and to achieve high levels of availability, reliability, and productivity in nuclear power plants is not readily available. The United States Nuclear Regulatory Commission (NRC) has published human factors guidance documents in some related areas that are intended for use by the NRC in reviewing proposed upgrades regarding safety issues. They do not provide additional guidance needed to specify, design, implement, operate, maintain, and train for cost-effective, integrated HSIs to achieve high levels of availability, reliability, and productivity. Nuclear power plant owners/operators are looking for guidelines to address the areas above for operating plants. A scoping and planning study for a project to develop these guidelines was done in the latter part of 2000 [1].

2. Control Room and HSI Endpoint Vision and Migration Path Definition

Nuclear power plant owners/operators have also identified a need for a process to determine the plant-specific vision for the control room at the end of the modernization program. This endpoint vision includes the role of operator, the type of interfaces, and the functionality of the systems and interfaces in the control room. An important aspect
in the definition of what should be in the control room and how it is implemented is the concept of operations that includes how the plant will be operated under normal conditions and abnormal conditions, including loss of displays, loss of controls, and loss of plant systems and equipment.

In the United States it is extremely unlikely that a nuclear power plant will shut down long enough in a single outage to do a complete modernization of the control room, HSIs, and I&C needed to reach the plant's endpoint vision for the control room, HSIs, and I&C systems and components. This is true in other countries as well. The owners/operators are reducing the duration of refueling outages in the plants to increase availability and power production. They are requiring that the modernization activities do not extend the planned refueling outage duration. The exception to do a complete modernization in one outage would be for a plant that is only going to do a minor modernization program that can be done within one normal refueling outage, or a plant that is planning an extended outage for other reasons and can use that as an opportunity to modernize. Therefore, another important process that is needed is how to develop a plant-specific migration strategy to achieve the control room endpoint vision over several modernization steps. This migration plan, as well as the control room endpoint vision, needs to be correlated with the overall plant-specific I&C endpoint vision and migration path and will mostly likely require some level of iteration. Again, it is important to make sure in the migration plans that the plant and control room configuration at the end of each step can completely handle the plant under normal and abnormal conditions. Although the intent is to complete the modernization program, conditions may change and the remaining part of the modernization program may not be able to be done. Therefore, each step should leave the plant in a state that it could be operated indefinitely.

3. Hybrid Control Room and HSI Guideline Development Project

The Electric Power Research Institute (EPRI) and the Department of Energy (DOE) have an on-going project started in 2001 to develop guidance, and the technical bases for the guidance, for hybrid control rooms and digital system HSI including human performance related issues. This guidance will support, in addition to meeting safety requirements and the plant's operational requirements, improved cost-effective plant and human performance and reduced likelihood of human errors, resulting in improved plant safety, availability, reliability, and cost-effective operation. This project is also developing technical bases to support the development of design and implementation guidance in new critical advanced technology areas related to control rooms, such as process automation and computerized operator support systems. Although the guidelines are being developed with hybrid control rooms in mind, the majority of the guidance applies to all-digital control rooms as well.

The guidance being developed in this project is of three types. The first is strategic planning guidance to help a utility develop its plant-specific control room operating concepts, including operation under abnormal conditions caused by loss of human-system interfaces, loss of plant equipment or systems, and external events. The planning guidance will also help a utility to develop its plant-specific endpoint vision for the
control room, to develop its plant-specific migration path over several fuel cycles to achieve the endpoint vision (assuming the modernization is not done completely in one step), human factors program planning, and planning for regulatory and licensing activities. These planning guidelines, except for the last two topics, have been developed and published [2]. The second type is guidance on processes for activities such as HSI design human factors engineering analyses, training and simulation, human verification and validation, and performance monitoring. The third type is detailed guidance on specific technical areas needed for control rooms and digital I&C system HSIs. Examples of these technical areas are information displays, display functions, soft control systems, alarm systems, computer-based procedure systems, computerized operator support systems, and maintainability of digital systems.

A working group of industry experts representing 20 nuclear power plant owners/operators, 4 suppliers, consultants, Brookhaven National Laboratory (BNL), DOE, EPRI, Nuclear Energy Institute (NEI), and NRC Research and Regulation Branches was put together to identify what guidance is needed, to prioritize development activities, to provide input, and to review and evaluate the resultant guidelines and technical bases behind them.

Since several plants are already starting comprehensive I&C modernization programs, the need for guidance in many areas, including the endpoint vision definition and migration plan, is urgent. Therefore, the plants cannot wait for the completion of the project for the guidance. To support this need, intermediate guidance results are being issued throughout the project based on the identified needs of the owners/operators in the working group [2, 3]. In addition to published reports, drafts of guidance and technical bases are being released to the working group members as they are developed.

4. Critical Goals and Strategic Vision

Modern technology, and its ability to better provide and use real-time information, offers the opportunity to improve productivity and to replace systems that are unreliable, obsolete, and costly to operate and maintain. Some of the critical goals for nuclear power plants are the following:

- Maximize plant capacity/output power levels,
- Achieve and maintain high reliability,
- Achieve and maintain high availability,
- Maintain high levels of safety,
- Maintain high levels of operator awareness of the plant and equipment states,
- Minimize the likelihood of human errors, and
- Integrate fault tolerance and fault recovery into the systems (both from potential human and equipment errors).

The EPRI I&C Steering Committee, which consists of nuclear plant owner/operators who are sponsoring the hybrid control room project, recently established a long term strategic vision for EPRI I&C activities: "The 100 Person Plant". This vision is really a concept rather than a specific objective and it reflects the need to operate plants more efficiently
and to reduce costs, and it also reflects the realization that the number of trained people in
the nuclear industry is decreasing. This vision provides a considerable challenge and
may not be able to be fully realized. However, this long-term objective will lead to a
journey of research and development activities that will provide substantial beneficial
products and advances that can be implemented in operating and new plants. Modern
control room, HSI, and I&C technology can provide significant tools to meet the above
critical goals and support the journey toward this strategic vision. Therefore, the
guidance for control rooms and digital HSI will support achieving both the critical goals
and the strategic vision.

5. Control Room Endpoint Definition and Modern Technology

A major aspect of the endpoint vision of the control room is the determination of the
capability/functionality of the systems and interfaces. In the past, nuclear power plants
had commonly looked at “like-for-like” replacements when they start defining the
modernization of old systems. That is, the plants just implement the same functionality
and capability of the old system with new technology. At the most, some simple
interface or other minor changes may be made. This may be the best modernization
solution in some cases. However, in many/most cases it is not. Therefore, it is important
to look at and take advantage of the improvements that modern, digital technology can
bring now and in the foreseeable future.

As part of the definition of the endpoint vision of the control room and HSIs, it is
important to consider what the new technology offers, how it can be used, and what the
benefits and drawbacks of the new technology are. Some of the areas that should be
considered include the following:
- Large screen displays,
- Video display unit (VDU) based information systems,
- Soft controls,
- On-line, computerized procedures,
- Advanced alarm processing and presentation techniques,
- Model- and task-based displays,
- Interface management strategies, including navigation,
- Computer-supported information collection, access, manipulation, distribution,
  storage, and documentation,
- Integrated displays (e.g., procedure displays that include process information and soft
  controls),
- Self-testing and diagnostics,
- Redundancy and diversity,
- On-line monitoring and diagnostics,
- Early fault detection and diagnostics,
- Fault tolerance and fault recovery,
- Process automation,
- Computerized operator support systems and decision aids,
- Maintenance aids, and
Engineering aids.

Consideration should be given to the full spectrum of operational and maintenance activities under normal and abnormal conditions.

While the main thrust of this paper is the modernization of the control rooms in operating nuclear power plants, many of the same considerations for defining the endpoint vision apply to the design of new plants. The major differences are that the starting point for a new plant is a blank sheet, as opposed to an existing control room, and that the new plant control room will be implemented all at one time, as opposed to a migration program over several outages. Another major difference is that the new plant can easily implement the entire infrastructure needed to support the control room, whereas in the operating plants there will be more limitations. These limitations will either have to be worked around or they will eliminate some of the possibilities in the control room and HSIs.


The guidelines are currently being developed. The development process involves four levels of completion—in outline form, under development, under review, and completed.

Some of the guidelines are identified in the annotated outline, but development of these guidelines has not started.

A second group of guidelines is under development. This means that the guideline is being developed but is not ready for review by the working group. There are several steps in the development process. The subset of the development team developing this guidance area may be working on the guidelines until they are ready for review and comments. The full development team may be in the process of reviewing and commenting on the guidelines. The original developers may be modifying the guidelines to address the input and comments from the remainder of the development team. This cycle goes on until all of the input and comments have been addressed and agreed upon by the development team.

The third group of guidelines is undergoing working group review. This means that the guideline has been developed, reviewed by other members of the development team and their comments and input incorporated into the guideline as appropriate, and the guideline has been sent to the working group for review and comments. The comments and input from the working group are also resolved, which may take more than one round of this cycle.

The last group of guidelines is complete. This means that the guideline has been developed and the working group's comments and input has been incorporated as appropriate. A variation of this category is continuing/complete to date. This is used for the appendices. The sections in the appendices will continue to grow as new guidelines are completed. This category means that the appendix is complete for the guidelines that
have been completed so far. The appendix will continue to have additional information as more guidelines are completed.

The status of each guidance area is provided below. This complete list of guidance areas has not been finalized as the working group may request more topics to be addressed as the project continues.

- Introduction (background, objectives and scope, general purposes of human factors engineering, intended users) – complete

- Planning
  - Management considerations - complete
  - Endpoint definition - complete
  - Migration strategy - complete
  - Human factors program planning – under development
  - Planning for regulatory and licensing activities – working group reviewing

- Process
  - Human system interface design and integration – under development
  - Human factors engineering analyses – under development
  - Training and simulation – under development
  - Human verification and validation processes - outline
  - Performance monitoring – outline

- Detailed human factors engineering guidelines
  - Information display – complete
  - Display functions – comments received from working group
  - User interface interaction and management – working group reviewing
  - Soft controls – complete
  - Alarms – complete
  - Computer-based procedures – complete
  - Computerized operator support systems - outline
  - Communications systems – outline
  - Workstations and workplaces – under development
  - Maintainability of digital systems - outline
  - Configuration management and security – under development

- Licensing
  - Regulatory requirements and expectations – outline
  - Engineering evaluations related to licensing – outline
  - 10 CFR 50.59 evaluations – outline
  - Licensing submittals – outline

- Appendices
  - Acronyms – continuing/complete to date
  - Glossary – continuing/complete to date
7. Related Activities

The working group and development team identified the current set of guidelines that are being addressed under this project. However, it is clear that there are other areas of concern that need guidance and technical basis development. The working group and development team put together a list of 20 topic areas. Several experts reviewed this list and ranked the topics using four criteria:

- Potential impact on productivity and cost
- Safety impact
- Scope which refers to whether it applies to a large number of plants or not
- Urgency

The topic areas and the results of the ranking have been described [4].

A workshop on control room modernization was developed and presented at the IEEE 7th Conference on Human Factors and Power Plants. The technical material used for the workshop was published for broader dissemination [5].

8. Conclusions

Obsolescence issues with existing I&C equipment and the need to improve plant performance is leading to modernization of I&C systems and components, including control rooms and HSIs, in nuclear power plants. These modernization programs offer the opportunity to take maximum advantage of modern technology to help achieve new, more aggressive plant goals and to support the journey towards the strategic long-term vision of “The 100 Person Plant”. Concern exists that, if the new digital technology is not specified, designed, implemented, operated, maintained, and properly trained for, the potential for human errors will increase and the benefits of the new technology will not be achieved. The guidance being developed by EPRI and DOE should minimize this concern.

8. References


Background

- Majority of I&C equipment in U.S. nuclear plants were designed 25 to 45 years ago
- Similar situation for many plants around the world
- Much of this equipment is still being used and is approaching or exceeding its life expectancy
- This results in increasing O&M costs to maintain acceptable performance
- Also limits possibilities for adding new beneficial capabilities to improve human and plant performance
Background (Cont’d)

• Obsolescence issues are increasing

• Several plants are committing to major I&C modernization programs that include wide scale control room and other human system interface (HSI) modernization

• Modernization will increase as:
  - Plants age
  - Plants receive license renewals (16 units in the U.S. so far, 14 under review by NRC, and 24 units scheduled to file)
  - Plants identify features of digital technology that support more cost-efficient operation

Background (Cont’d)

• Major control room and HSI questions are
  - What are the operating concepts
  - What should be the functional and HSI capabilities in the control room
  - How do you incorporate human factors engineering concepts
  - How do you reduce the likelihood of human errors
  - How do you achieve the potential benefits from the new technology
  - How do you train operators during the changes
Hybrid Control Rooms

- Modernized control rooms will most likely be the result of incremental modernization steps; as it is expected that most plants, if not all, will have to fit modernization activities within normal outages.

- This will result in hybrid control rooms (combination of analog and digital technology) that will keep changing over an extended period of time.

- Depending on how far the plant takes its modernization program, the control room may still be hybrid at the end of the modernization program.

Conventional Control Room
Early Stage Hybrid Control Room

Advanced Control Room
Control Room and HSI Modernization

• To support safe and effective operation, it is critical to specify, design, implement, train for, operate, and maintain control room and HSI changes to take advantage of human cognitive processing abilities

• This consideration of the human should be done to
  – Increase human and plant performance
  – Reduce the likelihood of human errors
  – Achieve the full benefits of new technology

Human Factors Guidelines

• Numerous human factors guidelines have been published

• Specific guidance is not readily available for nuclear plants to
  – Satisfy safety requirements
  – Achieve high levels of availability, reliability, and productivity

• NRC has guidance documents for use by the NRC in reviewing proposed upgrades regarding safety issues
Human Factors Guidelines (Cont’d)

- They do not provide additional guidance needed to specify, design, implement, operate, maintain, and train for control room functions and HSI's to achieve high levels of availability, reliability, and productivity.
- Guidelines, and the technical bases for them, to support owner/operators, suppliers, and third party integrators are being developed under a joint program by EPRI and the Department of Energy.

Human Factors Guidelines (Cont’d)

- In addition to meeting safety requirements and the plant's operational requirements, this guidance will support:
  - Improved plant and human performance
  - Reduced likelihood of human errors
- Since the guideline information is needed by some plants now, drafts of the sections of the guidelines are being made available to the plants before the guidelines are completed.
Endpoint Vision

- Definition of an endpoint vision for the control room and other HSI is essential to assure plant needs are satisfied
- It is critical to take a strategic look at the control room and HSI to meet the long term needs of the plant
- Major aspects are the determination of the operating concepts and the capability/functionality of the control room systems and interfaces
- Consideration should include operation and maintenance activities under normal and abnormal conditions

Endpoint Vision (Cont’d)

- As part of the endpoint vision for the control room and other HSI, it is important to consider
  - What new technology offers
  - How it can be used
  - What are its benefits and drawbacks
- Life-for-like replacements of existing equipment may make sense in some cases but for many cases it is not the best solution from a performance, and perhaps, safety point-of-view
Endpoint Vision (Cont’d)

• Should evaluate the advantages of the digital technology being implemented to maximize the benefits that can be achieved.

• Since the final realization of the endpoint vision will be several years out, the technology evaluation and associated benefits (and drawbacks) should consider anticipated future technology as well as current technology.

Human Factors Guidelines

Content

• The guidance being developed is of three types
  – Strategic planning guidance
  – General process guidance
  – Detailed guidance for detailed control room and HSI technical areas
Guideline Sections and Status

- Planning guidance
  - Need for planning, endpoint definition, migration path – final draft completed
  - Human factors program planning – draft under development
  - Planning for regulatory and licensing activities – first draft completed

- Licensing
  - Regulatory requirements - draft under development
  - Engineering evaluations related to licensing - draft under development
  - 10 CFR 50.59 evaluations - draft under development
  - Licensing submittals - draft under development

Guideline Sections and Status (Cont’d)

- Process guidance
  - Introduction to human factors engineering processes – first draft completed
  - Human system interface design and integration – draft under development
  - Human factors engineering analyses – draft under development
  - Training and simulation – draft under development
  - Verification and validation processes – outline
  - Performance monitoring – outline
Guideline Sections and Status
(Cont’d)

• Detailed human factors engineering guidance
  – Basic HSI elements
    • Information display – final draft completed
    • User-interface interaction and management – final draft completed
  – HSI systems
    • Alarm systems – final draft completed
    • Soft control systems – final draft completed
    • Computer based procedure systems – final draft completed

Guideline Sections and Status
(Cont’d)

• Computerized operator support systems – first draft completed
• Communications systems – outline
  – Workstation and workplace design
    • Workstations – draft under development
    • Workplaces – draft under development
  – HSI support activities
    • Maintainability of digital systems – outline
    • Configuration management and security – draft under development
Reports Published


• Nuclear Power Plant Control Room Modernization Planning, EPRI 1003569, Oct. 2002

• Critical Human Factors Technology Needs for Digital Instrumentation and Control and Control Room Modernization, EPRI 1007794, Mar. 2003

Reports Published (Cont’d)

• Technical Material for a Workshop on Control Room Upgrades, EPRI 1007795, Mar. 2003

• Interim Human Factors Guidance for Hybrid Control Rooms and Digital I&C Systems, EPRI 1003696, Sept. 2003
Conclusions

- Obsolescence issues with existing I&C equipment and the need to improve plant performance is leading to modernization of I&C systems and components, including control rooms and HSIs.

- These modernization programs offer the opportunity to take maximum advantage of modern technology to help achieve new, more aggressive plant goals and to support the journey towards the strategic long-term vision of "The 100 Person Plant".

- Concern exists that, if the new digital technology is not specified, designed, implemented, operated, maintained, and properly trained for, the potential for human errors will increase and the benefits of the new technology will not be achieved.

- Guidance being developed should minimize this concern.
A micro-macro human factors approach to improve teamwork after an incident

VAUTIER J.-F., TOSELLO M., BARNABE I., GARANDEL S., PAULUS V. and PAPIN B.
CEA, France

Emails: jean-francois.vautier@cea.fr, michele.tosello@cea.fr,
isabelle.barnabe@cea.fr, sylvie.garandel@cea.fr, valerie.paulus@cea.fr and
bernard.papin@cea.fr

Introduction

Why do we propose a micro-macro approach?

Description of a double approach related to human factors.

Illustration with an incident.
Why do we propose a micro-macro approach?

Most approaches in the nuclear safety field are focused on human errors or failings. A necessary but not sufficient aspect!

Necessity to examine also what explains that operators carry out correctly theirs tasks:

→ the management process of human factors

A double approach

A double approach related to human factors: the microscopic aspect.

A microscopic aspect focused on the human factors of work situations (work organization, team and operators, technical system and work environment).
The HF tree model

Effective activity of the team

Difficulties
- Team reliability
- Failings
- Team performance
- Physiological and psychological costs for the humans of the team
- Physiological and psychological benefits for the humans of the team

Microscopic aspect

Examination of the effective activity of the team and the difficulties and failings of operators.

The objective: understand what is the contribution of the human factors on these difficulties and failings in the incidental situation we are studying and propose ways of improvement.
A double approach related to human factors: the macroscopic aspect.

A macroscopic aspect focused on the management of the human factors e.g. the general provisions for designing and maintaining the quality of human factors in the work situations.

The occurring of the incident

This incident was imagined from very common work situations in industrial plants. It is fiction but it is often used in general training sessions to test the students’ reactions.

The work situation

In a plant, two operators manage the process of transformation of a fluid. They use a display and control board.
Microscopic aspect

Modifications to:
- incidental procedures,
- size of the team during the night-time work,
- skills of operator 2,
- displays and controls.
**Macroscopic aspect**

Modifications to the design process of human factors:
- design process of the incidental procedures and the size of the team,
- design process of the displays and controls,
- ...

Modifications to the conservation or maintaining process of human factors:
- management of skills and advancement,
- ...

**Conclusion**

A double approach to take into account the HF. Articulation of local and general aspects, short and long term points of view (microscopic and macroscopic approach) to carry out modifications.

This double approach is also carried out in preventive studies during recurring safety assessment of the nuclear facilities of CEA.
A CLASSIFICATION OF VALIDATION CRITERIA FOR NEW OPERATIONAL DESIGN CONCEPTS IN NUCLEAR PROCESS CONTROL

ANN BRITT MIBERG SKJERVE and GYRD SKRAANING JR
OECD Halden Reactor Project

Nuclear power plant control rooms are gradually changing as a function of technological improvements. In this modernization process, it is natural that new human-machine system design concepts are emerging. It is important, however, that operational design concepts are validated with respect to their usability. Existing ergonomic standards, such as ISO 9241, support identification of several validation criteria that can help to determine to which extent a design solution is usable. The term 'usability' is then used in a wide sense, including user acceptability, benefits to the operators' teamwork and taskwork, and the effects of the design solution on joint human-machine system performance. This paper suggests that validation criteria should be organized in accordance with human-centered design principles, maintaining user acceptability (support) as a key issue throughout the validation process. The proposed classification scheme is linked to a range of methodological approaches on the individual and team level, and represents a coherent and systematic approach to the validation of design solutions that have different levels of maturity. Furthermore, the paper addresses the relationship between different types of usability, and the risk/safety anchoring of validation criteria.

1. INTRODUCTION

When innovative operational design concepts are implemented there is a need to verify and validate the properties of the new human-machine system design. The practical objectives of the verification and validation (V&V) process are to ensure that the designed system fulfills the requirements stated in the design specification, and to support or corroborate that the system functions as intended, respectively. This paper will focus on the part of the V&V activities that concern usability validation.1

The introduction of new design solutions often involves aspects of human problem solving competence that are qualitatively different from previous solutions, e.g., the transition from conventional to computerized control rooms. Applying usability validation criteria from existing design solutions will thus constitute a mode error, since operators will behave on the basis of different psychological principles under principally different working conditions. This paper addresses the criterion problem, i.e., question of determining which criteria to evaluate measures against in a validation process (e.g., Stager, 2000), by suggesting a framework to support selection of relevant types of validation criteria. The suggested framework is intended to assist a designer's assessment of whether a design solution should be accepted or revised at different stages in a design process - not to provide detailed information to support diagnosis or remedies of specific problems related to functionality and interface design aspects. In this respect, the suggested framework should support design-related activities that are located in between Human factors engineering (HFE) design verification (see e.g., O'Hara, Higgins, Persensky, Levis, and Bongarra, 2002) and Integrated system validation (e.g., O'Hara, Stubler, Higgins, and Brown, 1997).

---

1 This paper should be considered as a position paper that accounts for the current line of thinking in terms of usability validation requirements within the OECD Halden Reactor Project's research programs:
“Development of Design Support based on HAMMLAB Data Sets” and “Integrated System Validation.”
2. PREMISES

2.1 The Objective of Usability Validation

The objective of a usability validation process can be defined differently in terms of the required degree of comprehensiveness.

It can be argued that a designed system, e.g., a decision support system, is valid, when operators can be demonstrated to achieve a set of specified operational goals within required standards for safety and efficiency, working with the system as a stand-alone application. From this perspective, the objective of the validation process is to ensure that the system is operational, i.e., that it contains the desired functionality and a human-machine interface that allows the operators to perform the selected tasks satisfactorily. Still, within the nuclear power plant (NPP) community, the above objective is generally considered to be too limited. It is argued that to pass a validation test, the designed system should further be demonstrated to support the joint human-machine system's performance in the intended context of use. The rational for the extended objective is to ensure that the designed system not merely is operational, but of actual benefit to the target organization.

Considering the above discussion it is, however, characteristic that neither of the suggested definitions explicitly addresses the issue of validation beyond the immediate or short-term perspective. They focus on whether operators can use the designed system, and if so, whether this can be expected to generate the anticipated benefits. Neither of the definitions explicitly addresses the extent to which the operators in practice can be expected to actually use the system in a longer-term perspective, i.e., as long as the context of use remains as implied in the validation process. The implicit assumption seems to be that if the operators can use the system, they will use the system. Still, the question of system use is critical to the purchaser of a system. Unless the operators in practice use the system, none of the anticipated benefits that are assumed to follow the system's implementation will ever become manifest. Another potentially critical issue related to longer-term use concerns the extent to which the operators will come to use the system in the manner envisaged by the system designer. This question seems particularly pertinent with reference to the transition period, i.e., the period in which the system is introduced in its intended context of use. Data from the aviation domain clearly demonstrate that the accident rate is significantly higher during the first introductory years of the different generation of aircrafts, than following this period (Airbus Industry Safety Department "Hangar Flying", June 1997, as referred in Pariès and Amalberti, 1999).

To take the considerations for future system use into account, in the sense discussed above, the objective of a usability validation process will be considered as: To uncover the extent to which the designed system will come to support the operators' performance in its intended context to ensure that production is carried within the required standards for safety and efficiency.

2.2 Usability

To validate a design solution in terms of usability implies that the concept of usability initially should be defined. Dumas and Redish (1999, 4) define usability as a requirement to ensure that "... the people who use the product can do so quickly and easily to accomplish their own tasks." Similar definitions may be found in various textbooks. For the purpose of the present paper, a focus solely on validation criteria
related to user performance will, however, not be sufficient. The reason is that criteria related exclusively to user performance can be expected to capture only one part of the validation objective, i.e., the extent to which the users can use the system, but not the second part that concerns the extent to which the users will use the system in practice. ISO 9241-11 provides a broader and more comprehensive definition of the usability concept. In this standard usability is defined as the:

"Extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." (ISO 9241-11, 1998, 2)

The definition provided by ISO 9241-11 may thus suggest that usability should be validated with reference to three types of criteria: effectiveness, efficiency, and satisfaction. Effectiveness is defined as the "Accuracy and completeness with which users achieve specified goals." (ibid.). This criterion can be interpreted to concern how effectively the operational goal is achieved by the joint human-machine system. Efficiency is defined as "Resources expended in relation to the accuracy and completeness with which users achieve goals." (ibid). This criterion may be seen as concerning the operators' work process, and refer to the level of resources required by the operators to achieve the operational goal. Satisfaction is defined as "Freedom from discomfort, and positive attitudes towards the use of the product." (ibid.). This criterion thus relate to the operators' subjective evaluation of the designed system's characteristics and adequacy.

The definition of usability suggested by the ISO 9241-11 seems to capture the various aspects of usability of relevance both to the users and to the purchasers of a designed system, and it seems reasonable to apply these as basic elements in a usability validation process.

2.3 Discussion of the Three Types of Usability Criteria in relation to Validation

Applying the three criteria suggested by ISO 9241-11, effectiveness, efficiency, and satisfaction, as a starting point for defining usability validation criteria, the question is how the three criteria should be conceptualized to accommodate the objective of the usability validation process (see page 2).

2.3.1 Satisfaction – User Acceptance

The Human-Centered Design approach (Rouse, 1991) takes as its primary focus the role and capabilities of the operator. It regards systems as tools, which should be designed to support operators' performance, based on the argument that the human operators will ultimately be responsible for outcome of the task performance process (Billings, 1991). One of the key objectives in human-centered designs is to foster user acceptance by ensuring that the operators are provided with roles that they consider to be satisfactory (Rouse, 1991).

Given that the operators are sufficiently skilled to operate a designed system, it seems fair to assume that the operators also will use the system if they consider the system to provide adequate support and benefits, i.e., if the users accept the system. This implies that criteria, which are somehow related to satisfaction, will constitute a key factor when predicting to what extent a designed system will actually be used. Rasmussen and Goodstein (1988) also stress the importance of user acceptance, and suggest that user...
acceptability is a key factor for determining the extent to which system upgrades will actually be used. Still, in a situation where a design solution affects the entire set of operator tasks (e.g., a complete redesign of the control room), or a complete sub-set of the tasks (e.g., computerization of procedures), operators may in practice be left with little choice but to use the new system. In these situations, human adaptability may sometimes ensure that the operators eventually will come to appreciate the system and use it as intended. However, the risk remains that the operators’ adaptation to the system will imply the development of informal work routines which ensure that the disapproved of system features are avoided to the extent possible. When deviations occur that the operators are expected to handle using the disapproved of system features, the operators’ level of familiarity with these may thus be substantially lower than presumed by the system’s designer, whereby the risk for inefficient handling increases.

Holmgren (1998) performed a series of long-term usability studies. She assessed usability based on repeated measurements of operators’ subjective judgments of the production system they worked with, as expressed in questionnaires and interviews. The shortest study covered a period of 6 months, the longest a period of 15 years. One of the issues addressed by Holmgren was what system characteristic the operators appreciate most in computer-based systems. She found that a system’s quality, as judged by its users, could be determined with reference to five variables:

- System reliability
- Information reliability (the information provided should be trustworthy)
- Recommend the system to others (the operators would do only recommend the system if it was perceived to be reliable)
- System usability or support at disturbances
- The possibility to work in a rational way using the system.

Holmgren further found that the factor, which seemed to have the strongest influence on operators’ assessment of a system's quality, was the extent to which the system was perceived to be useful/supportive during disturbance situations. This could indicate that situations in which operators can be expected to have the least experience – and thus to have adapted the ‘least’ to - play a critical role when they assess the usefulness of a design solution, seen in a longer-term perspective. Since a key reason why operators are in the plants today is to function as deviation handlers, and since efficient deviations handling is of vital importance to plant safety, the results obtained by Holmgren may be interpreted to support the argument for emphasizing issues related to user acceptance in a usability validation process.

Based on the above, it may be hypothesized that the operators’ perception of the designed system could serve as a latent condition that continually will influence their decisions on when and how to use the designed system, i.e., their motivation for using the system. Thus, if the operators in practice are reluctant to use the designed system, refuse to use the system, or use the system markedly different from what the designer intended, the reason can be assumed to be that they consider the system to be inadequate in some way.  

---

1 Experimental studies have indicated that, e.g., the variable of trust in automation may work in this way. In situations where the operators hold a high level of trust in an automatic system, their tendency to intervene in the system’s activity when deviations occur seems to be lower, than in situations where they hold a lower level of trust in the system (Lee and Moray, 1992, 1994; Tan and Lewandowsky, 1996).
The above discussion suggests that the concept of user acceptance should imply that the users have a need for and actively require the support provided by the designed system when performing the operational task in their normal work environment - and thus, in a validation process, in a full-scale environment (i.e., a full-scale simulator or a full-scale mockup of some kind). If users, who are fully skilled to operate the system, do not use the system in a full-scale environment, this will indicate that they do not consider the system to be of practical use, i.e., that they do not accept the system as a useful part of their current work environment - even if they in principle feel satisfied with the system's design. And if the same type of users uses the system inappropriately, this can be taken to indicate that they do not fully accept the role or function, which the designed system is intended to fulfill in the full-scale environment.

In general, the question of how operators' perceive a designed system seems to be framed in terms of the system's functionality and its interface design. Lack of user acceptance is thus commonly interpreted to imply a need for changes in either or both of these factors. In some cases, it may in addition, or as an alternative to the above, be argued that the training level, the operating procedure, etc. should be changed. However, animosity against a design solution may also relate to - and/or be interrelated with - factors that need not be directly linked to the particular design solution. The operators may, e.g., feel anxious that the introduction of the new system (in particular if the system contains high levels of automation) may imply that their operational skills will gradually degrade and/or that the system will come to change the status associated with the operator job and thus in the long run lead to wage reduction and/or that the introduction of the system will lead to reduction in the staffing level, etc (see also Bainbridge, 1987). In relation to system upgrades, Harwood (1993) suggests that issues of job satisfaction, self-esteem, professional standing among colleagues and individual merit may often have been overlooked, and she stresses that this may have serious consequences for safety and efficiency.

The above discussion suggests that user acceptance, i.e., the users' admittance or approval of the system, is important for the extent to which a system will be used - and to the extent that it will be used as intended by the system designer - and thus a factor that should be of key concern in a usability validation process. It further indicates that user acceptance might be a more appropriate concept than satisfaction to characterize this type of usability validation criteria, to underline that the user not only should be free of discomfort and hold positive attitudes towards the designed system (ISO 9241-11, 1998), but also in practice should demonstrate to accept the system as a useful part of the integrated operational environment. Finally, it should be stressed that a designer will only be able to deal with some of the factors that affect the users' acceptance of the designed system, i.e., the factors concerned with system functionality and design within his or her area of authority. In relation to factors, which go beyond this, the management of the target organization will have to be involved. This issue will not be further addressed here, but it underlines the need for management involvement in the design and validation processes.

2.3.2 Efficiency

In an NPP environment, a system will be considered as valid only to the extent that the users are able to operate the system in a safe and reliable manner. This points to the need for usability criteria that relate to the users' work process. The key factor in work process assessments has traditionally been to determine the level of resources required by the users (e.g., in terms of workload) to perform the operational task, to assess the
probability for safe and efficient performance. For this reason, the concept of efficiency, as defined in ISO 9241-1 (1998, 2), i.e., as the resources expended in relation to the accuracy and completeness, with which users achieve goals, seems to adequately capture the core of these concerns.

2.3.3 Effectiveness - Productivity

In practice, a designed system might not be implemented unless it can be demonstrated to improve (or at least not degrade) the target organization's productivity. To reach the required standard for productivity, the task performance process must be reliable both in terms of safety and efficiency. If accidents/incidents occur and/or if the production rate is low, productivity will be reduced. For this reason, the validation process has to focus on the joint human-machine system's performance and its outcome. The requirement for ensuring productivity might be captured in the definition of effectiveness suggested by ISO 9241-11 (1998, 2), i.e., as the accuracy and completeness with which users achieve specified goal. However, to stress that both safety and efficiency concerns are addressed, and that these factors will be determined by the joint human-machine system's activity, the concept of productivity seems to better capture the content of this validation criteria type.

3. SUGGESTED TAXONOMY OF VALIDATION CRITERIA ORGANIZED WITH REFERENCE TO A DESIGN PROCESS

ISO standard 11064 (2000, part 1), IEC 60964 (1989) and similar standards recommend that V&V activities should be carried out as an integrated part of the design process. As Hopkin (1993, 30-31) points out "... to learn from operational experience that the verification and validation have been insufficient is to leave the lesson too late." To support the performance of usability validation as part of a design process, the usability criteria identified above are organized into three levels: Level 1 - Acceptability, level 2 - Benefits to the operators' work process, and level 3 - Benefits to system performance (see further below). It should be noted that each level may embrace one or more of the above suggested validation criteria types. The reason is that the levels inherit the validation criteria type from the previous level(s), implying that user acceptance will remain a key issue through out the validation process. A level 0 is furthermore added to constitute the baseline condition where no explicit design validation activities are performed. The levels are independent in the sense that a validation study can focus on level 1, 2, or 3 only, or level 1&2, 1&3, 2&3, or 1&2&3 at the same time, and each level may in principle be addressed through out a design process using different assessment techniques, depending on the maturity of the design solution. However, to argue that a system is valid in terms of usability will require that the three levels have been systematically covered in the validation process (see Figure 1). The idea behind this suggestion is that if user acceptance is maintained as a key issue though out the design process without neglecting criteria related to operator and system performance - something which application of the three levels is intended to support - this will contribute to ensure: (1) that the user will come to accept and use the final design solution, (2) that the potential difficulties associated with the transition period will be reduced since the system's characteristics should match the needs of the users, and (3) that the immediate and long term performance effects will be satisfactory. It further

---

5 It should, however, be noted that validation as currently practiced is often considered as "...a culminating activity, generally occurring just prior to the commissioning of a system for active service." (Davey, 2002,2).
implies that the requirements for introducing changes into the designed solution within the first couple of years of its lifetime should be reduced.

**Figure 1.** The figure illustrates that to be considered as valid in terms of usability, a designed solution must meet the requirements on each of the three levels. It further illustrates that each of the three levels may be addressed independently or in conjunction, at any point in time throughout a design process.

The suggested validation criteria levels will be presented below. To facilitate the description of how the levels may be applied in a design process, the presentation is organized with reference to one specific of the many possible approaches for application of the levels (see Figure 2).
Figure 2. Overall schematic representation that illustrates one way in which the suggested levels may be organized as part of a design process.

3.1 Level 0 - Baseline

This is the classical engineering approach where the designer is responsible for the validation of his/her own design solutions. Hence, the validation criteria are based upon the designer’s intuition and knowledge about:

- Mechanical and computational properties of the technological system
- Operational characteristics of the technological system
- Human capabilities and limitations, and the particular characteristics of the particular operator population for which the system is designed.

3.2 Level 1 - User acceptance

In the early part of a design process, the validation criteria applied will refer to the intended operators’ evaluation of the designed system’s characteristics and adequacy seen in relation to the functions that the system is intended to serve in its context of use. Operators test the design solution and express their subjective (expert) opinions concurrently and/or in debriefing sessions with reference to simple prototypes. The validation criteria for the assessment of acceptability are thus based upon operator judgment of the design solution after short-term exposure to a new operational concept. The operators’ assessments may comprise a broad range of usability-related issues, such as the characteristics of the system, the conditions under which the system should be applied, but also the possible implications that may follow from implementing the system in its intended context of use:
• How can the design solution be improved to meet the operators' needs with regard to usability, task performance, and job satisfaction?
• Under which conditions are the new design solution acceptable, e.g., by changing training requirements, operator roles, task allocation, teamwork styles, organization?
• Do the operators have other types of reservations with reference to the consequences of introducing the designed product?

It should be noted that the operators' concern could relate to issues, which are beyond the authority of the system designer, as discussed above.

In Figure 2, the 'acceptability' box has dotted – as opposed to solid – lines. The dotted lines are used to indicate that this box might not be mandatory in the early phase of a design process. The extent to which the designer will adhere to the user's feedback at this point in time may differ. If the designer, e.g., finds that the users' opinions are based on misconceptions of what the innovative design concept will come to imply, he or she may decide to ask the users to perform a new assessment when the design solution has further matured.

3.3 Level 2 - Benefits to the operators' work process

As the design solution matures, the possibility for performing validation tests with reference to still more realistic prototype versions of the design solution increases. At level 2, the benefits to the operators' work process are evaluated in terms of safety, i.e., if the operators are able to perform the tasks to the required standard for safety when working with the system, through systematic testing, analysis of event reports, and/or simulator experiments. The design solution is validated by scientific evidence indicating whether the operators' work process is supported or degraded by the new design, in terms of individual and team performance. Level 2 further inherits the criteria related to user acceptance from level 1. At level 2, these criteria are included to uncover motivational issues related to the operators' work processes. Examples of applicable criteria are listed below:

Performance related:
• Physical positioning and anthropometry in general
• Cognitive and behavioral task demand. Does the design produce too high or too low cognitive and/or behavioral demand (workload)?
• Use of operating procedures, alarm system, support systems etc.
• Innovative problem solving processes and cognitive flexibility. Are innovative problem solving processes and cognitive flexibility supported by the design, e.g., sufficient autonomy is given to the operators and error tolerance is embedded in the system?
• Operator understanding and information-processing (gathering of adequate system information, ability to generate effective solutions, inductive and deductive reasoning, separate relevant from irrelevant information, “Situation Awareness” etc.)?
• Out-of-the loop effects
• Discrepancy from good operating practice for crews. Is the operators' taskwork judged to be in accordance with “good practice” for operators in the specific human-machine system, e.g., successful verification of information, effective
navigation in computer interfaces, utilization of operator support systems, reasonable balance between manual and automatic control etc.?

- Group processes (risky-shift, conformity etc.)

User acceptance:
- Are long-term motivational aspects taken into account by the design, e.g., preserve self-confidence and internal locus of control etc.?
- Are long-term loss of cognitive competence and system knowledge counteracted by the design (avoid 'out of the loop' effects)?
- Operators' judgment of Human-Automation co-operation quality
- Measures to reveal degradation of teamwork skills
- The operators' level of trust in automation
- Is the quality of operators’ information processing enhanced
- Is long-term degradation of taskwork skills counteracted by the design (avoid deskilling).

In situations where problems are identified at level 2, it will initially be relevant to examine if these might be related to lack of operator education and training, insufficient operating procedures, etc. Changes in these factors may imply that the work process becomes satisfactory in terms of performance and user acceptability. However, if the changes do not produce the required results, it will be relevant to examine whether more general issues related to job satisfaction may play a role, before the design solution is revised.

3.4 Level 3 - Benefits to the joint system's performance

At level 3, the design concept is validated by simulator experiments in order to scientifically demonstrate performance benefits of the new design solution with regard to effectiveness - which includes concerns for safety, as discussed above. This type of criteria will refer to the productivity that may be expected to follow from the implementation of the design solution, and thus in longer-terms to the economic benefits.

Level 3 will inherit the criteria types from the two levels above. Criteria related to efficiency will be used to assess the extent to which the operators' work processes are satisfactory in terms of effectiveness. Criteria related to user acceptance will imply a requirement for the operators to demonstrate that they are able use the design solution as intended in a full-scale context. This last type of criteria is necessary to ensure that the test actually refers to the design solution, as in principle the outcome of the joint human-machine system's performance may be acceptable even if the design solution or various of its relevant subsystems are not used - or not used as intended. Input from simulator studies will answer the following questions:

- Are the resulting physical system states tolerable?
- Are the required productivity standards adhered to?
- Are the operators' work processes satisfactory in terms of effectiveness?
- Do the operators demonstrate to be able to use the system efficiently?

It should be noted that Eurocontrol is currently in the process of working out a set of non-mandatory "Guidelines for Trust in Future ATM Systems". Currently, three reports on the subject have been issued. These are available at: http://www.eurocontrol.int/humanfactors/publ.html.
If the above requirements are not fulfilled, the reasons may be related to the technical solution and/or inadequacies in the operators' work process. In the last case, it may e.g., turn out that even if the work process of the operators using the designed system is safe (level 2) it is not sufficiently efficient, i.e., that the operators' work process is actually too time-consuming to meet the criteria on effectiveness. In both cases the design solution will have to be revised.

3.5 Relationship between Types of Validation Criteria

Design validation experiments in Halden Man-Machine Laboratory (HAMMLAB) have traditionally focused on level 2&3 (ignoring usability aspects on level 2). It has generally been assumed that human performance indicators on level 2 should be related to system performance indicators on level 3 in order to be criterion valid. Validation experiments outside HAMMLAB (e.g., in air traffic control) focus mostly on level 1&2 with an emphasis on level 2 usability aspects. Level 3 data are sometimes collected, but are not used systemically to produce design input, or as a criterion for validation of level 1&2 indicators. Still, both validation approaches claim that they provide useful and trustworthy information to system designers. Given this situation, there is a need to rethink the status of information generated by the three levels of validation criteria as input to system designers, as well as the relation between the levels.

4. ANCHORING OF VALIDATION CRITERIA

One important topic in this respect is how level 1 and 2 criteria should be anchored by level 3 criteria. Theoretically it has to be assumed that acceptability, usability, cognitive performance, teamwork, taskwork skills etc. are related to the performance of the human-machine system. If, for example, a new design solution is hard to use, or the communication between crewmembers is poor, this is expected to affect the operators' ability to control the system. If this were not the case, there would be no rational basis for giving design recommendations using level 1 or 2 criteria. The critical question, however, is whether it is necessary to establish an explicit empirical link between, (a) acceptability and the assessed quality of the operators' work process [level 1&2], and (b) system performance [level 3]. This empirical link may be a necessity for performance analysis of well-known systems, but is probably an unreasonable requirement when the purpose is to provide input to system designers. The following arguments apply:

- Measures of system performance are insensitive, i.e., system states are normally not deviating from the performance standard, required operator actions are usually performed, and the operators typically execute critical actions in time. Hence, there is not sufficient performance variation to create a basis for validation of level 1&2 performance indicators. One exception from this rule is extreme accident situations, where system performance indicators may be sensitive.

- In complex human-machine systems, there is an indefinite number of possible system events. It is therefore extremely difficult to sample representative task conditions (scenarios). In addition, task effects are known to moderate (interact with) design properties, e.g., an alarm system configuration may be beneficial for some events, but not for others. Hence, a sample of a few scenarios are not likely to cover situations where level 1&2 criteria are empirically related to level 3 criteria.

- Technological development changes the content of human-machine interaction. For example, the role of the human operator may change completely in a new system. It
is rather normal that completely new sides of human problem solving competence are taken into use, such as in the transition from conventional to computerized control rooms, or the change from full manual control to high levels of automation. Another example is that the operators may take design solutions into use in unexpected ways. It will often take years of actual operation before the true benefits and risks associated with a new design are revealed. Thus, human-machine system performance is implicitly vague and ill defined in the design phase, and cannot serve as a solid anchor for level 1&2 criteria. In other words, it is known what the new system should do, but it is not known how the operators will pursue the new goals. Using system performance validation criteria from existing design solutions constitutes a mode error, since operators behave on the basis of different psychological principles under principally different working conditions.\(^5\)

- System performance effects are immediate, while many of the level 1&2 validation criteria are long-term. Loss of self-confidence and job satisfaction, for example, may take years. The anchoring of long-term effects should therefore be basic psychological research or longitudinal operational experiences from previous design implementations.

In general, level 1&2 validation criteria should predict how human operators adapt to new and principally different working conditions, represented by innovative operational design concepts. Such criteria can be anchored by, (a) established psychological principles (e.g., loss of motivation degrades performance in the long run), (b) longitudinal operational experience (e.g., it is important for operators to trust the automatic system, follow the procedures etc.), or (c) immediate system performance effects (e.g., there is an empirical relationship between the perceived task demand and system performance in a sample of system events). Hence, it is not a requirement that design validation criteria are justified by statistical relationships to system performance in a given data set.

**References**


\(^5\) This is not identical to performing under rare and complicated situations under the same working conditions, which is the focus of Human Reliability Assessment (HRA).


A Classification of Validation Criteria for New Operational Design Concepts in Nuclear Process Control

Ann Britt Miberg Skjerve and Gyrd Skraaning Jr.
OECD Halden Reactor Project

Purpose: To suggest a human-centred approach for classification and prioritization of criteria for usability validation.

Practical aim: To suggest an approach for selection of validation criteria types that may assist designers in assessing whether a design solution should be accepted or revised at various stages in the design process.

OECD Halden Reactor Project's research programs:
(1) Development of Design Support based on HAMMLAB Data Sets, and (2) Integrated System Validation.
The Objective of 'Human Factors' Validation

The objective of a validation process: to support or corroborate that the system functions as intended.

The comprehensiveness required:
- Operators should be able to achieve a set of specified operational goals within required standards for safety and efficiency, working with the designed system as a stand-alone application.
- The designed system should be demonstrated to improve the joint human-machine system's performance in the intended context of use.

Can use = Will use? - the longer-term perspective

- Tests should indicate the extent to which the operators can be expected to actually use the designed system according to the designer's intentions in the intended context of use, in a longer-term perspective.

What is Usability?

- Criteria for Usability Validation, i.e., standards against which measures are compared to judge their acceptability.

Defining Usability:

"Extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use." (ISO 9241-11, 1998, 2)

Effectiveness: Accuracy and completeness with which users achieve specified goals.

Efficiency: Resources expended in relation to the accuracy and completeness with which users achieve goals.

Satisfaction: Freedom from discomfort, and positive attitudes towards the use of the product.
Human-Centred Approach

Human-Centred Designs: (Rouse, 1991)
- The human operators are responsible for the outcome
- Systems should be designed as tools to support the operators in fulfilling their responsibility
- One of the main objectives: To foster user acceptance.

Suggestion:
- Basic assumption: The operators' are trained to use the system.

Hypothesis: Operators will use the system if they consider the system to provide adequate support and benefits in the context of use.

Usefulness → Satisfaction / User acceptance

Usefulness - System Quality

- User adaptability
  - "operators will always adapt to the system..."
  - no choice but to adapt
  - 'maladjustments'

- Priority of usefulness (Holmgren, 1998)
  1. Disturbances → Low Adaptation?
  2. Start/Stop → High
  3. Normal operation

- User acceptance - system quality:
  - Users' perception of usability in disturbance situations should be emphasized during validation
User Acceptance, the Basic Element

Assumptions:
- if operators are reluctant to use, refuse to use, or use the system markedly different from what the designer intended, the reason will be that they consider the system to be inadequate - in some way.

Suggestion:
- the operators' perception of the system's characteristics serves as a latent condition that will continually influence the operators' decisions on when and how to use the system.
- the operators' perception of the system's usefulness may be a reasonable basic element in a usability validation process.

Validation Criteria Taxonomy

LEVEL 1: Criteria related to operator acceptability
(User acceptance)
- whether to use
- how to use

LEVEL 2: Criteria related to benefits to the operator work process (Efficiency)
- cognitive and physical resources spend
- safety

LEVEL 3: Criteria related to benefits to the joint human-machine system's performance (Effectiveness)
- productivity
- economic benefits
During a Design Process
- one Possible Approach

**Design solution**

**Level 2: Benefits to the operators' work process**
- **USER ACCEPTANCE**: Is the work process acceptable to the operators?
  - **not acceptable**
  - **acceptable**
- **LEVEL 2: Acceptability**
  - **not acceptable**
  - **acceptable**

**Level 3: Benefits to the joint system's performance**
- **USER ACCEPTANCE**: Do the operators demonstrate to use the designed product as intended?
  - **not acceptable**
  - **acceptable**
- **LEVEL 3: Acceptability**
  - **not acceptable**
  - **acceptable**

**Adjustments**
- in education, training, procedures, etc.
- in technical or work process design or in other characteristics?

**Level 1: Acceptability**
- **USER ACCEPTANCE**: Do the operators find that the design solution may fulfill the operational needs, and that it may function well as an integrated part of the intended context of use?
  - **not acceptable**
  - **acceptable**

**Level 0: Baseline**
- **Designer validates his/her own design solution with reference to his/her knowledge and experience**
  - **acceptable**
Level 1: Acceptability

- Operator acceptability after exposure to new design solutions
- How can the design solution be improved to meet the operators' needs with regard to usability, task performance, and job satisfaction?
- Under which conditions are the new design solution acceptable, e.g. by changing training requirements, operator roles, task allocation, teamwork styles, organization?
- Do the operators have other types of reservations with reference to the consequences that may follow by introducing the designed product?

Level 2: Benefits to the operators' work process

- Scientific evidence indicating the extent to which the operators' work process is supported by the new design in terms of safety
  - Evaluated through systematic testing, analysis of event reports, and/or simulator experiments.

Performance
  - Cognitive task demand
  - Situation awareness
  - Are innovative problem solving processes and cognitive flexibility supported?
  - Group processes (risky-shift, conformity etc.).

User acceptance
  - Is human-human and human-automation co-operation quality adequate?
  - Is the quality of operators' information processing enhanced?
  - Is the operators' trust in automation well calibrated?

examples
## Level 3: Benefits to the joint system's performance

- Simulator experiments used to scientifically demonstrate the performance benefits of the new design solution (with regard to risk/safety or production)

- When operators work with the new design:
  - Are the resulting physical system states tolerable?
  - Are the operators' work processes satisfactory in terms of effectiveness?
  - Do the operators demonstrate to be able to use the system efficiently?

## Anchoring of Validation Criteria

- Acceptability, user satisfaction, cognitive performance, task- and teamwork quality etc. have to be related to the performance of the human-machine system (predictive validity)

- How should this relationship this be demonstrated?
  - Appealing to human intuition, or the importance Human-Factors seems too weak
  - Requiring empirical demonstration of causal relationships between Level 1&2 and Level 3 criteria seems too strong
  - System performance scales typically lack sensitivity
  - Unrepresentative sampling of task conditions
  - System indicators can only capture immediate effects.
Anchoring of Validation Criteria, cont.

- Compromise solution - Level 1&2 criteria can be anchored by:
  - Established psychological principles that are undisputed by the research community, or consistent psychological models
  - Long-term operational experience from NPPs (uncontroversial)
  - Empirical relationship to system performance revealed by simulator experiments or event analysis.

Hypothesized Consequences

The validation criteria classification and organization with respect to a design process is hypothesized to support:

1. that the user will come to accept and use the final design solution
2. that the potential difficulties associated with the transition period will be reduced
3. that the immediate and long term performance effects will be satisfactory.

- And that the need for introducing changes into the designed solution shortly after its introduction will be reduced.
Guidelines for Trust in Automation

Guidelines for Trust in Future ATM Systems: Principles
Outline of and the briefing for the break-out sessions

Parallel Stream 1: HUMAN FACTOR

Theme: How to take lessons from feedback experience?

Presentation: Analysis of maintenance history for identification and prevention human CCFs originating from minor modifications and maintenance................................. 143
K. LAAKSO (VTT, Finland)

Theme: How to improve the consideration of potential impact of modification as soon as possible?

Presentation: Taking into account of socio-organizational and human aspects into upgrade packages (technical or not) ......................... 175
L. QUENTIN, D. NIGER (EdF/UNIPE, France)

Parallel Stream 2: OPERATING EXPERIENCE

Theme: Is it possible to set a reference basis to define which modifications, considered as minor, have to be taken into account because of their potential impact on safety?

The Swiss modification process in NPP Regulatory Regime – Regulator/Operator process and experience related to events with safety impact ................................................................. 183
H. DEUTSCHMANN (HSK, Switzerland)

Theme: How to improve the national modification processes?

Presentation: Temporary modifications and minor changes: a threat for the safety of NPP’s................................................................. 201
H. WERDINE (IAEA)
Analysis of maintenance history for identification and prevention of human CCFs originating from modifications and maintenance

Kari Laakso
VTT Industrial Systems
FIN– 02044 VTT

Abstract

The focus in human reliability analysis of nuclear power plants has traditionally been on human performance in disturbance conditions. On the other hand, human maintenance failures and design deficiencies, remained latent in the system, have an impact on the severity of a disturbance, e.g. by disabling safety-related equipment on demand. Especially common cause and other dependent failures of safety related systems can affect the core damage risk to a significant extent. The topic has been addressed in Finnish studies, where experiences of latent human errors have been searched and analysed in detail from the maintenance history of the both NPP sites.

The analysis of this maintenance and operating experience from the power plant information systems at the both sites shows that most errors stem from the refuelling and maintenance outage periods. The analysis also shows that less than half of the dependent errors remained latent after start-ups from outages to the power operating periods. The causes of these failures have often been complex event sequences, involving human and organisational factors. The “missed detection events”, i.e. CCFs which have passed inspections and functional tests to the operation, have been analysed and classified systematically and documented as event reports.

The review of the bulk of the identified and analysed single and multiple errors of the both NPP sites showed that the instrumentation & control and electrical equipment are more prone to human error caused failure events than the other maintenance objects. The classification and review of all the analysed multiple errors showed that plant modifications and difficulties in planning of maintenance and operability verification were significant sources of common cause failures. The most dependent human errors originating from modifications could be reduced by a more tailored planning and coverage of their start-up testing programs. Improvements could also be achieved by identification of those complex repair and preventive maintenance works which are prone to errors or to cause small changes in the system. Such cases in important equipment require a planning of tailored or larger coverage of installation inspections and functional testing.

Methods for analysis and classification of maintenance history information, examples of presentation of the analysis results and a number of conclusions and recommendations for identification and prevention of latent human common cause failures, are be described in this paper.
Foreword

These studies have been performed within the Finnish research programmes on nuclear safety and financed by the Finnish Radiation and Nuclear Safety Authority (STUK) primarily and secondarily by the Ministry of Trade and Industry (KTM).

We are thankful to the maintenance, operation, safety and reliability personnel of the utilities Teollisuuden Voima Oy and Fortum Generation, who have provided the maintenance history data and participated constructively in the interviews, analyses and work meetings during the studies. As well we are thankful to the STUK experts who have supported the studies by their safety knowledge and operational experience in commenting the methods and analyses prepared during the study.

List of contents

Abstract.......................................................................................................................... 1
Foreword......................................................................................................................... 2
List of contents.............................................................................................................. 2
List of Figures.............................................................................................................. 2
List of Tables.............................................................................................................. 2
1. Introduction............................................................................................................. 3
2. The scope of the studies of human common cause failures in relation to maintenance activities........................................................................................................ 3
3. Search, classification and analysis methods of single and multiple errors.............. 4
4. Review and results from the bulk of error and event analyses.................................. 9
5. Proposals and recommendations on remedial actions and practises....................... 13
References..................................................................................................................... 16

List of Figures

Fig. 1. Equipment types involved in single human errors in relation to maintenance........ 9
Fig. 2. Distribution of human common cause failures among equipment types............. 10
Fig. 3. Distribution of the types of erroneous tasks leading to common cause failures...... 11
Fig. 4. Distribution of the fault detection states of the human common cause failures born during a maintenance outage................................................................. 11
Fig. 5. Weakness identified in operative defensive barriers against common cause failures. 12

List of Tables

Table 1. Cause coding of failures at a NPP work order system.................................... 4
Table 2. Coding of probable time of failure entry at a NPP work order system............... 5
Table 3. A classification of human errors effects on equipment level in relation to maintenance............................................................... 5
Table 4. Classification and definition of root causes of multiple human errors in relation to maintenance................................................................. 6
Table 5. An example of a maintenance event report.................................................... 8
1. Introduction

The focus in human reliability analysis of nuclear power plants has traditionally been on control room operator performance in disturbance conditions. In the area of maintenance activities, the emphasis has been on human reliability of non-destructive inspections. On the other hand, incidents have shown that errors related to maintenance, which have taken place earlier in plant history, may have an impact on the severity of a disturbance, e.g. by disabling safety related equipment.

The causes of these failures have often been complex event sequences, involving human, organisational and technical factors. Especially common cause and other dependent failures of safety systems may significantly contribute to the reactor core damage risk. The topic has been addressed in the Finnish studies of human common cause failures, where experiences on latent human errors have been searched and analysed in detail from the maintenance history. In the Finnish projects, one aim has also been to promote the studies of human factors related to maintenance [Oedewald & Reiman 2002].

2. The scope of the studies of human common cause failures in relation to maintenance activities

Pilot case studies for identification and analysis of human common cause failures in relation to the maintenance activities from maintenance history in the plant information systems have been conducted for both Finnish nuclear power plant sites. Apart from the safety systems, this study focuses thus to other systems of the plant units also due to the fact that human error mechanisms may be the same. Also a more extensive database will be obtained, and all from the risk point of view significant systems are not classified as safety systems.

The analysis of the Olkiluoto units 1 and 2 three-year experience during 1992–1994 covered 4400 fault repair work orders. Totally 334 human error cases were identified and among them the number of single errors was 206. The number of dependent human error event cases derived and analysed was 14. In the corresponding study of the Loviisa nuclear power plant units 1 and 2 maintenance history during 1995-1997, the number of fault repair work orders was 14091. The number of single errors identified was 149 and dependent human error cases identified and analysed was 34 [Laakso & Saarelainen, 2003].

The numbers of the different plant sites are not directly comparable because in the Olkiluoto case all the 4400 fault repair work orders were studied but the scope of the examined work orders was limited in the Loviisa plant case by creating a data screening procedure. The screening procedure had a hit rate of 2/3 in error identification in the detailed analysis of the studied fault work orders.

The analysis results of the Olkiluoto plant study and recommendations of actions were summarised and published in 1998 [Laakso, Pyy & Reiman 1998]. The other aim of the Olkiluoto analysis work was to support PSA be extending the applicability of
human reliability analysis to study of the effects of wrong human actions in relation to maintenance [Pyy 2000].

3. Search, classification and analysis methods of single and multiple errors

The power plant information systems in Finnish NPPs include work planning and fault, maintenance and operation place histories. The experience data is well documented and has a good coverage from the 80’s. The documentation and classification of the fault and repair history information is performed by the maintenance and operation personnel. Most of the plant personnel use these plant information systems.

Within the Olkiluoto and Olkiluoto plant case studies detailed classification models for human errors related to maintenance activities were developed and adopted for a trial use. The purpose of the new classification models was to provide an enhanced basis for identification, appearance and statistical analysis of human and also quality errors related to maintenance activities, and especially of human CCF events, utilising the maintenance work order database.

The original cause coding for the failure and repair work orders used at the Loviisa nuclear power plant (coding being rather similar with corresponding coding at the Olkiluoto plant) is shown in Table 1.

**Table 1. Cause coding of failures at a NPP work order system.**

<table>
<thead>
<tr>
<th>A</th>
<th>EQUIPMENT AND DESIGN</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td>Design</td>
</tr>
<tr>
<td>AB</td>
<td>Material</td>
</tr>
<tr>
<td>AC</td>
<td>Manufacturing</td>
</tr>
<tr>
<td>AD</td>
<td>Installation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C</th>
<th>CONSEQUENCE OF OPERATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>Exceeding a limit value</td>
</tr>
<tr>
<td>CB</td>
<td>Over-stressing</td>
</tr>
<tr>
<td>CC</td>
<td>Blockage, sediment, stagnation</td>
</tr>
<tr>
<td>CD</td>
<td>Foreign objects</td>
</tr>
<tr>
<td>CE</td>
<td>Normal wear of lifetime</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B</th>
<th>PERSONNEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>BA</td>
<td>Control or operational error</td>
</tr>
<tr>
<td>BB</td>
<td>Wrong setting or control</td>
</tr>
<tr>
<td>BC</td>
<td>Maintenance or repair error</td>
</tr>
<tr>
<td>BD</td>
<td>Lack of or delayed action</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D</th>
<th>MISCELLANEOUS CAUSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DA</td>
<td>Cascade failure</td>
</tr>
<tr>
<td>DB</td>
<td>External cause</td>
</tr>
<tr>
<td>DC</td>
<td>Deficient work order or instruction</td>
</tr>
</tbody>
</table>

Z OTHER (give extra description)

For the classification of failures and repairs in electrical and instrumentation equipment, some additional cause codes e.g. “BE = human error” and “CG = Break, connection fault” have been recently added to the example coding list.
One specific and useful feature in the maintenance history reporting in one of the plants, the Loviisa plant, is that a classification is performed also with respect to the probable entry of the failure, see Table 2.

Table 2. Coding of probable time of failure entry at a NPP work order system.

<table>
<thead>
<tr>
<th>Code</th>
<th>Time of Failure Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Before previous test</td>
</tr>
<tr>
<td>02</td>
<td>Before previous maintenance or repair</td>
</tr>
<tr>
<td>11</td>
<td>During previous test</td>
</tr>
<tr>
<td>12</td>
<td>During previous maintenance or repair</td>
</tr>
<tr>
<td>13</td>
<td>During previous operation</td>
</tr>
<tr>
<td>21</td>
<td>After previous test</td>
</tr>
<tr>
<td>22</td>
<td>After previous maintenance or repair</td>
</tr>
<tr>
<td>23</td>
<td>After previous operation</td>
</tr>
<tr>
<td>31</td>
<td>Immediately before detection</td>
</tr>
<tr>
<td>32</td>
<td>After previous shift walk-around</td>
</tr>
</tbody>
</table>

The above coding (especially 12) in Table 2 helped us to identify a subgroup of failures with a probable failure origin in previous maintenance or repair.

In a detailed review of the failure and repair feedback reporting classified like so, a number of maintenance and modification related errors, and weaknesses in work planning could be retrieved. This first screening phase of the errors was performed by comparing the written descriptions on symptoms, causes and actions with the given cause classification codes (in Table 1) in the single work orders. Almost all the identified single and multiple human failures had been cause classified to originate from installation, wrong setting or control, maintenance or repair error, and human error. After that all the failure and repair reports belonging to these four cause coding classes, plus those coded as probably introduced during previous maintenance or repair, were selected as candidates for further study. After the review and discussion of the example human errors and the screening method with the plant maintenance planning staff and experts at the regulatory body the all screened error candidates were decided for further study.

In connection to review and preliminary verification of the dominating human error classes from the maintenance history, the classifications systems of both single and multiple human errors were developed. The developed new classification models of human and quality errors related to maintenance were firstly tested and verified in identification and review of a subset of the human errors with the plant maintenance and safety staffs and refined during the case studies. Mainly, the idea at later study on the Loviisa plant was to identify and verify the time and nature of the error origin in a more detailed way than in the earlier Olkiluoto case. The later advancements of the classification models of maintenance related human errors have been applied only for the Loviisa plant. The used error classification in Table 3 structures and shows how human error effects appear on equipment level.

Table 3. A classification of human errors effects on equipment level in relation to maintenance.
Errors of Omission (missing human action)

1. Restoration errors after work, such as omission of the realignment of process or instrument valves, disconnectors, breakers, fuses or limit settings.
   Omission of refilling of fluid or gas into lines, tanks or drainings.
2. Cables or electronic components not connected, settings or adjustments omitted.
   Omission to install packing or control component.
3. Foreign objects or impurities left behind inside the object of the work. Examples are dirt, garbage, tools, scaffolds or covering material.

Errors of Commission (wrong human action)

Wrong order or direction.
4. Wrong order, such as cables or instrument pipelines crosswise connected.
5. Wrong direction, such as reversed or twisted installation of valve or another sub-component. Wrong positioning of valve.

Wrong selection.
6. Wrong place or object, such as cabling fixed on wrong connection, setting of wrong tripping conditions or draining of wrong pipeline. Item installed on wrong equipment place.
7. Wrong or mixed parts, materials, tools, fluids or chemicals selected for work.

Wrong settings/adjustments/calibrations.
8. Wrong settings of trip limits, limit switches, reference, indication or time delay values, or of adjusting devices. Deficient alignment of shaft, stem/spindle or pipe. Wrong setting of pipe support.

Other quality problems.
9. Too little force, e.g. loose connections of bolts, nuts, cables or sensors,
10. Too much force, e.g. excessive tightening or greasing,
11. Damaging other equipment e.g. cabling, cable trays or small diameter piping by falling material or slugging/contacting. Can be due to carelessness and narrow spaces for work or transport.
12. Other carelessness (if 1-11 are not applicable). E.g. worn tools, falling, deficient weld, solder joint or insulation. Unclear trips initiated during testing, installation or maintenance, wrong subtitling or recording, wrong timing.

In the detailed analysis of the fault repair work orders the single human errors were classified according to following explaining factors: Equipment type influenced by error, direct error effects (see Table 3), plant operating state at failure detection, how failure was detected, erroneous task (and related plant state and time instant) and whether the error was single or multiple (HCCF).

Apart from the observed and direct error effects on equipment, also the underlying contributing factors analysed and classified for the dependent human errors according to another new classification. The root causes of the multiple errors (HCCFs) could be assigned to one of the following groups:

Table 4. Classification and definition of root causes of multiple human errors in relation to maintenance.
1. **Maintenance and operability planning deficiency:**
   Incorrect, incomplete or unclear maintenance or maintenance or operability verification planning, in such as maintenance, repair, installation inspection or functional testing phases. Deficiencies in coverage of start-up tests or installation inspections of modifications. Deficiencies in procedure, work order, operation order or definition of work scope.

2. **Design deficiency:**
   Error or deficiency in design or documentation of modification, equipment, system, installation or computer program. Documentation not updated to correspond changes.

3. **Violation of procedure or order:**
   Violation due to insufficient knowledge or poor information. Deviations from procedure or order due to gradual organisational learning of “bad habits”. Or conscious violation.

4. **Poor co-ordination, supervision or information transfer:**
   Poor project co-ordination or supervision of subcontractors, poor information transfer due to organisational changes or boundaries. Or weaknesses in experience feedback such as recurrence of events with known phenomena. Or poor quality control.

5. **Insufficient knowledge:**
   Lacking training, specialist or cross-functional knowledge.

A good quality of the maintenance history data in the plant information system is helpful in the identification and analysis of errors and missed detection opportunities, e.g. deficient operability verifications. A structured classification and systematic analysis helps the identification and analysis of the errors which have penetrated the barrier functions such as functional or visual installation inspections or functional tests and thus resulted in latent faults.

One target of the study was to identify the dependent human error mechanisms and search for causes of missed detection of the errors in the operative and organisational defensive barriers. This analysis was done in interaction with plant maintenance and operability experts based on analysis of the maintenance history information. The analysis facilitated to capture the tacit knowledge of the equipment place history before the fault detection and of the of the plant experts to close the feedback loop of operating experience.

The identified dependent human errors were analysed and summarised in condensed maintenance event reports including a qualitative description of the:

- multiple error and its failure consequence,
- originating erroneous or defective work task, e.g. in maintenance or modification design, and
• primary missed opportunity for detection, e.g. deficiency in operability verification, allowing the errors or faults to remain latent in the system throughout the testing and start-up program at the end of the maintenance outage or during extended time periods.

One of the maintenance event reports prepared during the studies is given as an example in Table 5.

Table 5. An example of a maintenance event report.

<table>
<thead>
<tr>
<th>Identifier marking</th>
<th>Work order time and number</th>
<th>Title and description of event</th>
<th>Operating event identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1HCCFYP 12</td>
<td>1996-10-08</td>
<td>Deficient adjustment and testing of the actuators as implementing new motor operated blowdown valves in the pressurizing system</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>238769D, 238769A, 238769B, 238769C</td>
<td>The gate valves 12YP12S038, 12YP12S039, and 11YP12S036, 11YP12S037 were not tight in hot state during power operation 1996-10-08. New motor operated gate valves (MOVs) had been installed during the preceding maintenance outage in September 1996. - The MOVs had to be closed as a corrective action by manual operations from the switch-gear during the power operation state at 1996-10-09. - The common cause setting errors had passed from the maintenance outage through to the power operation period, because the setting of the limit and torque switches of the MOVs in the cold state only was insufficient as start-up testing of the modification work.</td>
<td></td>
</tr>
</tbody>
</table>

As can be seen from the above example maintenance event report, a combination of several fault repair work orders is needed for identification of common cause failures. In the studies, in average about two fault repair work orders where faults had been detected within the time frame of the surveillance testing interval, had to be combined to build up a CCF event. But some CCFs could be identified from single fault repair work orders, too.

In addition to the basic classification of single human errors, the human CCFs were additionally classified with respect to the missed detection of the errors in operative or organisational defensive barriers and their root causes (see Table 4).
The bulk of the identified multiple human errors (HCCFs), as well as single human errors, were statistically treated based on their classification classes. Also the quantitative occurrence of the errors within groups of the classification classes such as combinations of equipment and error types, equipment and root cause types, and erroneous task and missed barrier types etc were studied in order to identify possible dominating problem areas. The deviating problem area candidates were then reviewed qualitatively in order to identify significant opportunities for remedial actions or practises.

4. Review and results from the bulk of error and event analyses

According to the review of the analysis results of the bulk of the error events at the both plant sites, the instrumentation & control (IC) and electrical equipment were noticed to be more prone to human error caused failure events than the other maintenance objects.

![Fig. 1. Equipment types involved in single human errors in relation to maintenance.](image)

It should be noticed that the single and more rare errors influencing the safety related mechanical equipment can however be serious and have also caused forced plant outages in Finnish nuclear power units.
Fig. 2. Distribution of human common cause failures among equipment types.

It should also be noted that the common cause failures have been divided into functionally critical human common cause failures (HCCFs) and common cause non-critical failures (HCCNs). The HCCNs can be regarded as an early warning of causes or mechanisms leading otherwise or in higher plant operational states to HCCFs.

The identification of the dominating portion of the IC involved in single and multiple human failures does not depend on the IC's error proneness only, but also on the high number of the IC maintenance objects, and the evident functional effects on the equipment and systems of such errors on IC.

But this result emphasizes as an example the responsibility and requirements of both the versatility and specialisation of the design, maintenance and operability planning, as well as the instrument mechanician's skills and knowledge of work, on IC and automation.

The sources of the multiple errors could be searched in expert sessions at the plants from the plant information systems where the probable origin of the human failures was identified and evaluated by examining the earlier tasks from the work order history of the concerned equipment operation places. In a number of the analysed multiple error events the plant modifications appeared to be the origin, but also the predetermined preventive maintenance was found to be a significant source of common cause failures, see Figure 3.
Fig. 3. Distribution of the types of erroneous tasks leading to common cause failures.

The review of the analysed set of single and multiple human errors (HCCFs and HCCNs) at the both sites showed that most errors in relation to maintenance stem from the refuelling and maintenance outage period. This is a natural result because the dominating part of the modifications, preventive maintenance and repairs are performed during the annual maintenance outages. Distribution of the plant operational states, where the common cause failures originating from maintenance and modifications during the refuelling and maintenance outages, is shown in Figure 4.

Fig. 4. Distribution of the fault detection states of the human common cause failures born during a maintenance outage.

The more on left in the Figure 4 the operational states of the detection of the multiple failure events are, the better is the maintenance planning and operability verification.

The analysis shows that less than half of the multiple human errors (HCCFs) remained latent after start-ups from outages to the power operating periods at the
both sites. At the first site about a third of the multiple failures were identified during the same outage. At the second site about 40 percent of the multiple failures were detected during the outage or the following plant start-up to the power operation period. The contents of the figure 4 can represent a direct performance indicator of the quality and outcome of the maintenance and operability verification planning at the plants.

The review of the broken barriers in analysed set of human common cause failures showed that the most missed primary opportunities for detection were in the installation checks and inspections, start-up testing and functional testing. Installation inspections, and start-up and functional tests were thus identified as the most significant contributors to weaknesses in the operative defensive barriers against common cause failures, see Figure 5.

![Fig. 5. Weakness identified in operative defensive barriers against common cause failures.](image)

The review of the root causes of all analysed human common cause failure events shows also that planning of maintenance, work phases and operability verification are very demanding tasks due to the complex planning environment of different objectives, safety requirements and instructions, and needs of multifunctional plant technical, maintenance and operability knowledge.
5. Proposals and recommendations on remedial actions and practises

In the following, a number of recommendations and proposals for remedies and improvements are presented based on the conclusions related to and findings from the studies.

Planning of maintenance and operability. Development needs have been identified in maintenance and operability planning. The most dependent human errors originating from modifications, e.g. renewals of actuators, motor operated valves, solenoid valves, transformers, etc. could be reduced by a more tailored specification and coverage of the related start-up testing programs. In planning the test arrangements at least the component and system level testing needs, real operating conditions and multiple train risks, should be evaluated. Improvements could also be achieved by a more case specific planning of the installation inspections of instrumentation, automation and electrical equipment in complicated maintenance works and in modifications.

A more agile initiation of necessary adjustments to the pre-planned work orders to correspond specific local conditions identified by maintenance personnel at work would also help. At planned maintenance or installation works, additional disconnection of cables or actuators have proven necessary to facilitate maintenance or installation of other equipment, but the increased needs of installation inspections or testing were not post-planned during the work orders in some common cause failure cases.

Generally the analysis results show that maintenance and operability planning should not be regarded as separate functions but performed better as an integrated planning activity.

Grading of planning requirements. Grading the planning requirements of the maintenance work objects based on their safety and availability importance or work complexity would also prioritise the resource allocation for planning and select the work orders and plans which could be reviewed before the work permit. For instance the complex repairs should be identified in planning and one should evaluate, if the repairs are prone to errors or could imply small modifications in the equipment or system? Such cases in important equipment would require a larger or tailored coverage of installation inspections and functional testing.

Experience based RCM planning. The maintenance strategies and actions covering the equipment operating places and systems can be selected by the experience based RCM planning approach. In the maintenance planning method, the operability requirements of the equipment are graded based on their importance. In the operating plants, the method utilises the maintenance history data in the planning of changes into the actions and intervals of the maintenance programs, including small redesigns, to reach the operability and maintenance objectives. Identification of effective actions for detection and prevention of common cause failures and operability verification of important equipment should be integrated to the planning approach.

Use of condition monitoring for operative maintenance steering. An increased use and analysis of existing condition monitoring information have a great potential in
increasing condition based maintenance. A combined strategy of condition based and predetermined preventive maintenance can be applied for very important equipment to reduce functionally critical failures and damages. Another realistic aim of the analysis of condition monitoring information is to reduce the number of error prone predetermined maintenance and disassembling maintenance actions. A case specific maintenance steering of corrective actions against degradations in equipment performance or operability would also contribute to a better utilisation of the personnel expertise and equipment responsibility.

**Decision of modifications.** A modification in an operating plant should be considered as a risk. Thus modifications in old plants should always be very well justified. A high number of thousands of technical modifications were implemented at the studied sites during the analysis periods. It is difficult to cover all latent functional relationships, failure modes and effects of modifications without a well planned and comprehensive start-up testing program. Modifications which are needed for providing significant safety, reliability, capacity, efficiency or maintainability remedies of shortcomings or enhancements, including related auxiliary system changes, are naturally justified. As well, the obsolete technology which exhibits missing spares and know-how has to be replaced. However to select the best decision option, a risk evaluation of e.g. teething problems in design and operation of the modification should be included in the decision criteria.

**Understanding the maintenance and operability verification process.** Modelling of the maintenance and operability verification process including the organisational interfaces, and covering both the small modifications and maintenance, is recommended. The errors, their progress, missed detection and occurrence of the common cause failures could be compared with the process models and be made visible in them. The modelling would help to increase the understanding of the planning and work order practises and identify and visualize the weaknesses requiring remedies in the process.

**Turn-over procedures.** Distinct turn-over and acceptance procedures of the technical modifications and their documentation between the project phases design, installation, start-up testing and operation, and simultaneously between the responsible organisational units (mostly internal suppliers to internal customers) are recommended for consideration. Such acceptance procedures have been applied for the technical systems during the installation and start-up testing phases in the latest Nordic BWRs. These procedures would help as organisational defensive barriers against unfinished modifications and deficient procedures or documentation passing through into operation.

**Identification and event analysis of common cause failures.** A proposal has been done to complement the failure and repair work order feedback data (on the screen of the power plant information system) by a question and relevant text description of a suspected common cause failure. This enhancement on the fault repair work order feedback has been introduced at one of the sites. This routine would help to operatively identify CCFs earlier and better from the plant information system and to start continuous CCF event investigations for their prevention in the future.
Training. The event analyses of latent maintenance related multiple errors would also provide a good plant-specific material for training of the maintenance, operability and technical personnel.

Living PSA. A check of the coverage of the identified multiple human errors in the common cause failure models and data in the PSA studies of today is also recommended.

Concluding remarks. Although the studied events suggest negative experience, experts and managers in the nuclear power plants and regulatory body view them as extremely valuable for experience feedback and the development of safety, operability and control of maintenance. The feedback from discussions of the analysis results with plant experts and professionals is still crucial in developing the final conclusions and recommendations that meet the specific development needs of actions and practises at the plants. The aim is to turn the negative experiences of failures and errors into so uneventful operation as reasonably practicable. Learning from one’s experienced errors is the best way to learn for the actors.
References


LOTI. Loviisa power plant information system. Brochure 4 p. For further information contact Fortum Power & Heat Oy. Loviisa nuclear power plant. FIN-07900 Loviisa, Finland.


Analysis of maintenance history for identification and prevention of human CCFs originating from modifications and maintenance

Kari Laakso
VTT Industrial Systems
FIN– 02044 VTT

• Introduction
• Scope of the studies
• Basic terms and definitions
• Search, classification and analysis methods
• Review of the bulk of error and event analyses
• Proposals and recommendations on remedial actions and practises.
Introduction and Background.

• Focus in human reliability analysis of NPPs has traditionally been on control room operator performance in disturbance conditions.
• But incidents have shown that errors related to maintenance, which take place earlier in plant history, may have an impact on the severity of a disturbance, e.g. by disabling safety related equipment.
• This problem was addressed in Finnish studies of human originated common cause failures, where experiences on latent human errors have been searched and analysed from the maintenance history.

Scope of the studies of human originated common failures in relation to maintenance activities

• The aim of the studies was identification and analysis of human originated common cause as well as single failures in relation to the maintenance activities
• An analysis using the maintenance history in the plant information systems was done with both Finnish nuclear power plant sites.
• The NPPs are Loviisa PWR and Olkiluoto BWR.
• The number fault repair work orders (WO) covered were:
  • 14091 WOs in Loviisa units 1 and 2 covering 1995-1997,
Power plant information systems

- The information systems in Finnish NPPs include work planning and management plus fault, maintenance and operation place histories.
- This experience feedback data is rather well documented and has a good coverage from the 80's.
- The feedback documentation and classification of the fault and repair history information is performed by the maintenance and operation personnel.
- Most of the plant personnel use these plant information systems (ERP systems).

Work order history data in the plant information systems being object for the studies

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Plant units I &amp; II</th>
<th>Plant units 1 &amp; 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of repair WOs</td>
<td>4400</td>
<td>14091</td>
</tr>
<tr>
<td>Number of PM actions</td>
<td>9469</td>
<td>27769</td>
</tr>
<tr>
<td>Number of modifications</td>
<td>1084</td>
<td>2715 (CM + KM)</td>
</tr>
<tr>
<td>Number of marked equipment places</td>
<td>~50000 *)</td>
<td>~70000 *)</td>
</tr>
</tbody>
</table>

Kari Laakso, VTT/TUO, 7.10.2003
An example analysis of a human error in relation to maintenance from fault repair feedback data.

<table>
<thead>
<tr>
<th>Equipment place</th>
<th>Failure report number</th>
<th>Date</th>
<th>Explanation</th>
<th>Plant state at the time of error</th>
<th>Equipment code</th>
<th>Case</th>
<th>Case effect</th>
<th>Case duration</th>
<th>Additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.327062</td>
<td>124821 (03850)</td>
<td>07.06.1992</td>
<td>Circuit card 6.058.326 failed and damaged mechanically in a modification task</td>
<td>SHUT</td>
<td>IC</td>
<td>BF</td>
<td>DCF</td>
<td>14.5.92</td>
<td>Maintenance event analysis 26ecE2D1.0Ac</td>
</tr>
</tbody>
</table>

Coding in a repair work order of the probable time of failure entry

- Undefined
- 01 Before previous test
- 02 Before previous maintenance or repair
- 11 During previous test
- 12 **During previous maintenance or repair**
- 13 During previous operation
- 21 After previous test
- 22 After previous maintenance or repair
- 23 After previous operation
- 31 Immediately before detection
- 32 After previous shift walk-around
**Cause coding***) of fault repair work order feedback at a plant information system

<table>
<thead>
<tr>
<th>A EQUIPMENT AND DESIGN</th>
<th>C CONSEQUENCE OF OPERATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA Design</td>
<td>CA Exceeding a limit value</td>
</tr>
<tr>
<td>AB Material</td>
<td>CB Over-stressing</td>
</tr>
<tr>
<td>AC Manufacturing</td>
<td>CC Blockage, sediment, stagnation</td>
</tr>
<tr>
<td>AD Installation</td>
<td>CD Foreign objects</td>
</tr>
<tr>
<td></td>
<td>CE Normal wear of lifetime</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>B PERSONNEL</th>
<th>D MISCELLANEOUS CAUSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>BA Control or operational error</td>
<td>DA Cascade failure</td>
</tr>
<tr>
<td>BB Wrong setting in control</td>
<td>DB External cause</td>
</tr>
<tr>
<td>BC Maintenance error</td>
<td>DC Deficient work order or instruction</td>
</tr>
<tr>
<td>BD Lack of or delayed action</td>
<td>Z OTHER (give extra description)</td>
</tr>
</tbody>
</table>

*) Additional cause codes BE = human error, and CG = break, connection fault have recently been added to the cause classification list based on experiences related to IC and electrical equipment.

---

**Overview of the single and multiple error analyses and related analysis data bases prepared for one plant**

- 232 reports showing errors
- 149 fault repair work order feedback reports (selected error candidates)
- 113 reports Other than human error screened out
- 345 fault repair work order feedback reports (selected error candidates)
- Analysis and classification of single errors, combination into common cause failures, and determination of error origin from earlier work orders of the same equipment places or trains
- 83 error analysis reports covering dependency cases
- Event analyses and reports of CCPs (incl. identification of root causes and broken barriers)
- HCCF and HCCN event analysis bases
- Human shared equipment faults (dependencies)

Kari Laakso, VTT/TUO, 7.10.2003
Human error

- A failure of a human action due to human error mechanisms which cause an unintended result.
- For example, an omission of the realignment of process or instrument valves, after the maintenance work causes a failure of the physical item to perform its function.
- For example, instrument pipelines of pressure difference measurements are connected crosswise due to deficient documentation, knowledge or carelessness, and the connections are not correctly checked during the work.
- In some sources, human errors are further divided, e.g., into slips, lapses, mistakes, violations, omissions and commissions [see e.g. Swain & Guttman 1983, Reason 1990].

Common cause failures (CCFs)

- Common cause failure. Common cause failures (CCF) are similar failure causes or mechanisms, that may apparently result or have resulted in multiple functionally critical failures in redundant components in real demand situations (are unable to perform their required function).
- Common cause non-critical failure. Common cause non-critical failures (CCNs) are similar causes or mechanisms which result simultaneously in lack or deficiency of functionally non-critical requirements of redundant components. If getting worse or propagating, these precursors can develop into common cause failures. CCNs are early warnings of similar causes or mechanisms otherwise leading to functionally critical CCFs.
An example of a latent multiple error in relation to maintenance, HCCN

<table>
<thead>
<tr>
<th>Dependent error id. marking</th>
<th>Work order time (number)</th>
<th>Title and description of event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1HCCNRC51</td>
<td>19950628 (220691A)</td>
<td>Temperature measurements 1ORC51T001 and T002 crosswise connected in repair. The temperature measurements 1ORC51T001 and 1ORC51T002 after the parallel ejectors 1ORC51N001 and 1ORC51N003 of the steam dumping line 1ORC51Z of the condenser indicated too much. The reason of wrong indications was crosswise connection of the temperature measurements in the previous repair during operation. - The cause of the wrong crosswise connection was wrong cable marking at the down lead box. - The wrong order of the cables had passed through the installation inspections of the automation repair and remained latent about two years.</td>
</tr>
</tbody>
</table>

Kari Laakso, VTT/TUO, 7.10.2003

A classification of human errors in relation to maintenance. Effects on equipment level.

- Errors of Omission (missing human action)
  
  - 1. Restoration errors after work, such as omission of the realignment of process or instrument valves, disconnectors, breakers, fuses or limit settings. Omission of refilling of fluid or gas into lines, tanks or drainings.
  
  - 2. Cables or electronic components not connected, settings or adjustments omitted. Omission to install packing or control component.
  
  - 3. Foreign objects or impurities left behind inside the object of the work. Examples are dirt, garbage, tools, scaffolds or covering material.

Kari Laakso, VTT/TUO, 7.10.2003
Errors of Commission (wrong human action)

- **Wrong order or direction.**
  - 4. Wrong order, such as cables or instrument pipelines crosswise connected
  - 5. Wrong direction, such as reversed or twisted installation of valve or another sub-component. Wrong positioning of valve.

- **Wrong selection,**
  - 6. Wrong place or object, such as cabling fixed on wrong connection, setting of wrong tripping conditions, or draining of wrong pipeline. Item installed on wrong equipment place.
  - 7. Wrong or mixed parts, materials, tools, fluids, or chemicals selected for work.

Wrong human actions in relation to maintenance (cont.)

- **Wrong settings/adjustments/calibrations,**
  - 7. Wrong settings of trip limits, limit switches, reference, indication or time delay values, or of adjusting devices.
  - Deficient alignment of shaft, stem/spindle or pipe.
  - Wrong setting of pipe support.
Wrong human actions in relation to maintenance (cont.)

- Other quality problems.
  
  - 9. Too little force, e.g. loose connections of bolts, nuts, cables or sensors,
  - 10. Too much force, e.g. excessive tightening or greasing,
  - 11. Damaging other equipment e.g. cabling, cable trays or small diameter piping by falling material or slugging/contacting. Can be due to carelessness and narrow spaces for work or transport.
  - 12. Other carelessness (if 1-11 are not applicable). E.g. worn tools, falling, deficient weld, solder joint or insulation. Unclear trips initiated during testing, installation or maintenance, wrong subtitling or recording, wrong timing.

Kari Laakso, VTT/TUO, 7.10.2003

Dependent human errors were summarised in condensed Maintenance Event Reports

Reports include a qualitative description of:

- multiple error and its failure consequence,
- originating erroneous or defective work task, e.g. in maintenance or modification design, and
- primary missed opportunity for detection, e.g. deficiency in operability verification, allowing the errors or faults to remain latent in the system throughout the testing and start-up program at the end of the maintenance outage or during extended time periods.

Kari Laakso, VTT/TUO, 7.10.2003
An example of a Maintenance Event Report

<table>
<thead>
<tr>
<th>Identifier marking</th>
<th>Work order time and number</th>
<th>Title and description of event</th>
<th>Operating event identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>IHCCFYP 12</td>
<td>1996-10-08</td>
<td>Deficient adjustment and testing of the actuators as implementing new motor operated blowdown valves in the pressurizing system</td>
<td>No</td>
</tr>
</tbody>
</table>

- The gate valves 12YP12S038, 12YP12S039, and 11YP12S036, 11YP12S037 were not tight in hot state during power operation 1996-10-08.

- New motor operated gate valves (MOV) had been installed during the preceding maintenance outage in September 1996.

- The MOVs had to be closed as a corrective action by manual operations from the switch-gear during the power operation state at 1996-10-09.

- The common cause setting errors had passed from the maintenance outage through to the power operation period, because the setting of the limit and torque switches of the MOVs in the cold state only was insufficient as start-up testing of the modification work.

Kari Laakso, VTT/TUO, 7.10.2003

Classification and definition of root causes of multiple human errors related to maintenance.

1. Maintenance and operability planning deficiency:
   Incorrect, incomplete or unclear maintenance or maintenance and operability verification planning, in such as maintenance, repair, installation inspection or functional testing phases.
   Deficiencies in procedure, work order, operation order or definition of work scope.

2. Design deficiency:
   Equipment, system, or computer program.

3. Violation of procedure or order:
   Violation due to insufficient knowledge or poor information. Deviations from procedure or order due to gradual organizational learning of "bad habits". Or conscious violation.

4. Poor co-ordination, supervision or information transfer:
   Poor project co-ordination or supervision of subcontractors, poor information transfer due to organizational changes or boundaries. Or weaknesses in experience feedback such as recurrence of events with known phenomena. Or poor quality control.

5. Insufficient knowledge:
   Lacking training, specialist or cross-functional knowledge.

Kari Laakso, VTT/TUO, 7.10.2003
Reviewing the bulk of the analyses of single errors in relation to maintenance

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IC</td>
<td>10</td>
<td>10</td>
</tr>
<tr>
<td>EL</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>MEC</td>
<td>15</td>
<td>25</td>
</tr>
<tr>
<td>VAL</td>
<td>25</td>
<td>15</td>
</tr>
<tr>
<td>IVAL</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

IC = Instrumentation & control equipment or software, EL = Electrical equipment, MEC = Mechanical equipment, VAL = Process valves, ventilation dampers or channel hatches, IVAL = Block or primary valves in instrument lines, RM = Radiation monitoring equipment.

Kari Laakso, VTT/TUO, 7.10.2003

Reviewing the bulk of the analyses of common cause failures in relation to maintenance

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IC</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>EL</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>MEC</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>VAL</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>IVAL</td>
<td>12</td>
<td>12</td>
</tr>
</tbody>
</table>

IC = Instrumentation & control equipment and software, EL = Electrical equipment, IVAL = Block or primary valves in instrument lines, RM = Radiation monitoring equipment.

Kari Laakso, VTT/TUO, 7.10.2003
Distribution of the types of erroneous tasks leading to common cause failures.

**TVO 1 & 2.** Erroneous task types of dependent human errors

- **Functional testing:** 13% (2 cases)
- **Modification:** 47% (4 cases)
- **Installation:** 13% (2 cases)
- **Repair:** 13% (2 cases)
- **Preventive maintenance:** 13% (2 cases)

**Lovisa 1 & 2.** Erroneous task types of dependent human errors

- **Installation:** 0% (1 case)
- **Repair:** 18% (6 cases)
- **Preventive maintenance:** 32% (11 cases)
- **Modification:** 41% (14 cases)

Kari Laakso, VTT/TUO, 7.10.2003
Weakness identified in operative defensive barriers against common cause failures.

Distribution of the fault detection states of the human common cause failures born during a maintenance outage.

Type of detection: testing or preventive maintenance (PREV), otherwise (OTH)
Operating states: power operation (POW), refueling outage prior to start-up (OUT), hot shutdown (HOT), cold shutdown (COLD), plant start-up (STOP), plant shutdown (SHDN)

Kari Laakso, VTT/TUO, 7.10.2003
Weaknesses in organisational barriers against human CCFs

Proposals and recommendations on remedial actions and practises

Planning of maintenance and operability

- Most dependent human errors originating from modifications, e.g. renewals of actuators, motor operated valves, solenoid valves, transformers, etc. could be reduced by a more tailored/focused specification and coverage of the start-up testing programs.

- In planning the test arrangements, at least the component and system level testing needs, real operating conditions and multiple train risks, should be evaluated.

- Improvements could also be achieved by a more case specific planning of the installation inspections of instrumentation, automation and electrical equipment in complicated maintenance works and in modifications.
Planning of maintenance and operability (cont.)

• At planned maintenance or installation works, additional disconnection of cables or actuators have proven necessary to facilitate planned maintenance or installation of other equipment, but the increased needs of installation inspections or testing were not post-planned to the work orders in some common cause failure cases. An agile initiation of necessary adjustments to the pre-planned work orders to correspond specific local conditions identified by maintenance personnel at work would help.

• Generally the analysis results show that maintenance and operability planning should not be regarded as separate functions but performed better as an integrated planning activity.

Proposal: Grading of planning requirements

• Grading the planning requirements of the maintenance work objects based on their safety and availability importance (~ maintenance classification) or work complexity would prioritise the resource allocation for planning. Also the important work orders and plans could be so selected for the review before the work permit.

• Complex repairs should be identified in planning and one should evaluate, if the repairs are prone to errors or could imply small modifications in the equipment or system? Such cases in important equipment would require a larger or tailored/focused coverage of installation inspections and functional testing.
Proposal: Turn-over procedures.

- Distinct turn-over and acceptance procedures of the technical modifications and their documentation between the project phases design, installation, start-up testing and operation, and simultaneously between the responsible organisational units are recommended for consideration.
- Such procedures would help as organisational defensive barriers against unfinished modifications and deficient procedures or documentation passing through into operation.

Identification and event analysis of common cause failures.

- A proposal has been done to complement the failure and repair work order feedback data (on the screen of the power plant information system) by a question and relevant text description of a suspected common cause failure.
- This routine would help the utilities to:
  - operatively identify CCFs earlier and better from the plant information system
  - start continuous CCF event investigations for their prevention and learning in the future.
- The aim of this R&D was also to generate a model for corresponding studies to be performed by utilities in the continuation.
Deploying an approach to socio-organisational and human impact (SOH) studies

CORPORATE CONTEXT

- **EDF Generation and Trading policy** is intent upon improving the way in which human factor is factored into operational activities and upgrades.

- **New expectations of** nuclear engineering support structures.

- **Weaknesses identified in providing guidance to** plants for implementation of changes.

- **Request from regulatory authority** for human factor to be incorporated into certain modification packages.

- **Managers with a purely technical background** have difficulty in forecasting impacts in the area of human factor.

- **Increasing number of requests for support** coming from plants.
EDF INVESTIGATION

- **CHALLENGES:**
  - IMPROVEMENT OF "PRODUCTS" DELIVERED TO SITES

- **OBJECTIVES OF PROJECT GROUP OVERSEEN BY THE CAPE:**
  - FACILITATE INCORPORATION OF SOCIO-ORGANISATIONAL AND human ASPECTS INTO PARK UPGRADES
    - Help those in charge of upgrade packages to conduct socio-organisational and Human impact studies
    - Assist in ensuring consistency of practices
    - Clarify responsibilities of various players

- **EXPECTED OUTCOME:**
  - SOH impact-study guide, endorsed by specific examples, with coaching provided to potential users.

---

**SOH METHOD AND SYSTEM**

*For what purpose? For whom? How?*

- **Help** to improve quality of products delivered to sites,

- **For** those in charge of upgrade packages,

- **By proposing** a tool to facilitate identification of SOH impacts:
  - Specifying areas concerned.
  - Providing an SOH impact-study method that can be adapted to user practices.
  - By identifying resources to provide support.
SCOPE OF THE GUIDE

The guide does not extend to:

• Design ergonomics
  (these guidelines already exist)

• Addressing and resolving problems

A 3-PART GUIDE
1: Users’ Instructions

- Reminder of principles on which to base impact studies
  - The impact study must be carried out at the very earliest during the strategic phase, and must be updated throughout the entire upgrade development process.

  - It applies to every strategy or solution being considered.

  - It brings together sites and support structures (expert analysis, HF, etc.)

  - Depending on the complexity and challenges associated with the issue in question, not all impacts need to be processed or given special attention.
MINIMISING THE IMPACTS OF A DISRUPTION

Socio-organisational and human impacts

Permanent activity

Design

Guidance and «coaching»

Initial activity

APPRAOCH TO SOH IMPACT STUDIES

Strategic phase

Implementation phase

Pilot unit

Extension to other plants

Decision → ADOPTED STRATEGY → CRAFT GUIDANCE

Guidance planning

Identification of impacts

Identification and processing of impacts for each strategy

S.O.H tools (CAPE)

Generic

Implementation of guidance phase

S.O.H update

D-day - 2 years

S.O.H extended across the board

SOH tool

(UNIPE)

S.O.H update

D-day - 6 months

Guidance provided to all plants
A THREE-PART GUIDE
2- Investigative framework

» Initiate investigation with maximum room for manoeuvre.

» Lines of enquiry are not restricted: this is not a check list.

» The study is embarked upon through one of two lines of enquiry:
  ➔ Organisational aspects
  ➔ social and human aspects

A THREE-PART GUIDE
3- Glossary of terms used

In order to:

- Facilitate comprehension of all those involved

- Promote a common understanding of terms and notions being conveyed
COACHING PRINCIPLES ADOPTED
FOR THE IMPLEMENTATION OF CHANGES:
Who needs to be coached?

- **Users** for whom an upgrade or development brings about a change in their duties, working methods or knowledge required to perform their job...

- **Plant management** and more especially, senior management

- **Engineering support** and more generally speaking, people who are actively involved in incorporating upgrades and who may serve as an interface in providing users with coaching and guidance

- **Contractors and designers.**

---

COACHING PRINCIPLES:
**Key points during implementation phase**

- **Specify type of guidance to be deployed** on the first plant, as well as the type of coaching that could be deployed for extension to other plants:
  - Adapt coaching to identified SOH impacts and challenges raised by the change in question
  - Determine what proportion of coaching is provided to engineering support/designer/site

- Collect **experience feedback from guidance** conducted for the initial upgrade.

- **Check that coaching has been given** and that it has been effective.
**APPROACH TO SOH IMPACT STUDY:**

**UNIPE guide**

- **CONTENT**
  - Identify impacts for each CRAFT/ORGANISATION

- **FORM**
  - Adapted to operational requirements, and therefore to users.
  - Craft and organisation-specific use

- **PROCESS**
  - ONE outline, regardless of phase.

- **ADAPTATION TO WORKING METHODS**
  1: Identify crafts and organisational structures,
  2: Answer general questions for each craft and organisation:
     - First stage: general section outline,
     - Second stage: general sub-section outline

---

**APPROACH TO SOH IMPACT STUDY:**

*Review and prospects*

- **Guide ownership**
  - By potential users
  - On cases currently being investigated

- **Initial experience feedback**
  - **Positive aspects** regarding changes in practices and the incorporation of human factor into upgrade packages.
  - **Weaknesses**: Guidance in need of improvement, delayed implementation within project groups, guide not sufficiently self-explanatory, etc.

- **Prospects**
  - **Analyse deficiencies** through a certain number of actions designed to make the SOH process sustainable for all upgrade packages handled by EDF Generation and Trading.
  - **Extend** the use of this approach to all products in step with the strategic phases of new upgrades
NEA / WGOE and SEGHOF and IAEA Workshop on Modifications at Nuclear Power Plants - Operating Experience, Safety Significance and Role of Human Factors 8-10. October 2003, Paris

The Swiss Modification Process in Nuclear Power Plants Regulatory Regime - Regulator/Operator process and Experience Related to Events with Safety Impact

Prepared by Herbert Deutschmann Swiss Federal Nuclear Safety Inspectorate
Abstract:
Modifications at NPPs are one of the important processes in regulatory and operator tasks for safe operation. Experience shows that many of the most significant Swiss events have their origin in previous modifications. The paper outlines the main Swiss regulatory guidelines and the regulatory body impact in the modification process. Examples of events related to plant modifications illustrate the importance of a systematic and comprehensive modification process.

Introduction
Failures were sometimes latent, over a long time. Important elements of the whole quality chain are the Quality Management Systems of the operators. The latter has also to control the activity of suppliers and manufacturers. The other important element is the regulation and the supervision by the regulatory body (RB), and their related organisations. The paper outlines the main Swiss regulatory guidelines and the RB impact, which depends on the safety impact of modifications and on the type of modifications (large or small, new technology or known standard technology). Experience shows that large modifications performed by qualified suppliers have resulted in few events, small modifications by plant personnel have led to significant events.

Derived from these events, the following proposals are made:

- Applying Human Factor principles should be an integral element of all modifications. Such principles should be defined in an IAEA safety guide or TECDOC.
- Using operating experience should also be a standard element in the modification process. A powerful computerised intelligent search tool to extract the relevant information from large databases (e.g. IRS) should be developed by related organisations.

Swiss Regulatory Regime Regarding Modifications in NPPs

Regulatory Guidelines
The Swiss Regulatory Guidelines regarding modifications (or construction of a plant) are listed in the following, with a short comment on their content.

The most important Guideline in this context is HSK-R-15, the reporting Guideline which defines the regulatory body's competence to approve modifications.

Depending on the safety significance, three groups of notification levels are applied:

A. Notification before starting the work (work requires HSK approval);
B. Notification without HSK approval (the change is reported, HSK has to react if it doesn't agree);
C. No reporting to Regulatory Body necessary (some information on changes appears in monthly reports or are reported during inspections).

HSK requires that modifications on all safety classified equipment (safety systems) have to be notified. For safety related systems it will be decided on a case by case basis (e.g. plant process computer). A new Guideline regarding computer software classification is in development.

Group A: This Group applies to modifications of the hardware in the mechanical safety classes 1, 2, 3, and 4 and electrical 1E and "safety related" components and systems.
They are defined in the HSK-Guidelines
R-04 and 05: Supervisory procedure covering the construction of buildings and mechanical equipment
R-06: Safety Classification. Interface between classes and construction regulation concerning the equipment of light water reactor nuclear power plants.
R-18: Supervision of repairs, modifications and replacement of mechanical equipment in nuclear installations.
R-23: Supervision of revisions, testing, replacement, repair and modification of electrical equipment
R-30: Supervisory procedures for construction and operation of nuclear installation (include 4 HSK approval steps – concept, design, construction/manufacturing, operation)
R-35: Supervisory procedures covering the construction of nuclear power plants (System engineering, refers also to safety related systems in the IAEA Safety Guide Design).
R-60 and R-61: Supervision on nuclear fuel design and manufacturing.
R-31: Supervisory procedures covering the construction of nuclear power plants: 1E classified electrical equipment.

According to HSK-R-15 (reporting Guideline), this group also applies to modifications in the Technical Specifications of the plant and modifications of the plant internal Emergency Regulation, as well as to plant tests with implication of safety systems.

**Group B:** This group applies to the safety related issues not mentioned in group A
Examples are modifications outside the safety buildings, which may impact safety buildings or equipment etc.

In addition, this group also applies to certain organizational issues like changes in the organization (only managers), in the organizational plant procedure, the radiation protection procedure, the quality management procedure, the emergency operating procedures, plant tests with possible impact on safety, etc.

The procedure on the management of change in the case of modifications of the organization changes is explicitly described in the HSK-Guideline "Organization of NPPs" (HSK-R-17).

**Group C:** This group applies to minor changes in material like lubricants, diesel fuels, bearings, seals for safety systems etc.

Changes in procedures to operate the plant and the other documented procedures in the QM System fall into this group as well.

**Swiss Regulatory Review Process for approval of Modifications**
As HSK has applied a formal QM system, the process is defined in a flow chart. Input for start: Application for modification by operator (following Guideline R-15). Depending on safety importance, large or small modification, new technology or well known technology etc. it will be decided to form a project group (project leader) or it will be dealt within the HSK approval process (process owner).
For larger modifications, including changes of safety systems, normally 4 approval steps are defined where the operator has to provide the requested analysis and documentation (according HSK-R-30/35):

**Step 1: Concept**

Operator: Provides the list of applicable regulatory guides and requirements, description and main data to the change, assessment of safety impact incl. at the SAR; QA concept for change.

HSK: Review and assessment; approval (sometimes with specific requirements).

**Step 2: Design**

Operator: Provides detailed information on the design of the modification with all relevant documentation.

HSK: Review and assessment, approval (sometimes with specific requirements).

**Step 3: Implementation**

Operator: Provides detailed documentation for manufacturing and installation, implements the modification after approval by HSK.

HSK: Review and assessment, approval (sometimes with specific requirements).

**Step 4: Commissioning**

Operator: Provides detailed documentation for commissioning and operation, final adoption of the safety report, commissioning tests, operational procedures, personnel training etc.

HSK: Review and assessment, approval with according control and hold points and potential additional requirements.

For safety related systems, step 2 and 3 may be combined. If only a safety component is changed, the documentation of all 4 steps is provided and approved in one step.

**Application of the licensee's Quality Management System (QMS) to the modification process**

The licensee is responsible for safety, and has to demonstrate adequate quality and safety control for modifications in a systematic way. HSK requires that the QMS of the Swiss NPPs fulfill the requirements of the IAEA Quality Assurance Document SS Nr. 50C/SG-Q.

Large projects or projects with new technologies involved require a Quality Assurance Plan based on Quality Elements of the plant's QM System and the QM system of the main designer/supplier. Smaller projects are controlled by the process "plant modification" within the QMS of the licensee. The real process is related to the 4 steps of the procedure guideline for modification. All steps are finished by a formal approval of HSK.
Swiss Experience with modifications drawn from safety events

Large modification: Back fitting of second level protection systems including 3rd safety injection train with emergency diesel generator and accumulators (1990 – 1994).

The main contractor was the reactor supplier; it was a key turn project. The licensee was strongly engaged to interpret the Swiss requirement to the supplier which was a company from overseas and wasn’t familiar with requirements. As the licensee hasn’t had a headquarters project group, plant personnel were engaged in the review tasks.

HSK has found during its review more non-conformances, which normally should have been found by the licensee’s review. Connection of the new systems to the existing plant systems and components and the commissioning tests were performed during longer refuelling outages. This has led to additional time pressure for all participants.

Only a few events with lower safety significance occurred during back fitting.

The following latent failures have been detected some years later:

IRS 7090: Detection of a control valve delayed closure during review of recorded data after an automatic scram.
Cause: Wrongly assembled solenoid valve to close control valve faster during Scram.
Root cause: No adequate test procedure resp. no specific test (may be included in an envelope test as Scram).

Not reported to IRS (1999): Second level diesel generator has been interlocked with a non-protected external transformer protection signal.

Cause: Interlock not in accordance with the design basis of the system (unusual situation for electrical designers, who are not familiar with such "protected systems").
Root cause: Commissioning test not realised or procedure not adequate. Periodical test so far has been performed with busbar and diesel generator in shut-off position, therefore the error could not be detected.

Lesson learned from both: After modification, a comprehensive resp. systematic test programme with traceable documentation should be performed.

Other Swiss Events Originated by Smaller Modifications (notified/approved or not reportable changes, MINIMS) in NPPs.

4 Events after small modification with HSK approval

IRS 1437: Spurious pressure spike in a reference line of the reactor level measurement (Operation Experience; Change of reference pot of reactor level measurement, approved by HSK )

Provisions for reactor level measurement have been changed (reference pot). It had not been taken into account that an accumulation of radiolysis gases in the pot could occur. An explosion in the pot was seen later as the most likely cause, as a pressure spike happened, with Scram and different spurious actuations of safety systems. The event plant response was difficult to interpret, because a lot of sensors were supplied by the affected line.

Detection: Experienced Event
Lesson learned: All modifications where BWR reactor steam is collected and condensed an accumulation of radiolysis gases may occur. Adequate countermeasures against hydrogen gas explosion are necessary. This operating experience was available (IRS system).

**IRS 7097: Enhanced localized corrosion in nuclear fuel**
(Operating experience; Reactor coolant water chemistry parameters related to changed fuel cladding and spacer material, approved by HSK)

Event: During post irradiation examination, severe local corrosion (up to 40% of cladding thickness) in spacer region was detected.

The phenomenon of "shadow corrosion" between fuel cladding and spacer has been observed for more than 20 years, but with low intensity (in the order of several tens of microns). In this case, the corrosion was unexpectedly high. Examination of the phenomenon in nine plants showed enhanced corrosion in three plants. Their reactor water chemistry data showed a low (Fe/Zn+Ni) ion concentration. This is related to the material used for cladding and spacer. The basic root cause is unknown, but with strictly controlled and adjusted water coolant chemistry parameters, the problem has been solved. The event has had a significant impact on the reloading concept.

Detection: Post irradiation examination

Lesson learned: Try to evaluate all impacts before changing sensitive materials. Use intensive operating experience or research data. Better data evaluation by the supplier.

**IRS 7242: Open Safety relief valve with reactor at power operation** (Human Factor case- Change of safety relevant component, approved by HSK)

Safety relief valve has been changed to another type with a different closure characteristic (with closure hysteresis curve of ca. 3 bar), but both are triggered by solenoid valve.

Failure: The commissioning test has been performed with reactor on power but with lower pressure than normal (4 bar) to prevent an unnecessary Scram. Therefore, after closing the solenoid during the test, the relief valve closed immediately. Consequences: Operator got the wrong impression that the new valve has the same closure characteristic as the older one (hysteresis of the new one not recognized). During the experienced event, as the relief valve has been opened by human error, shift team wasn't able to close it in time because of wrong mental awareness of the valve closure characteristic. They concentrated on closing the solenoid valve instead of reducing the primary pressure under the hysteresis curve, although this was mentioned in the procedure. The wrong valve closure characteristic was also implemented on the plant simulator model.

Detection: Experienced Event

Lesson learned:

No compromise on commissioning tests to get the correct plant (component) response, above all, if hysteresis effects are involved. The case shows that no sheer technical changes exist-therefore the designer and commission team of the change has also to think about the operating personnel, respectively on HuIRS 7541: Deformation of containment penetration during leak rate test.

(Change of containment design pressure, approved by HSK)
Modification: Installation of rupture disc to limit containment overpressure in severe accident (50% higher containment pressure). Failure: Some existing specific containment penetrations haven't been adequately adapted against new axial forces for the high pressure (too large penetration diameter related to the small process pipe).

Cause: Design review on sensitive penetrations has not detected the deviation (but for penetrations in general, a new stress calculation has been performed).

Lesson learned: More systematic design review

5 Events after small modification without HSK approval (notified or not reportable change)

IRS 7089: Reportable events for emergency diesels with high supplier implication (MINIMS; Change of diesel fuel and change of internal part of solenoid valve, no information to HSK)

A) Change of diesel fuel: The final test for requalification after maintenance failed, caused by a blocked controller for the fuel injection pump. The root cause couldn't be found, in spite of involving supplier and manufacturer. By chance, the injection pump manufacturer has been contacted: Nothing has changed, except a change to low sulfur diesel fuel. He was aware of the problem because of similar cases in smaller engines in the industry. Additional additives are necessary to assure functionality. The case had a large potential for a common cause failure because the other diesels use similar type of injection pump.

Detection: Event and chance (root cause finding)

Lesson learned: The dependency was not contained in the specification because at the time of installation of diesels, no low sulfur diesel was in discussion. Fuels of emergency machines and lubricant of safety components should be monitored more closely, specified or be tested by qualification tests and the supplier/manufacturer should better be involved in case of changes.

B) Change of internal part of solenoid valve for diesel start-up device.

A small change to an O-Ring seal on internals by the manufacturer, without adequate communication to the operator, led to a start-up failure of the emergency diesel. The root cause was difficult to find. The valve was assembled by the manufacturer, the plant delivery conformity test, a simple function test, hadn't detected the failure. Within the diesel system, the internal part was only slightly too slow to trigger the 3 way solenoid to shift correct. The failure was detected after many tests, using other solenoid valves and specific instrumentation.

Detection: Event and specific tests with special instrumentation.

Lesson learned: Operator relied too much on the QM system of manufacturer. Now, a better documentation is required and independent testing by the operator within the plant system will be performed.

IRS 1588: Trip of main generator lead to cavitation of feedwater pumps

(MINIM; Change of measurement devices of condenser hotwell level, no safety classified equipment, not notified to HSK)

Few years ago, the measurement device of condenser hotwell level should be improved by modification (weakness of the pneumatic controller with one transmitter). The
operator installed 4 transmitters and a digital controller, using an average level of the 4 transmitters. The generator tripped at full power, caused by a failure of the hydrogen seal oil system, and the reactor run back to 60% was automatically triggered. Later, a reactor level trip occurred, followed by loss of main heat sink. The cause was the wrong response of the level measurement device, the controller released too much condensate to the feedwater tank, feedwater pumps cavitated and condensate pumps were shut off by low level. The test after modification had only been performed by 60% power, believing that the response could be extrapolated theoretically to 100%. But in the event, performed at 100% power, the response of the 4 transmitters were totally different, which caused the event. Shift personnel were surprised about that plant response and acted "ad hoc".

Detection: Experienced Event

Lesson learned: Qualification test after modification should cover a worse case, otherwise a latent failure with unexpected consequences can occur. Extrapolations to save tests under more stringent conditions should be used with care.

IRS 1309: Deviation from specified boron concentration for refuelling due to calibration error (MINIM; Personnel change, not notified to HSK)

Automatic boron titration needs a calibration which is based on manual laboratory results. The primary coolant has been borated, but due to a calibration error there was a deviation of minus 10%. It was caused by the cognitive error of two new technicians, that the depletion factor of a used standard solution was calculated as 1.08 (it could be 1.0 at the highest, i.e. no depletion). The two technicians worked together, therefore no independent review happened. Both were not adequately trained or experienced because in the 16 year operation of the plant in the past, no similar event occurred.

Detection: Experienced Event

Lesson learned: Changing personnel imposes a risk that mistakes can happen, because the procedure was adequate for the experienced operator but not for the new ones. This is difficult to control. It would be better if an experienced person leads the beginner for important safety tasks for as long as he has got the necessary competence and experience.

IRS 1123: Reactor startup with degraded reactor shutdown system (HF case; 2 changes, Hardware and later on operational procedure, the first was approved by HSK, the latter notified but without approval)

Two changes had happened previous to the event:

1) The charging water valve in the control rod drive system has been equipped with a motor actuator (without consultation of reactor supplier). The reason was to have, in case of ATWS, by closing that valve, the possibility to insert the rods manually. This change was notified and approved by HSK.

2) Later, the operator experienced during start-up and shut-down many IRM (neutron flux) Scrams. By resetting the Scram signal, the accumulators became refilled automatically. The following Scram signal leads again to a fast control rod injection. This was found an unnecessary stress for the control rods, and the operator changed the operating procedure. After an IRM Scram, the charging valve was closed, the accumulators stayed unloaded and additional Scram signals had no consequences on the control rods. If the reactor was stable, the valve has to be opened. HSK has been informed, but no formal approval was necessary.
Event Sequence: An IRM Scram occurred during start-up. According to the new procedure, the operator closed the charging valve. Start-up proceeded again, the reactor went critical, with discharged accumulators (violation of Techn. Spezification). Three and a half hours later, during shift turnover, the deficiency was detected. The event has attracted much attention by the operator and by HSK and by the Swiss Commission for Nuclear Safety.

Cause/Root cause:

Ergonomic situation:

Unfavourable Alarm concept for control rods: To monitor the control rods, a wall chart display of the core and the control rods is available in the main control room. Each control rod has a green and a red light. The red light has multiple functions and indicates:

- Accumulator failure
- Rod drift
- Disconnection
- Position failure
- Rod out position

All Alarms except "Rod out" can be reset. The reason for this is because the alarm system is not "dynamic", this means, without reset, one cannot identify whether a new alarm appears. Therefore, with the reset, all red lights of the discharged accu disappeared, only on yellow indication on the desk remained with the description "accumulator fault". The situation would be the same, if only one Accu is unloaded, or 10 or all 149 of them.

There are more than 20 similar indications on the control room desk, and it is normal that after a Scram, some of them are indicating. In this case two others lit up. Considering the many activities during Scram recovery, overseeing this indication by the operators is not unlikely.

Alarm concept of the rest of the control room: It is different to that of the control rods since it has a dynamic system. It means, that an alarm light can't be reset unless the reason for the alarm disappears. If there are also more criteria on one alarm indication, every new alarm arriving produces a flashing of the light. The operator identifies it on the screen of the process computer and recognizes it by the reset. The light remains on but the flashing is absent.

Unfavorable Procedures:

The new procedure has been introduced, with sufficient information and training. It was not in the form of a check-list with signature of every step but it was in the form of a general guidance. Therefore, the critical step for the charging valve read: "Reopen of charging valve when reactor is stable". This is not an exact definition and open to different interpretations.

The general start-up procedure does not include an accumulator check if the downtime was shorter than 48 hours (this was here the case). Therefore, there was no back-up control in case that the operator failed to follow the procedure.

Not fully used Operating Experience:
A few years before that modification, a similar event happened in another plant abroad (IRS System; Scram system unavailable during single road scram test). HSK required from the operator an in-depth analysis to prevent recurrence.

The evaluation, after an initial insufficient version, was, after additional work, finally approved by HSK.

But during the modifications of the operating procedure, which has in reference to the event high importance, the mentioned event has not been analysed. Therefore, the former analysis, after the modification, was practically useless.

Detection: Experienced Event

Lesson learned: Improve the Human Factor Engineering or ergonomic assessment on modifications, even if it seems at first that no reference exists. The affected plant implemented an independent review for all modifications with impact on operational safety by experienced shift safety engineers. As they have at least more than 6 years real operating experience (plant operator, turbine and reactor operator and shift supervisor), they should have the necessary competence to prevent the recurrence of similar events (Human Factor Engineering competence not required by regulation)

**IRS 0728: Uncontrolled radioactivity release** (MINIM; Change in operation mode of the central hydroextractor for resins, not notified to HSK).

The extractor has been operated dry and unloaded during night (this is anormal, since normally it operates wet and loaded). This has produced abnormal particles (ca. 50 μm), which led to particulate deposit in the sensing line of the radiation monitoring system (particles not detected). The hydroextractor was directly connected to the exhaust ventilation, but the filter was defect. By these main reasons, the uncontrolled radioactive release couldn't be detected. It was revealed by the periodic control of ground contamination in the vicinity of the plant. The event attracted large public and regulatory and international attention.

Detection: Periodic control of ground contamination (loss of defence in depth).

Lesson learned: The event revealed a specific phenomen (abnormal particle deposition in sensing line) as a lesson learned for the nuclear community, and many latent failures in the plant. Uncontrolled changing of operation mode on such types of equipment may lead to an undefined situation. All operating modes on such types of processes should be verified by commissioning tests with specific instrumentation before routine operation.

There are additional Swiss events which are not reported to IRS. They are not mentioned here because their nature are similar to the IRS cases.

**Lessons to be learned from the mentioned Swiss (IRS) events:**

In spite of a relative close regulatory regime regarding modification, significant events couldn't be prevented. The Swiss experience shows, that the risk during or after large plant backfitting or modification projects by an experienced supplier is lower than small or not regulatory notifiable changes or modifications in hardware, operating modes, procedures or personnel. Some of them would have been easy to be prevent if operating experience and ergonomics would have been applied adequately in the operating organisation. Therefore, it will benefit of the operating organisation and the regulator to optimize the modification process related to operating experience and Human Factor.

It seems difficult for minor modifications that Human Factor review can't be done by professional ergonomists. As experience shows, the Human Factor implication is sometimes hidden e.g. a
mechanical component change with inadequate component response test has led to a significant HF event.

Human performance aspects and operating experience should not be separated from normal modification design, it should be a common duty for all project or process participants. A prerequisite for better communication among the team members should be, that the necessary training on Human Factor Principles is applied. Important traceable standard elements for Human Factor Engineering and operating experience application should be defined.

For large projects, professional Human Factor competence (ergonomist) may be contracted. The Swiss experience with a contract for regulatory support on a technologically new project (computerized emergency procedures) showed very good results. But the contractor was extraordinary qualified, as he licenced a very large new technology project (digitale control room including procedures), some years ago. The use of his new developed methodology for integrated control room validation has saved a lot of time and effort with very good results. This was also mentioned by the operator and the independent contractor, which performed the work for the operating organisation. A lot of lessons learned from the methodology have been adapted by the licensee for periodic simulator training.

Conclusions

The Swiss contribution should support international discussions on implementing operating experience feedback in the modification process. Condition: a "powerful intelligent computerized tool" should be developed to find quickly and easily the important related "lesson learned" e.g. in the IRS database. The existing tool is not helpful in this respect. This may help to reduce the risk of MINIMs recurrence and may lead to better design reviews and an improvement of acceptance or commissioning tests.

Experience has showed that missing Human Factor or Ergonomic principles in the modification process in minor changes may lead to significant events or latent failures. Human Factor shouldn't be considered separately from the more technical issues. Therefore, the Human Factor consideration is not the job of one "human factor expert", who does a separate analysis. Plant modifications are multidisciplinary tasks. A minimum of Human Factor expertise has always to be present in the modification team.

For large control room changes, or similar projects, the involvement of professional Human Factor expertise in the modification process team may be done according to NUREG 711. Since Operators have to review modifications, the need for appropriate HF expertise in evaluating HF aspects is necessary. On the regulatory side, similar involvement should be considered (own competence or experienced consultant) for its approval process.

Start international discussion for developing "standards" and tools, for instance:

- Adaption of IAEA Safety Guide Modification to implement the use of operational experience and applying Human Factor principles (perhaps an additional TECDOC for specific aspects on modifications -e.g. minor- may be helpful).
- Development of powerful intelligent computerized search tool e.g. for IRS or (and) WANO database, for efficient implementation of operating experience in the modification process, will increase the quality of the modification process control. This aspect is, above all, important for younger personnel without high experience.

References:


Swiss Modification Process in NPP's: Overview on Regulatory Regime, Regulator and Operator processes; Experience related to events with safety impact

Prepared by
Herbert Deutschmann
Swiss Federal Nuclear Safety Inspectorate

Contents:
• Overview on Main Swiss regulatory guidelines regarding notification and supervision related to modification
• Simplified Swiss Regulatory Review Process for approval of modification
• Simplified Operator Modification Process
• Swiss Experience on Modification gained from safety related events (different types- large backfitting project, MINIM, HFE)
• Lesson Learned from Swiss Events
• Conclusion
NEA CSNI WGOE/SEGHOF Workshop: Modification at NPP

Main Swiss HSK Guidelines regarding modification
Swiss Guidelines are not obligations, they explain to licensees’ and designers how the Swiss regulatory body put his duty in concrete terms (except reporting guideline). They are flexible and concrete. But they are not standards how to perform detail work. (New Atomic law and a decree is foreseen for 2005)

Reporting guideline (R-15): Contains all types of information which has to provide to regulatory body. Regarding modifications 3 types are defined:
A) Modifications which has to be approved by regulatory body
B) Modifications which has to be reported to regulatory body
C) No reporting necessary
Some modifications are between (e.g. plant process computer)

Guideline for safety classification R-06: Defines the safety classes of mechanical and electrical equipment for NPP. It is very important for modifications because it assigns the different types of regulatory impact. 4 mechanical classes (1 to 4) and 2 electrical (1E and 0E); 2 earthquake classes (safety and operational).

Guidelines for supervision R 04,05,18,23,30,35 etc.: Different types for construction, mechanical, electrical equipment, systems, procedure for construction and operation, fuel manufacturing etc. They give concrete advice how to deal with the specific equipment or systems, what analysis regarding safety has to be performed, what documentation has to be provided for application on the 4 different project steps (concept, design, construction, operation)
NEA CSNI WGOE/SEGHOF Workshop: Modification at NPP

Swiss regulatory review process for NPP modification

As the steps of the project are defined in the procedure guideline, regulatory body has to assess and review the provided documents. This may include to request additional investigation or analysis or specific requirements. Important points are the definition of standards to be applied, the analysis of the safety impact, the quality assurance plan for the project provided by the licensee, the technology applied (new or referenced by other projects). The sequence of work is fixed in a formal flow chart in the management manual, which directs also the other normal project elements as responsibilities, reporting, controlling, etc. The processes follows the management concept of ISO 9001.

Modification process in the QM system of the licensee:

Licensee is responsible for safety (can’t be delegated to designer) and has to demonstrate adequate quality and safety control for the modification in a systematic way. It is the applicant, it controls the whole communication with regulatory body. The related processes are defined in the Management Manual, which has to follow the IAEA Code/SG QA. Important guides in this respect are Design, Procurement, Inspection and Testing for acceptance etc. This guides recommend concrete elements how to plan and perform work in accordance with standards which contain also Human Factor elements. Appropriate procedures are used. The real modification process is related to the 4 steps of the procedure guideline. All steps are finished by a formal approval of HSK.
NEA CSNI WGOE/SEGHOF Workshop: Modification at NPP

Swiss Experience on Modification derived by saf.rel. events

11 Events (10 in IRS) analysed regarding modification impact

2 Events are related to a large backfitting project; reactor supplier was the main contractor (1990 to 1994): Installation of a 2nd level bunkered protection system including accumulators and 3rd HP safety injection and low pressure recirculation train, emergency diesel and the complete control system.

IRS 7090 and an event not reported to IRS: Wrong interlock of emergency diesel by protection signal of non protected transformer.

4 Events after small modification with HSK approval
IRS 1437, 7097, 7242, 7541
Example: IRS 7242 HFE case due to changing a component
A safety/relief valve in a BWR has been replaced by an other type. An inadequate functional test has caused that plant personnel missed the correct awareness of the new component closure behaviour (4 bar hysteresis to close with solenoid valve). Event: Failopen of safety/relief valve on rated power by human error, operators were unable to Scram the reactor timely (5min). 2nd level protection system triggered Scram automatically after 15 min.

H. Deutschmann, Swiss Federal Nuclear Safety Inspectorate

5 Events after small modifications without HSK approval (notified or not reportable change): IRS 7089, 1588, 1309, 1123, 0728
Example: IRS 1123 highest safety importance of all Swiss IRS events; HF case by modification in lowest safety class part and later on operational procedure in the control rod drive system
Manual valve equipped with motor actuator (without consultation of reactor sup.)
Later, for optimizing operation (reduce control rod load by reducing unnecessary rod injection), die valve has to be closed after Scram (till „reactor is stable“)
Event: IRM Scram during start up, valve was closed; start up proceeded and reactor becomes critical without pressurized fast scram accus. 3,5 h later the mistake was detected, valve opened and the accus become reloaded.
Consequences: Valve is now interlocked with control rod actuation, modified alarm system, modified procedure and independ modification review by experienced shift engineer.

H. Deutschmann, Swiss Federal Nuclear Safety Inspectorate
NEA CSNI WGOE/SEGHOF Workshop: Modification at NPP

Lesson learned from the event analysis related to modification
In spite of relative close regulatory supervision, events caused by modification couldn’t be prevented.
Large projects, with reactor supplier involved posed not a high risk as minor modification (done by licensee alone)
Human Factor impact is not always clear during modification, this may lead to latent deficiency over a long time
Efficient use of Operating Experience as a standard element of the modification process may lead to reduction of recurrence
Systematic modification process by the licensee and a efficient independent supervision by regulator reduce the risk.

H. Deutschmann, Swiss Federal Nuclear Safety Inspectorate

Conclusion from the lesson learned:
Develop or revise international guidance (e.g. IAEA safety guide modification) for efficient implementation of the process elements operating experience and Human Factor Engineering principle as a „standard“.
Develop intelligent computerized tool for efficient use of large operating experience data basis (e.g. IRS). Manual searching in large data basis is extrem time consuming, people lose the motivation. The main work should be done by the „machine“, user has to do the „intelligent“ work.
All modification team members have to deal with Human Factor principle, it is not the duty of one assigned person.

H. Deutschmann, Swiss Federal Nuclear Safety Inspectorate
TEMPORARY MODIFICATIONS AND MINOR CHANGES – THREATS TO SAFETY?

WORKSHOP PARTICIPANTS BEHAVIOUR

Get involved and ask questions

the only stupid question is the one you do not ask!
MINOR CHANGES AND TEMPORARY MODIFICATIONS

• Generally speaking every operating Nuclear Power Plant in the world faced, faces and will face operating abnormalities caused by improper installation of minor changes and or temporary modifications.

MINOR CHANGES AND TEMPORARY MODIFICATIONS

• One of the questions normally brought up from the root cause analysis of such events is: does the existing process to approve and install such changes have an embodied safety analysis on it?
MINOR CHANGES AND TEMPORARY MODIFICATIONS

• One fact is that it is easier to install a temporary modification than a permanent minor change, due to the specifics traits of such processes.

MINOR CHANGES AND TEMPORARY MODIFICATIONS

• Another fact is that the temporary modification is a serious candidate to a permanent minor change, without the necessary technical and safety review analysis.
PLANT CONFIGURATION CONTROL – A REAL EXAMPLE

<table>
<thead>
<tr>
<th></th>
<th>PRIMARY SYSTEMS</th>
<th>SECDARY SYSTEMS</th>
<th>TOTAL</th>
<th>COLOR CODE</th>
</tr>
</thead>
<tbody>
<tr>
<td>TM</td>
<td>04</td>
<td>07</td>
<td>11</td>
<td>RED</td>
</tr>
<tr>
<td>ANN. LIT</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>YELLOW</td>
</tr>
<tr>
<td>Controllers in Manual</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>GREEN</td>
</tr>
</tbody>
</table>

Are Mods adequately controlled?

- The international experience also demonstrates that not all modifications installed at the plant are controlled, because what deserves control is different from plant to plant. This is specially true at the old plants in the panels with relay actuation devices.
Are Mods adequately controlled?

• In some plants, at the operating floor, there are common practices of installing masking tapes or similar things to hold relays contacts. Other practices allow for the installation of hoses, wire extensions and floor drain caps without adequate paperwork, because they are simple, would only stay for some hours or days, they would not be left unattended, etc, etc and mainly because the required paperwork will take hours or even days to be approved.

DRIVING FORCES

• This sense of urgency is one of the driving force that motivates the installation of unauthorized temporary modifications.

• Another driving force is the internal bureaucracy related to the approval of a Temporary Modification.
The criteria are not equal

• The bar or the criteria to identify plant alterations that should deserve a dedicated process control, unfortunately is not the same for every plant.

PLANT ALTERATIONS THAT REQUIRES A CONTROLLED PROCESS

International experience demonstrate that the following plant alterations should be identified and processed through controlled means:
PLANT ALTERATIONS THAT REQUIRE A CONTROLLED PROCESS

1. Disabled alarms (annunciators)

2. Lifted leads

3. Electrical jumpers

4. Temporary set point changes

5. Blind flanges or plug installation

6. Floor drain temporary closures
PLANT ALTERATIONS THAT REQUIRES A CONTROLLED PROCESS

7. Temporary disable of safety and relief valves
8. Temporary pipelines installation
9. Pulled circuit boards
10. Temporary electrical connections.

THE PROCESS OF APPROVAL

• ANY OF THE PROPOSED ALTERATIONS SHOULD BE FORMALLY APPROVED, THROUGH A COMPREHENSIVE CONTROLLED PROCESS.

• This formal control process should include a necessity for a technical review and a safety review, if the modification is anyhow related to the safety.
Contents of a Technical Review

• The Technical Review form should contain a series of questions to be answered by the qualified reviewer, type Yes/No/NA.

• These questions should covered the whole spectrum of a design change, such as:

1. Mechanical, Electrical and Hydraulic issues
2. Fire Protection
3. Security Protection
4. ALARA and Environmental effects
5. Industrial Safety and Chemical effects
6. Instrumentation and Control aspects
7. Structural effects
8. Operability
9. Analysis of failure mode
10. Procedures affected, applicable norms and codes
Technical Review

For each part of the sections (10 in this case), a series of questions should be answered. Only to give an example, for the Part 8 – Operability:

1. It is required its operability in all modes of the operation of the Plan?
2. Is it required to operate during an emergency?
3. Does it require training for the operators?
4. Do some procedures have to be modified?

Technical Review

- For the Part 6 – Instrumentation and Control:
  1. Does it have sufficient adequate instruments to be monitored by the operators?
  2. Is there alarm signal and where?
  3. Does it require periodic calibration?
  4. Does it affect the sensor time response as addressed in the FSAR?
  5. Does it require any manual actuation from the operators?
Contents of a Safety Review

• In the case a Minor change or a Temporary change is somehow safety related or important to safety, as determined by the qualified reviewer, a more comprehensive analysis should be performed, in addition to the Technical Review.

• Similarly, several related questions are addressed:

Safety Review (examples of some required analysis)

1. List of documents and procedures to be affected.
2. Is the Containment integrity affected?
3. What about seismic analysis?
4. Radioactive release are foreseen?
5. Is there a need for Environmental Qualification?
6. Does it fail safe?
7. And the separation and redundancy criteria?
8. How is affected the probability of any accident described in the FSAR?
9. It could create any possibility of an accident or event not foreseen by the FSAR?
10. Could the safety margins as described in the FSAR and Technical Specifications be affected?
CONCLUSIONS

1. Minor changes and Temporary changes could be a threat to the operability and to the operational safety of Nuclear Power Plant if they are installed without formal comprehensive processes.

2. The well spread justification of a sense of urgency for its installation is in the vast majority of the cases analysed, not justified.

3. Such modifications are very like an iceberg. Who requests them only see the surface. The persons in charge for its analysis and approval have to see the entire ice block.

4. When something goes wrong, caused by inappropriate process related to the the minor changes and temporary modifications, it is very easy to blame on the front line workers. This is a futile exercise!
Human Error and the Law

• In most instances of human error, the blaming of front line workers is an almost futile exercise and concentration on this aspect as opposed to organisational and/or engineering investigation and probing is a recipe for disaster in the future.

IAEA – Operating Experience Unit

MANY THANKS FOR YOUR KIND ATTENTION!
Session 1: HUMAN FACTORS, METHODS & TOOLS

Theme: Which tools and methods can be used for integrating human factor in the design process of a modification?

Presentation: Providing ergonomics guidance to engineers when designing Human-Machine interfaces for nuclear plants installations........ 217
D. GREGSON, E. MARSHALL, A. GAIT, N. HICKLING (Synergy Consultant Ltd, UK)

Session 2: OPERATING EXPERIENCE, ROLE OF THE REGULATOR

Theme: How can the regulator and his TSO help to improve detection of shortcomings due to modifications?

Presentation: Regulatory aspects of plant's modifications......................... 229
M. JUAN (DGSNR, France)
Providing Ergonomics Guidance to Engineers when Designing Human Machine Interfaces for Nuclear Plant Installations

Ed Marshall & Dave Gregson
Synergy Consultants Ltd
6th October 2003

Background

• Application of ergonomics (safety, efficiency and operating reliability)
• Research Project as part of the UK IMC Generic Nuclear Research Programme
• Develop toolset to provide ergonomics guidance to assist C&I engineers in designing new or modifying existing HMIs in nuclear plant control rooms
• Toolset should support different stages of a refurbishment process
• Also beneficial to ergonomics professionals with experience of interface specification and design for process control
Summary of Ergonomics Benefits

- More fluent operation (e.g. designs consider sequence of use, functional grouping)
- Reduction in the likelihood of human error (e.g. design matches user expectations, design consistency)
- Reduction in frustration (e.g. timely system feedback, error recovery, on-line help)
- Improvements in user attitudes (e.g. users are not alienated from the process)
- More effective process operation (e.g. provision of well-designed overview displays)

Site Survey

- 16 UK sites surveyed (nuclear industry and related industrial applications)
- Questionnaire / Interviews
- Benefits of ergonomics usually understood
- Lack of formal ergonomics input
- Ergonomics standards and guidelines used ineffectively
- Apparent that guidance needed to be provided in a clearer and more practical way
Problems with Providing Ergonomic Guidance

- Understanding of ergonomics (consequences of non-compliance, use of language)
- How much guidance to provide? (difficult to rationalize exclusion of available guidance)
- Contextual understanding (guidance often needs to be application specific to be most effective)

Difficulties to Overcome

- Make guidance clear and unambiguous
- Help design engineers to appreciate the risks of non-compliance
- Assist design engineers to locate the relevant guidance to their specific application
- Identify when professional ergonomics support should be sought
Design Aims of Toolset

- To ensure that HMIs will support reliable and effective performance
- Provide a structured approach to the procurement and design of HMIs
- Make the toolset usable for non-ergonomists

Toolset Trials

- Initial version of toolset trialled using design engineers
- Current experience of refurbishing user interfaces but no formal Human Factors training or background
- Areas for improvement identified from feedback and subsequent discussions (e.g. Expand guidance, improve consistency, remove ambiguities and allow toolset to be fully functional on-line)
Overview of Toolset

**STRATEGIC PROJECT DECISION-MAKING FLOWCHARTS**

Presents series of questions requiring yes/no responses to identify the key ergonomics issues and whether professional ergonomics support is required.

**GUIDELINES DOCUMENT**

Can be used as a stand-alone document.

Divided into 16 sections (e.g. Data displays, Control Devices, Data Entry etc.)

**MATRICES**

Spreadsheets listing the sub-headings of the guidelines document.

Matrix completion records the degree of compliance with the guidelines.

Selected guidance from several sources

---

**Strategic Project Decision-Making Flowcharts**

- Flowcharts useful to identify the key ergonomics issues at an early design stage
- Flowcharts detail some of the ergonomics techniques that may be necessary
- User rates ergonomics issues in terms of ergonomics complexity and safety criticality
- Identifies whether professional ergonomic support is required
Strategic Project Decision-Making
Flowcharts

1) Ergonomics Involvement and Philosophy
2) Records of Operational Issues
3) Automation and Controls
4) Software Operating Environment Procurement
5) Alarms
6) Information Presentation

Flowchart Assessment Judgements

<table>
<thead>
<tr>
<th>Rating</th>
<th>Safety Criticality</th>
<th>Ergonomics Difficulty</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>No concern to safety</td>
<td>Very accessible and easy to undertake</td>
</tr>
<tr>
<td>B</td>
<td>Some relationship to safety</td>
<td>Process accessible with some learning</td>
</tr>
<tr>
<td>C</td>
<td>Strongly related to safety equipment or tasks</td>
<td>Difficult process requiring considerable experience</td>
</tr>
</tbody>
</table>
3.1 Are entire panels being replaced? No

3.2 Are the panels to be entirely replaced by a soft desk? Yes

3.2a A plant overview display and validation of soft desk control commands significant to nuclear safety are definitely required. C C

3.3 Are some process controls to be implemented via computer displays? No

3.3a A software environment should be chosen and a navigational hierarchy designed. C C

3.4 Are new or replacement controls being installed? No

Guidelines Document

- Details majority of guidance available
- Guidance gathered from over 30 selected sources. Examples include The Design of Interfaces for Station Control Rooms (DISC) produced for the UK Nuclear Industry and guidance produced by the American FAA
- Consolidated and structured into meaningful headings and sections
- Early sections more broadly applicable
Guidelines Document Sections

1. Allocation of Function  
2. General HCI Principles  
3. The Room Environment  
4. Control Devices  
5. Display Screens  
6. Software Operating Environment  
7. Windowing  
8. Soft Controls  
9. Structure and Navigation  
10. Designing Displays  
11. Colour and Other Coding Techniques  
12. Alarm Systems  
13. Mimics  
14. Task-based Displays  
15. Data Displays  
16. Data Entry

Matrices

Used to assess and keep a record of ergonomics compliance with the guidelines document.

- Assess a design concept  
- Assess detailed work-in-progress designs  
- Compare different HMI systems at the tendering / procurement stage  
- Assessing finalized designs  
- Checking a complete HMI system
The relative humidity should be maintained between 40% to 65%.
Source: Parsons (1993)

3.7 Air movement
There should be some air movement, but this should not exceed 0.2 m per second at the operating positions. Draughts and unwanted air movement can be both uncomfortable and problematic for operators carrying out sedentary work and should, therefore, be eliminated or at least controlled.
Source: Parsons (1993)

3.8 Air changes
The total room air should be changed approximately 10 times per hour. In circumstances where total air recirculation is required, it is strongly recommended that specialist physiological advice is sought.
Source: Parsons (1993)

<table>
<thead>
<tr>
<th>Judgement</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>The item or object fully complies with the guideline(s)</td>
</tr>
<tr>
<td>Poor</td>
<td>The item or object fails to meet the requirements of the guideline(s)</td>
</tr>
<tr>
<td>N/A</td>
<td>The guideline is not applicable to the item or object</td>
</tr>
</tbody>
</table>
## Conclusions 1

### Benefits

- Large body of guidance collated and structured
- Useful tool for both ergonomists and non-ergonomists
- Toolset helps to determine when professional ergonomics support may be required
- Matrix completion encourages communication between design engineers and ergonomists
Conclusions 2

Issues to be resolved

• Prioritisation of guidance
• Subjectivity of method
• Further trials welcomed to assess and improve usability
Regulatory aspects of plant's modifications
to PWR

The regulation

• The french law:
  - Décret n° 63-1228 December, 11th 1963 about nuclear plant (Article 5 and 6)
    - Modifications which impact:
      - General operating rules
      - Safety report
      - Emergency organisation
  - Ministerial order august, 10th 1984 (Quality)
  - Specific requirements for primary and secondary circuits

• Concerns only modifications Important to safety
EDF Modification management

- **Batch:**
  - Coherent set of modifications based on modifications of conception which impact the general operation of reactors

- **Others:**
  - Specifically scheduled modifications which present an emergency or other strength which have to be integrated early.

- **Objectives for EDF:**
  - Better management of batches scheduling
  - Better management of documents modification
  - Settle serie standard

New assessment objectives

- Adapt regulator's instruction depending on modification's safety impact
  - Modifications classification
  - Different approval modalities regarding the classification

- Improve the regulator's vision of modifications implementations on reactors
  - To make Regulator's control easier
  - (time to check every aspect of safety)
New assessment process

- Classification process:
  - Classify modification regarding their safety impact

  ![Diagram showing classification process]

  - **GROUP 1**: Approval before implementation
  - **GROUP 2**: Approval before generalization
  - **GROUP 3**: No approval

New assessment process

- Classification criteria:
  - **Group 1**: Deep impact on the safety demonstration (safety report) +
    - introduce new risk (weaken a support safety function)
    - new design technologies
    - no possible direct test
  - **Group 2**: No important impact on safety demonstration, but has a risk on integration or operation +
    - requalification criteria validation needed
    - efficiency validation or experience feedback
  - **Group 3**: No safety impact or not in group 1 or 2
New assessment process

Implementation file contents

- Part 1 Synthesis
- Part 2 referencial document
- Part 3 test and requalification documents
- Part 4 integration strength
- Part 5 contract management
- Part 6 realisation file
- Part 7 local specification
- Part 8 impact on referential
- Part 9 spare part

Content of regulator information: Preliminary information

- Groupe 1: Part 3 + information note + feedback results
- Groupe 2: Part 3 + information note + feedback results
- Groupe 3: information note

Information note contents

- synthesis (indice, origine, technical aspects...)
- Risk analysis
- human factor aspects
- General operating rules impact
- Safety report impact
- spare parts management
- radiation protection...

Feedback on integration and requalification for group 1 + 2
### New assessment process

**Modification classification by Regulator**

<table>
<thead>
<tr>
<th>Group I:</th>
<th>Group II:</th>
<th>TTS</th>
<th>Group I et II:</th>
<th>Generalization</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Information note</td>
<td>-Information note</td>
<td></td>
<td>-Feedback</td>
<td></td>
</tr>
<tr>
<td>-IF (part 3)</td>
<td></td>
<td></td>
<td>-Integration</td>
<td></td>
</tr>
<tr>
<td>Preliminary information</td>
<td>Group II et III:</td>
<td></td>
<td>-Requalification</td>
<td></td>
</tr>
</tbody>
</table>

**Definitive list Documents approved by ASN**

- CTE-3
- CTE-9
- Jo-12
- Jo-9
- Jo-6
- Jo-4
- J0
- Div+4
- J1-6
- J1

**Additional informations from operator:**

- yearly check up of ITS modification realisation on every reactors
- Regulator demands in IF
- information about schedule changes
- Information of local regulators about no ITS modification list implemented (designed and managed by units) if demanded...

**Advantages:**

- better vision on technical state of reactors
- better management of modification instruction
- better inspection preparation
New assessment process

- The regulator therefore carefully monitors:

  - The quality of modification design
    - Early information and adapted depth of instruction
  - The quality of modification implementation
    - Yearly regulator information
    - Regarding its safety issue (conformity...)
  - The associated experience feedback (implementation & operation)

Batch VD2-900 MWe

- CPY series Batch VD2
  - VD2: 38 modifications
  - PIS 2: 55 modifications

  Modifications classified by issue:
  - Safety: 55 % including 38 % derived from experience feedback
  - Safety review: 29 % including fire action plan
  - Availability: 11 %
  - Cost control: 3 %
  - Others: 2 %
SEGHOF – First Task Group Meeting

SUMMARY OF QUESTIONNAIRE ON HUMAN FACTORS IN ENGINEERING CHANGES
(11 countries responded)

Do you think it is important to take human factors into account in the design change process?

- All respondents said YES
What are the main reasons why you think it is important to consider human factors?

- Design determines actions and work processes needed to run the plant
- Humans play a role in initiating, controlling and mitigating events
- Prevention of human errors
- Optimization of human-machine interface

Main reasons (cont’d)

- Ensure the needs of users are considered (human-centred design)
- Identify safety-significant actions which are credited to operators and ensure operator actions are achievable
- In some countries, HF is a legal requirement
- HF can be a link between different groups involved in design changes (engineering, staffing, training, procedure writing)
What regulatory requirements exist in your country regarding incorporation of human factors into the design change process?

- HF in design changes is addressed through
  - regulations
  - regulatory documents (guides, directives, safety assessment principles)
  - generic requests and specific requirements

- Several respondents stated that design changes are carried out under a quality assurance framework.

Which standards and guidelines are used to incorporate human factors into the design change process?

- Standards mentioned most often were
  - NUREG 0711 (5 countries)
  - IEC 964 (4)
  - NUREG 0700 (3)
  - NUREG/CR-6393 (3)
  - IEC 1771 (2)
  - ISO 13407 (2)
  - NUREG 6105 (2)
For regulators, what actions do you take to ensure that licensees incorporate human factors into the design change process?

- General actions by regulators
  - review of design, meetings, letters, engineering judgment, observation on site, etc.

- More and more focus on evaluating the design process

- Actions to convince the licensees (joint research, seminars, letters ...)

If there is not sufficient integration of human factors, what actions are undertaken for improving it?

- General actions by regulators
  - ask for improvement (design result and/or process)
  - recommend not to approve change
  - postpone the project until HF work is done
  - To place a legal requirement on the licensee, but ... “it is rare to use it in HF area”
During the review, do you consider the methods and techniques used by licensees when incorporating human factors in the design change process?

- More importance given to the evaluation of the HF process (methods & techniques, project plan, team, ...)

- The « best way to review this kind of change is to consider the methods and techniques », not just the final product

- Considering the process is a « cost-effective use of limited HF resources »

What criteria do licensees use for deciding when to integrate human factors aspects into a design change?

- Safety significance

- Impact on tasks and activities

- Other
  - Economics
  - Minor / major modifications
  - Control Room / Plant
  - Complexity of change
At which stage of the modification are human factors aspects generally taken into account by licensees?

Potential for HF Principles to be Incorporated

- Conception
- Design
- Verification & Validation

Which methods and techniques are used by licensees when incorporating human factors in the design change process?

- Methods and techniques depend on characteristics of the modification
- Techniques include:
  - operating experience review
  - function allocation, task analysis, workload evaluation
  - human reliability analysis / human error analysis
  - walk through, talk through
  - discuss HF in small groups of relevant parties
  - verification and validation (methods depend on the change)
What are the main difficulties encountered when incorporating human factors into design changes in your NPP or your country?

- Still a lack of knowledge and awareness about HF (NPPs & regulators)
- Trade-offs between HF and other technical issues
- Difficult to measure costs versus benefits of integrating HF
- Incorporation of HF before contract is finalized
- Some are seeing improvements

What future actions would you suggest for discussion during the upcoming workshop?

- Exchange of experience
  - licensees: processes for incorporating HF and examples of design changes involving HF
  - regulators: use of regulation and how HF in design is enforced and monitored
  - events related to poor HF designs
Topics for discussion during the upcoming workshop (cont’d)

• Current international standards and guidelines

• Strategies for Promoting Human Factors and Educating Engineering / Design Team Staff

• Continuing Training for Human Factors Specialists

Are there any other related topics which you would like to see discussed during the upcoming workshop?

• Modernization, computerized systems

• Engineers and licensee HF staff invited, not only a HF regulators workshop

• Specific tools
  – Virtual reality for design and validation
  – Database of good / poor HF designs
  – Relevance of MANPRINT in nuclear industry
Summary of SEGHOF Paper Presentations and Discussions

During the first day of the workshop, all participants attended eight paper presentations. On the following two days, participants were separated into four groups with three focusing on human factors in modifications and the other focusing on minor and non-identified modifications. There were three discussion sessions during the workshop. Each discussion session was introduced by a paper presentation. The groups that focused on human factors in modification processes had the following discussion topics:

1. Operating experience with human factors in design – Costs and Benefits
2. Incorporating human factors into the modification process – screening process and criteria
3. Methods and tools for human factors in the modification process
4. Role of the regulator in human factors in design changes
5. Areas for improvement
6. Recommendations

This section summarizes the discussions about human factors in modification processes and the papers that are relevant to each discussion topic.

1. Operating Experience with Human Factors in Design - Costs and Benefits

Workshop participants shared their experience related to the incorporation of human factors in modifications. Incorporation of human factors in the modification process means systematically considering the capabilities and limitations of system users (anthropometric, perceptual, cognitive, physiological and motor response) through application of human factors methods and principles. The goal of incorporating human factors in the modification process is developing a user-centered design in which plant systems support operators and maintainers in fulfilling their responsibilities. The following costs and benefits are based on papers, presentations, and the experience of workshop participants.

(a) Costs Associated with Inadequate Human Factors Work

- Problems with the usability of the design may lead to impaired operator performance, such as loss of situational awareness or unacceptable delays in completing tasks.
- Impaired operator performance leads to an increased potential for events due to human error. Many costs can be related to events, such as loss of power generation, increased regulatory scrutiny, and loss of public confidence.
- Rework costs to improve a design are incurred when problems with the usability are discovered after installation.
- Many regulators expect licensees to include human factors in their modification process. The regulator may increase surveillance activities if human factors is not in the modification process or if the process is not followed.
• Undetected problems with usability may lead to delayed plant start-up after installation of a modification.
• Late consideration of human factors may lead to
  o Delayed regulatory approvals, which may impact on the project schedule.
  o Project delays which may impact on power generation.
  o Increased costs to modify a contract at later stages of the project when design work is conducted by a contractor.
  o Lost opportunities for improvements to the usability of the design.
  o Human factors analysis work being used to justify the existing design/ modification rather than contributing to an improved design.

The cost of carrying out human factors work was discussed. One NPP found that the cost of human factors work is low when compared to the overall cost of a modification.

(b) **Benefits of Human Factors Work**

• A major benefit of incorporating human factors into modifications is to avoid the costs noted in the previous section (e.g. fewer events, less rework, less regulatory attention).
• The end result of human factors analysis work will be a user-friendly human-system interface (HSI) design. A user-friendly HSI and workplace design lead to
  o Reduced human error by operators and maintainers leading to improved profitability and safety.
  o Satisfied users (e.g. operators, maintainers).
  o Greater likelihood that the design will meet the needs of users.
  o Increased likelihood that the system will be used as was intended by the designer.
• Quantitative measurement of human performance throughout the design process provides confidence to the NPP and regulator that the modification will not have a negative impact on human performance, and thus, safety.
  o In one country, the regulator required a nuclear installation to demonstrate that modifications in the main control room would not have a negative impact on human performance. This was accomplished through quantitative measurements of human performance during validation testing.
• Human factors specialists and/or analysis techniques are a link between users and designers/engineers. Many of the human factors analysis techniques, such as gathering operating experience from users or running validation scenarios in a simulator, require design team members to interact with system users.
• User involvement in the design process, along with adequate and timely training, have been found to reduce difficulties during the transition period after a modification has been installed.
• Validation testing with users
  o Identifies problems with the design that can be corrected before installation.
  o Identifies problems with procedures.
• There will be improved public perception of nuclear power if the public has confidence that the risk of human error has been minimized by systematically considering the needs of workers.
• With each modification in which human factors is successfully incorporated, NPPs come to recognize the benefits of human factors work.

2. Incorporating Human Factors into the Modification Process - Screening Process and Criteria

There was general agreement among workshop participants that a full human factors review is not required for all modifications. In order to determine the level of human factors effort required, a screening process may be used. During this discussion session, the screening process and criteria were discussed.

(a) Screening Process

• Screening can be used to prioritize and scope and level of human factors effort required.
  o A documented process for screening design changes is required to ensure consistent results.
  o Screening must be done early in the design process.
  o Once the level of human factors effort has been determined, appropriate human factors staff should be involved in the design work early in the project. For example, the potential for human error should be a consideration when a pre-fabricated or “off-the-shelf” option is selected.
  o In some NPPs, screening to determine the level of human factors effort is done by multi-disciplinary teams that include operators and maintainers. In other NPPs, screening is done by designers using a checklist that asks questions about important human factors aspect of the modification.
  o Changes to maintenance tasks should be screened in the same way as changes to operations tasks.
• Screening to determine the level of human factors effort may be useful for other groups involved with human performance, such as training.

(b) Screening Criteria

• Any screening criteria should be clearly worded so there will be consistency between different people using them.
• Screening criteria currently in use include the following:
  o Safety significance or risk (categories discussed for defining risk include nuclear safety (based on safety analysis and probabilistic risk assessment), personal safety, environmental protection, safeguards/security, production and economics)
  o Impact on human actions or practices, such as changes to
    • Human-machine interface (HMI) (some use number of HMIs impacted)

245
- Simulator, procedures, training
- Information available to users
- Operator interactions
  - Nature of human error potential
  - Complexity of modification
  - Overall volume of work
  - IEC 964 screening criteria
  - Availability of station specific design guidance
  - Regulatory body requirements

(c) Availability of Human Factors Resources

- NPPs need to ensure there is competent human factors input as part of the modification design team.
- One NPP has human factors staff who have defined qualifications with a role to support plant human factors activities. The in-house human factors staff obtains external assistance when necessary.
- NPPs require an internal audit and self-assessment processes to ensure there is adequate incorporation of human factors into modifications.

3. Methods and Tools for Incorporating Human Factors in the Modification Process

NPPs must prepare a safety-related justification for modifications. The potential for staff, such as operators and maintainers, to impact on nuclear safety must be considered systematically as part of this safety-related justification. Results from the application of human factors methods are important for demonstrating that the modification will not have a negative impact on human performance.

One group of workshop participants discussed human factors methods that are currently used when modifications are planned. The group discussion about methods and tools is supplemented by several papers which focused on methods (Gregson et al., Jeanton, Naser et al., Quentin et al., Skjerve et al., Soares et al.).

There was not time to discuss incorporation of human factors in temporary changes among SEGHOF participants.

(a) Major Modifications

There is agreement that full human factors reviews should be conducted by human factors professionals for major changes. Many countries follow existing guidance to perform human factors reviews, such as NUREG 0711 (Human Factors Engineering Program Review Model).
There is also agreement among human factors professionals that system users must be included in the process. In fact, many analysis methods used by human factors professionals involve working with system users.

(i) Common Methods Used for Major Modifications

- Operating experience reviews may include
  - a review of past events.
  - talking to users.
  - obtaining information about similar designs in other plants.
  - questionnaires to gather feedback from users in a systematic way.
- Function analysis and allocation identify new or modified functions and assign functions to staff and/or equipment and automation.
- Task analysis identifies new tasks, modified tasks, or modified task demands (e.g. the time available to complete a task). The task analysis can be used to identify design requirements for completing tasks, procedural influences, environmental influences, communication interfaces, teamwork, training needs, etc.
- The Probabalistic Risk Assessment (PRA) or Human Reliability Analysis (HRA) is used to focus on tasks with the highest risk.
- Workload analysis determines the impact of the modification on staffing levels.
- Appropriate design guides are followed. Design guides may be general, such as NUREG 0700, or plant-specific.
- Verification is carried out to ensure the design complies with human factors guidelines. It is important to follow a design change through the installation to verify that all human factors specifications are implemented.
- Validation testing and evaluation of the design are generally carried out throughout the modification process. Validation activities include the following:
  - talk-throughs of activities using the proposed design.
  - walkthroughs of activities to verify the timing of tasks.
  - measuring human performance, using measures such as time, goal fulfillment, situation awareness, and trust (Skjerve et al.).
  - running through scenarios using mock-ups or simulators.
    - The PRA can be used to select scenarios with greatest likelihood of human error for validation exercises.
- Training needs analysis identifies required training on the modification.

(ii) Other Methods Used for Major Modifications

- When modifications will impact on human performance, several participants from NPPs begin by carrying out a field study. The purpose of the field study is to familiarize design team members with usability issues related to the modification through observing work and talking to current system users. There are variations in the scope of this field study between countries. There are also variations in who conducts the field study – human factors specialists or design team members. Field studies also assist in gaining an
understanding of how the modification may impact on functions, tasks, and workload. The field studies are used to develop design requirements.

- The OECD Halden Reactor Project developed a virtual reality model of a main control room. Through this virtual control room, compliance with design guidelines from NUREG 0700 was evaluated.
- Times to complete tasks from an Emergency Operating Procedure (EOP) were estimated using two cognitive task analysis tools: EPIC (Executive-Process-Interactive-Control) and MHP (Model Human Processor) (Soares et al.). Results from the cognitive task analyses were compared to times measured in a simulator. With further refinement, the cognitive task analysis tools should be useful for comparing cognitive workload between design options.
- Performance monitoring is carried out after modifications are in place to track any impacts of the change on human performance.

(b) **Minor Modifications**

- There was agreement that less human factors effort is required when modifications are screened as minor. The methods used for minor modifications should be similar to those used for major modifications, but may be done to less depth.
  - Guidance on the minor modification process and level of detail for human factors analysis work for minor modifications should be included in the NPP's modification process.
  - Expectations for human factors analysis work for minor changes must be clearly defined, especially if it will be done by designers who do not have a human factors background.
  - There must be a training program, so designers understand human factors principles and the NPP's minor change process.

- Common features of processes used for minor changes include the following:
  - Use of screening criteria to determine level of effort required
  - More reliance on designers for minor modifications
  - Availability of site-specific design guidance for use by the designer
  - Some NPPs use forms or questionnaires to guide design team members to pertinent issues when minor modifications are made. One licensee uses a form with questions that prompt the designer to consider the following key issues:
    - Operating experience review
    - Description of tasks and errors which may arise during each task
    - Use of plant-specific design guides
    - Validation of the design

(c) **Modifications Impacting on Maintenance Tasks**

- Maintenance errors are a common source of events.
• The needs of users during future system maintenance and testing must be considered to the same degree of detail as the needs of operators when modifications are planned.
• Co-ordination of work between operations and maintenance should also be considered when modifications are planned.
• One NPP has a practice of including training about ergonomics in the qualification of maintenance staff.

(d) **Installation and Commissioning**

• There was not time during this workshop for detailed discussions about human factors considerations during installation and commissioning.
• It was pointed out that critical task analysis prior to carrying out installation and commissioning work can be used to identify error likely tasks. Appropriate preventive measures can then be taken to reduce the risk of error when these tasks are done.
• One study found that approximately 70% of latent errors are due to maintenance, with many occurring during outages. Therefore, it is important to have reliable post-maintenance tests to detect these latent errors (Wild et al.)
• The importance of functional tests after modifications to assess the implications of modified characteristics was raised (Wild et al.).

4. **Role of the Regulator in Human Factors in Design Changes - Summary of Discussions and Related Paper Presentations**

(a) **Process-based approach**

• There was agreement about the benefits of a process-based regulatory approach.
  o It is resource-effective for regulator to ensure an acceptable process is in place for incorporating human factors into modifications.
  o There are varying approaches to the level of detail in regulatory processes.
  o Regulatory expectations for the use of human factors in the modification process need to be defined.
• In order to ensure licensee ownership, regulators expect NPPs to set out and follow their own modification process. Most regulators expect this process to include human factors.
  o Most regulators review and agree to licensee’s modification process.

(b) **Role of the Regulator in Reviewing Design Changes**

• Many regulators approve certain changes based on their potential impact safety. Individual changes which require regulatory approval may be reviewed in detail by the regulator. In this case, the legal duty to ensure compliance may require more than process-based approach.
  o Acceptance criteria may be required for specific changes. These acceptance criteria may be context-specific and may vary between design changes. The
acceptance criteria may be impacted by factors such as risk and/or the impact of the change on human error (e.g. introduction of new error modes and validity of existing assumptions in the PRA).

- NPP's should have an internal, and possibly external, review process to ensure modifications are adequately reviewed prior to submitting them for regulatory approval.
- After design changes are installed, regulatory bodies should follow-up by reviewing operating experience.

- Most regulators evaluate modification processes to ensure the process is followed by reviewing a sample of modifications in detail.

(c) **Role of Regulatory Human Factors Staff in Reviewing Design Changes**

- Human factors professionals should be involved in regulatory reviews of major modifications and evaluations of modification processes.
- A human factors assessment of an individual modification or the modification process is often integrated with other disciplines.

5. **Areas for Improvement**

Areas for improvement were identified during the first discussion session and throughout the workshop. Recommendations to address the areas requiring improvement are in the following section.

(a) There is still reluctance to consider human factors within design teams and in general.

- The benefits of applying human factors methods are not well-publicized and accepted.
- There is often an inadequate analysis of the human performance root causes of events. Therefore, the impact of modifications on human performance may not be fully understood.
- Communication of human factors expectations with designers requires improvement. A common language is needed between human factors professionals and designers.
- There is a tendency to use administrative controls, such as procedures and training, to work around deficiencies in the design.

(b) Incorporation of human factors into minor modifications requires improvement.

- Generally, when a large modification with high safety significance is planned, human factors is adequately considered. Human factors is more likely to be neglected in smaller design changes with less safety significance.
- Many minor modifications may have a significant cumulative impact on human performance.
(c) When design work is contracted out, contracts often do not include expectations about human factors.

- When design work is contracted out, the NPP's expectations for human factors must be incorporated into the contract.
- NPPs must have "intelligent customer capability" in order to ensure the adequacy of human factors work.

(d) General Weaknesses

- Assumptions related to human performance made in probabilistic risk assessments must be reviewed and challenged by staff with human factors expertise.
- NPPs must develop a human factors culture in the modification design teams and in the workplace in general. For example, human factors needs to be embedded in event analysis, trending, procedures, and risk assessment.
- Developing a human factors culture would be assisted by using a common human factors model for all plant activities (e.g. design, event analysis / trending, staffing changes).
- Regulators can assist NPPs in developing a human factors culture by incorporating human factors into regulatory processes.

6. Recommendations

In the final discussion group, SEGHOF participants discussed the areas for improvement in Section 4.0 and how they could be addressed. This discussion and the discussion in the plenary session resulted in the following recommendations.

1. Accumulate and publicize evidence demonstrating the value of human factors in design and human factors in general.

   - Document success stories.
     - Application: Conduct and publish cost-benefit analyses of human factors activities.
     - Research: Publish studies that demonstrate the impact of integrating human factors into the modification process.

2. Improve the collection and dissemination of information about modification-related events with human performance causes.

   - Capture and disseminate information about events related to minor modifications.
   - Rather than focusing on errors made by operations and maintenance, it may also be useful to focus on errors made by designers.
   - Improve collection and dissemination of event information internationally by
     - Using international standards for root cause analysis and coding of human performance causes of events.
     - Developing a common understanding of the safety significance of events.
3. Improve integration of human factors in modification processes, especially when modifications are minor.
   • Provide guidance on incorporating human factors in minor changes.
   • Distribute models/methods used to deal with minor modifications from different countries, including screening criteria.
   • Provide guidance on addressing the cumulative impact of several minor modifications on human performance.

4. Ensure modification processes include provisions for human factors when design work is contracted out.
   • When design work is contracted out, NPPs should ensure that contractors have suitably qualified and experienced human factors staff or provisions for obtaining appropriate human factors expertise.
   • Expectations for incorporating users and human factors input in the modification should be specifically identified as a condition of modification contract in addition to delivery of the technical system.
   • NPPs should verify that the contractor is carrying out the human factors work that was specified in the contract.
   • Licensees need “intelligent customer capability” in the area of human factors. The human factors capability required to act as an “intelligent customer” must be defined.
   • There should be regulatory scrutiny of contracts.

5. Develop a human factors culture in modification design teams and in the workplace in general.
   • Continue efforts to promote human factors and educate NPPs about human factors through international guidance and regulatory advice, guidance and requirements.
   • Increase awareness about human factors within regulatory bodies.

6. Improve communication between human factors professionals and designers by developing a common language.

Problems with communication between human factors professionals and designers have been recognized, and several paper presentations described actions that are underway improve usability of human factors guidance.

• In the United Kingdom, a research project was initiated to collate and structure a large body of human factors guidance in an electronic tool that can be used by ergonomists or non-ergonomists. The tool is intended to make human factors guidance clear and unambiguous and to identify when to seek professional ergonomics support. The toolset has been distributed to the United Kingdom nuclear community (Gregson et al.).
In the United States (Naser et al.), the following types of guidance are being developed for utilities, designers, and suppliers of digital instrumentation and control replacements:

- strategic planning to help a utility develop its plant-specific control room operating concepts, endpoint vision for the control room, and migration path to achieve the endpoint vision
- regulatory, licensing and human performance program plans
- general human-system interface principles for analysis, design, and verification and validation processes and for training, simulation and performance monitoring
- detailed design guidance for specific types of HSIs
- Electricité de France has developed a tool for modification project managers to ensure a structured and systematic approach is applied for considering socio-organizational and human (SOH) aspects when modifications are planned (Quentin et al.).

In order to review modifications of CRT displays, Chung et al. are developing an updated and expanded set of user-interface guidelines. These guidelines have been compiled from existing guidelines and technical papers related to information displays on CRTs.

7. There were several topics which were discussed briefly during this workshop which could be addressed in more detail in future discussions or workshops:

- Ensuring new staff involved in modifications (NPP and regulator) understand the technical basis of the plant design
- Operating experience and expectations for human factors in temporary changes and in installation and commissioning

Papers

Chung, Y., Goo, C. and Cha, W., Regulatory experience of human factors for operating nuclear power plants.

Deutschmann, H., The Swiss modification process in nuclear power plants regulatory regime - regulator/operator process and experience related to events with safety impact.


Jeanton, G., Electricité de France organization and process concerning modifications of nuclear plants.

Juan, P., Regulatory aspects of plant's modifications to PWR.

Laakso, K., Analysis of maintenance history for identification and prevention of human CCFs originating from modifications and maintenance.
Naser, J., Hanes, L., O'Hara, J., Fink, R., Hill, D. and Morris, G., Guidelines for control room modernization as part of instrument and control modernization programs.

O'Hara, J., Kramer, J. and Persensky, J., Identifying and addressing lessons learned from plant modification programs.

Quentin, L. and Niger, D., Taking into account of socio-organisational and human aspects into upgrade packages (technical or not).

Skjerve, A.B. and Skraaning, G., A classification of validation criteria for new operational design concepts in nuclear process control.


Werdine, H., Temporary modifications and minor changes - threats to safety?

Wild, V., Reported events in German nuclear power plants due to insufficient equipment labelling.
Theme 2: How to improve the national modification processes?

Temporary and minor modifications:
Temporary changes are easy to perform, but they can transfer into permanent changes when no adequate technical or safety review is performed.

Temporary modification time should be limited, e.g. 6 months at some plants. The number of temporary modifications is a management performance indicator.

Temporary modifications do not need to be performed in hurry pushed by operating organisations. We have good time to keep a technical review meeting, and if safety related also a safety committee meeting before the implementation of the temporary modification.

Guideline and checklists related to safety are needed to be applied before implementation of safety related modifications.

Identification of minor modifications from work ordered initially as repairs or preventive maintenance.

How to identify "black" or unknown modifications. At e.g. Loviisa plant repairs of failures are ordered and executed as repairs. But a part of these repairs are reclassified into modifications within the work planning and order process of the plant.

(A part tracking process at Bruce NPP has according to shown to be good). The criteria for identification of replaceable parts such as the same function, fit, form and material, and the definition of the acceptable equipment locations at the plant are needed in the part tracking process. When a new part from a new supplier or fabrication is installed in a plant equipment location which has not been approved for the part, the replacement shall be classified as modification and tested better. The new replacement parts shall also fulfill the environmental qualification requirements, if any.

The regulatory body should review that the modification processes including minor modifications applied by the utility is good and acceptable. Review also if the utility follows the process. Results should be followed by the regulator regularly, e.g. annually, e.g. failure rates, failure modes, common cause failures. This about the modification process should be included in the utility quality assurance program.

Modifications:
All modification should be analysed and approved.
The modification should be reviewed by qualified reviewers.
All modifications require a Technical Review.
If the modification is somehow safety related, or important to safety, as determined by a qualified reviewer, a comprehensive safety review shall be done in addition to the technical review.
If the modification is safety related, the utility should notify the regulator about the modification, even in the case of minor modifications.

How spare parts evolution is monitored?
The supplier of parts, equipment or spare parts does not have knowledge of the destination of his parts or equipment.
If the spare parts are getting obsolete, and the manufacturer of spares are changed, a qualified reviewer should evaluate if the change should be undergo the modification process. The modification process requires always a technical review, and if anyhow safety related also a safety review.

Modification processes should be developed.
Different modification processes are needed for big renewal projects and small modifications.
The modifications requiring a project organisation of several persons and a small modification project
requiring only one person do not require the same modification process. A too heavy routine of small modifications contributes to resistance in the organisation, and contributes to their classification as preventive maintenance not requiring any technical or safety review.

All modifications need a technical review and if safety related a safety review, too.

The review of all modifications should include an evaluation of the functional influences of the modification and an evaluation of the coverage of functional testing and installation inspections.
ANNEX 2 - LISTE OF PARTICIPANTS

BELGIUM

Mr. Hendrik VAN DEN BERGE
Electrabel - Nuclear Generation Area Doel
Haven 1800
Scheldemolenstraat
B-9130 Doel
Tel: +32 3 730 30 59
Fax: +32 3 202 20 08
Eml: hendrik.vandenberge@electrabel.com

Mr. Yves VAN DEN BERGHE
Projects & Experience Management Div.
Association Vinçotte Nuclear (AVN)
148, rue Walcourt
1070 Bruxelles
Tel: +32 (0) 2 528 0232
Fax: +32 (0) 2 528 0102
Eml: yvd@avn.be

CANADA

Ms. Angie KOZAK
Bruce Power
PO Box 1540,
Tiverton, Ontario,
N0H 2C2
Tel: +1 519 361-5014
Fax: +1 519 361-5645
Eml: angie.kozak@brucepower.com

Mr. Gord KOZAK
Bruce Power
P.O. Box 3000, B06,
Tiverton, Ontario,
N0G 2T0
Tel: +1 519 361-4536
Fax: +1 519 36104559
Eml: gord.kozak@brucepower.com

Ms. Helen MCROBBIE
Canadian Nuclear Safety Commission
P.O. Box 1046, Station B
280 Slater Street
Ottawa K1P 5S9
Tel: +1 613 947 0956
Fax: +1 613 995 5086
Eml: mcrobbieh@cnsc-ccsn.gc.ca

Ms. Adriana NICIC
Canadian Nuclear Safety Commission
P.O. Box 1046, Station B
280 Slater Street
Ottawa,
K1P 5S9
Tel: +1 613 995 5334
Fax:
Eml: nicica@cnsc-ccsn.gc.ca
CZECH REPUBLIC

Mr. Jan VAVERA  
Dukovany NPP  
Technical Engineering Department  
Dukovany NPP  
675 50 DUKOVANY

FINLAND

Dr. Kaisa ASTRAND  
Senior Researcher  
Radiation and Nuclear Safety Authority (STUK)  
P.O.Box 14,  
FIN-00881 Helsinki

Dr. Kari LAAKSO  
Senior Research Scientist  
VTT Industrial Systems  
P.O.Box 1301,  
FIN-02044 VTT

Dr. Leena NORROS  
Senior Research Scientist  
VTT Industrial Systems  
P.O.Box 1301,  
FIN-02044 VTT

FRANCE

Ms. Maud BOEL  
EDF/DPN/CAPE/GMS  
Site Cap Ampère  
1, place Pleyel  
93282 SAINT-DENIS CEDEX

Mme Geneviève FILIPPI  
R&D EDF  
1 av du Général de Gaulle,  
92140 Clamart

Mr. Gérard JEANTON  
UNIPE/DE - Electricité de France  
9 rue des cuirassiers  
BP 3181  
69402 LYON

Mr. Jean-Paul LABARTHE  
Electricité de France – R&D  
Management des Risques Industriels,  
1 avenue du Général de Gaulle  
92141 Clamart Cedex France
Mme Valérie LAGRANGE  
EDF DPN/EM  
1 place Pleyel 93282 St Denis  
93282 SAINT DENIS

Tel: +33 (0) 43 69 31 81  
Fax:  
Eml: valerie.lagrange@edf.fr

Mme Brigitte LE GUILCHER  
EDF R&D  
Recherche et Développement,  
1 Avenue du Général de Gaulle  
92141 CLAMART CEDEX

Tel: +33 (0) 47 65 58 94  
Fax: +33 (0) 47 65 51 73  
Eml: brigitte.le-guilcher@edf.fr

Mr. Jean-Christophe NIEL  
Director of Strategy Development & External Relations  
Institut de Radioprotection et de Sûreté Nucléaire  
B.P. No. 17,  
92265 Fontenay-aux-Roses Cedex

Tel: +33 1 58 35 86 64  
Fax: +33 1 58 35 91 24  
E-mail: jean-christophe.niel@irsn.fr

Mr. Didier NIGER  
EDF/DPN/UNIPE(BEM)  
Site cap ampère  
1, place pleyel  
93282 SAINT-DENIS CEDEX

Tel: +33 (0) 1 43 69 39 37  
Fax:  
Eml: didier.niger@edf.fr

Mr. Bernard PAPIN  
DEN/ DER/ STR  
CEA CADARACHE  
F-13108 St. PAUL LEZ DURANCE Cedex

Tel: +33 04 42 25 22 58  
Fax: +33 04 42 25 24 08  
Eml: bernard.papin@cea.fr

Mr. Dominique PIRUS  
EDF-SEPTEN  
12-14 Ave DUTRIEVOZ  
69628 VILLEURBANNE CEDEX

Tel: +33 (0)4 72 82 74 77  
Fax: +33 (0)4 72 82 77 44  
Eml: dominique.pirus@edf.fr

Ms. Laure QUENTIN  
EDF/DPN/CAPE/GMS  
Site cap ampère  
1, place pleyel  
93282 SAINT-DENIS CEDEX

Tel: +33 (0)1.43.69.33.08  
Fax:  
Eml: laure.quentin@edf.fr

Mr. Daniel TASSET  
DGSNR/SD2  
Route du Panorama Robert Schuman  
BP 83  
92266 Fontenay-aux-Roses Cedex

Tel: +33 (0)1 43.19.71.56  
Fax: +33 (0)1 43.19.70.89  
E-mail: daniel.tasset@asn.minefi.gouv.fr

M. Jean-François VAUTIER  
DPSN  
Commissariat Energie Atomique  
CEA/Saclay  
91191 Gif-sur-Yvette Cedex

Tel: +33 1 69 08 79 37  
Fax: +33 1 69 08 79 13  
Eml: jean-francois.vautier@cea.fr

Mr. Didier WATTRELOS  
IRSN/DSR  
B.P. 6  
F-92265 Fontenay-aux-Roses Cedex

Tel: +33 1 5835 7833  
Fax: +33 1 5835 3560  
E-mail: didier.wattrelos@irsn.fr
**GERMANY**

Dr. Michael MAQUA  
Gesellschaft für Anlagen- und Reaktorsicherheit mbH (GRS)  
Schwertnergasse 1  
D-50667 Köln  
Tel: +49 221 2068 718  
Fax: +49 221 2068 702  
Eml: maq@grs.de

Mr. Volker WILD  
GRS  
Schwertnergasse 1, 50667 Cologne  
Tel: +49 221 2068 761  
Fax: +49 221 2068 892  
Eml: wil@grs.de

**KOREA (REPUBLIC OF)**

Mr. Yun Hyung CHUNG  
Principal Researcher, Regulatory Safety Division  
Korea Institute of Nuclear Safety  
19 Guseong-Dong  
Yusung-gu  
Taejon, 305-600  
Tel: +82 42 868 0245  
Fax: +82 42 861 9945  
Eml: yhchung@kins.re.kr

Mr. Won-Dea JUNG  
Integrated Safety Ass. Team  
KAERI  
P.O. Box 105  
Yusong,  
Taejon 305-600  
Tel: +82 42 868 8296  
Fax: +82 42 868 8374  
Eml: wdjung@kaeri.re.kr

**NETHERLANDS**

Dr. Roberto MAY  
European Commission  
P.O. Box 2  
1755 ZG - Petten  
Tel: +31 224 56 5121  
Fax: +31 224 56 5615  
Eml: roberto.may@jrc.nl

Ms. Anna MENGOLINI  
EC-JRC  
Post office Box 2,  
NL- 1755 ZG Petten  
Tel: +31 224 565253  
Fax: +31 224 565641  
Eml: anna.mengolini@jrc.nl

**NORWAY**

Mr. Andreas BYE  
Institute for Energy Technology  
OECD Halden Reactor Project  
P.O.Box 173,  
NO-1751 Halden  
Tel:  
Fax: +47 69 21 24 60  
Eml: andreas.by@hrp.no
Mrs. Ann Britt SKJERVE
Section Head, Safety & Organisation
Institute for Energy Technology, OECD Halden React
P.O.Box 173,
NO-1751 Halden

Tel: +47 69 21 22 30
Fax: +47 69 21 24 60
Eml: ann.britt.skjerve@hrp.no

SPAIN

Mr. Luis ASENSIO
Almaraz NPP
A.I.E. Centrales Nucleares Almaraz Trillo,
Apartado 74 Navalmoral de la Mata,
10300 Cáceres

Tel: +34 927 545090
Fax:
Eml: lar@cnat.es

Mr. Blas FERNANDEZ MADRID
Asociación Nuclear Ascó-Vandellós II
A.I.E.
Apartado de correos, 48
43890 L’Hospitalet de l’Infant
Tarragona

Tel: +34 + 34 977 818800
Fax: +34 977 818943
Eml: bfernandez@anacnv.com

Mr. Benito GIL
PSA & Human Factors Division
Consejo de Seguridad Nuclear
C/ Justo Dorado, 11
28040 Madrid

Tel: +34 91 3460 256
Fax: +34 91 3460 496
Eml: bgm@csn.es

Mr. Roberto MIJANGOS
Sta. María de Garoña NPP (Nuclenor)
C. N. Sta. María de Garoña
Valle de Tobalina
09212 BURGOS

Tel: +34-947.34.94.00
Fax: +34-947.34.94.40
Eml: roberto.mijangos@nuclenor.es

Mr. Luis PENA
Almaraz-Trillo N.P.P’s
A.I.E. Centrales Nucleares Almaraz Trillo,
Pl Carlos Trías Bertrán,
Edif Sollube planta 7ª,
28020 Madrid

Tel: +34 91 5559111
Fax:
Eml: lpa@cnat.es

Mr. Antonio TOCA
Sta Maria de Garoña NPP (Nuclenor SA)
Hernan Cortes nº 26,
39003 Santander

Tel: +34-942.24.51.00
Fax: +34-942.24.51.23
Eml: antonio.toca@nuclenor.es

SWEDEN

Mr. Olle ANDERSSON
Avdelning FQ
Forsmarks Kraftgrupp AB
S-742 36 ÖSTHAMMAR

Tel: +46 173 81367
Fax: +46 173 81850
Eml: oas@forsmark.vattenfall.se
Ms. Anna Maria OSTLUND  
Swedish Nuclear Power Inspt.  
Klarabergsviadukten 90  
S-10658 STOCKHOLM  
Tel: +46 8 698 8671  
Fax: +46 8 661 9086  
Eml: annamaria.ostlund@ski.se

Dr. Per-Olof SANDEN  
Department of Man-Technology Organisation  
Swedish Nuclear Power Inspt.  
Klarabergsviadukten 90  
S-10658 STOCKHOLM  
Tel: +46 8 698 8473  
Fax: +46 8 661 9086  
Eml: perolof.sanden@ski.se

SWITZERLAND

Mr. Daniel BILLETER  
Hauptabteilung für die Sicherheit  
der Kernanlagen (HSK)  
5232 Villigen-HSK  
Tel: +41 56 310 39 35  
Fax: +41 56 310 49 35  
Eml: Daniel.Billeter@hsk.psi.ch

Mr. Herbert DEUTSCHMANN  
Division of Reactor Safety  
Swiss Federal Nuclear Safety  
Inspectorate (HSK)  
CH-5232 Villigen HSK  
Tel: +41 56 310 3811  
Fax: +41 56 310 3907  
Eml: herbert.deutschmann@hsk.psi.ch

UNITED KINGDOM

Mr. David GREGSON  
Synergy Consultants Ltd  
Chirnside  
Scrooby  
Doncaster DN10 6AJ  
Tel: +44 1332239372  
Fax:  
Eml: dave.gregson@synergy-ergs.com

Mr. Ed MARSHALL  
Synergy Consultants Ltd  
Chirnside  
Scrooby  
Doncaster DN106AJ  
Tel: +44 1302711447  
Fax:  
Eml: ed.marshall@synergy-ergs.com

Dr. Craig REIERSSEN  
Health & Safety Executive  
NII - Stanley Precinct  
St. Peter's House, Balliol Road  
Bootle, Merseyside L20 3LZ  
Tel: +44 151 951 3650  
Fax: +44 151 951 3942  
Eml: craig.reierssen@hse.gsi.gov.uk

UNITED STATES OF AMERICA

Mr. Hossein G. HAMZEHEE  
PRA Branch  
USNRC  
Two White Flint North,  
11545 Rockville Pike,  
Rockville, MD 20852-2738  
Tel: +1 (301)415-6228  
Fax: +1 (301)415-5062  
Eml: hgh@nrc.gov
Mr. Joel J. KRAMER
US Nuclear Regulatory Commission
11545 Rockville Pike
Rockville MD 20852
Tel: +1 301 415 5891
Fax: jjkl@nrc.gov

Dr. Joseph NASER
Manager, Instrumentation and Control
EPRI
3412 Hillview Avenue
Palo Alto, CA 94304-1395
Tel: +1 650 855 2107
Fax: +1 650 855 8759
Eml: jnaser@epri.com

Mr. John O'HARA
Brookhaven National Laboratory
Building 130,
Upton,
New York, 11973
Tel: +1-631-344-3638
Fax: +1-631-344-4900
Eml: ohara@bnl.gov

INTERNATIONAL ORGANISATIONS

International Atomic Energy Agency (IAEA)

Dr. Friedrich E. NIEHAUS
Head, Safety Assessment Section
IAEA Room B0852
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna
Austria
Tel: +43 1 26000 22036
Fax: +43 1 26007
E-mail: f.niehaus@iaea.org

Mr. Terence TAYLOR
International Atomic Energy Agency
Wagramerstrasse 5
PO Box 100
A-1400 Vienna
Austria
Tel: +43 1 2600 26179
Fax: +43 1 26007
E-mail: t.taylor@iaea.org

Mr. Humberto WERDINE Jr.
Senior Operational Safety Officer
IAEA
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna
Austria
Tel: +43 1 2600 2 6079
Fax: +43 1 26007
Eml: h.werdine@iaea.org

OECD Nuclear Energy Agency, Issy-les-Moulineaux

Dr. Pekka PYY
Nuclear Safety Division
OECD Nuclear Energy Agency
Le Seine Saint-Germain - Bât. B
12 boulevard des Îles
92130 Isssy-les-Moulineaux
France
Tel: +33 01 45 24 1054
Fax: +33 01 45 24 1129
Eml: pekka.pyy@oecd.org
World Association of Nuclear Operators, Paris (WANO)

Mr. Weiping ZHENG
WANO - Paris Centre
43 rue Vincouse
75116 Paris
France

Tel: +33 01 53 70 35 74
Fax: +33 (0)1 53 70 35 53
Eml: weiping.zheng@wanopc.org
Joint CSNI WGOE/SEGHOF Workshop

"Modifications at Nuclear Power Plants – Operating Experience, Safety Significance and the Role of Human Factors"

organised by
the OECD/NEA

In cooperation with the Institut de Radioprotection et de Sûreté Nucléaire (IRSN)

OECD Headquarters, La Muette
Paris, France
6-8 October 2003

CALL FOR PAPERS

Deadline for abstracts: 15 May, 2003
Notification of authors: 20 June, 2003
Submission of full papers and registration: 15 September, 2003
CALL FOR PAPERS

1 MAIN OBJECTIVE
The general objective of the workshop is to bring experts together to exchange and disseminate information about the safety aspects of NPP modifications. International experience of events and modification processes will be disseminated during the workshop. A principal aim is to share and discuss good practices for regulators and licensees. Task forces of the CSNI Working Group on Operating Experience (WGOE) and Special Expert group on Human and Organisational Factors (SEGHOF) will present their ongoing activities. The workshop results will be used to steer international developments in the area of NPP modification safety. It is expected that the results will also aid participants to manage and regulate modifications more effectively in their countries.

2 WORKSHOP BACKGROUND
Operating experience repeatedly shows that modifications at nuclear power plants (NPPs) may lead to safety significant events. At the same time, modifications are necessary to ensure the economic and safe functioning of NPPs. Human input is made at different stages of the plant modification process, and these inputs may compromise safety if not properly specified and understood. Finally, the plant personnel has to operate and maintain the altered or changed equipment, which may lead to different types of problems.

The background of this joint workshop are two initiatives proposed by CSNI task forces: the WGOE “Minor modifications and their safety significance” and the SEGHOF “Human and Organisational Factors in NPP Modifications”. The emphasis will be on addressing these topics. However, the workshop will not exclude other areas related to NPP modifications, their management and regulation.

The impulse for the WGOE task “Minor modifications and their safety significance” is that operating experience feedback has revealed safety relevant events caused by minor changes in components, materials or spare parts. These modifications were not initially recognised as being safety significant, but nonetheless presented a real challenge to the safety of nuclear power reactors. Such minor or non-identified modification events (MiNIMs) can reduce significantly the availability and reliability of equipment important for safety, and they can even generate common cause failures. Moreover, if the problem can only be revealed when operating in accident conditions, as for standby safety systems, it can be considered as a latent fault. Such anomalies are may not be always identified by preoperational or periodic tests. Furthermore, if the mechanism is spread through the nuclear power stations (e.g. wrong lubricant or widely used spare part), it may be difficult to carry out corrective actions in a timely manner.
SEGHOF recognises and shares the concerns identified by WGOE. NPPs undergo technical changes throughout their lifecycle that may have an impact on safety. Technical or document modifications may result either from regulatory issues or for internally driven reasons, e.g. to replace ageing equipment. These modifications can have an impact on the operation and/or maintenance of the installation and, in turn, may present new challenges to plant personnel who are competent and experienced in using different equipment. Organisational changes are excluded from the scope of this workshop, since they are covered by other SEGHOF activities.

3 WORKSHOP TOPICS

The following main topics will be discussed during the workshop:

1. Safety implications of events due to NPP modifications;
2. Differences in approach to regulating and managing significant and minor modifications;
3. Examples of different types of modification processes, their key elements and (both regulatory and licensee) guidelines dealing with modifications in NEA member countries;
4. Why and how human and organisational factors need to be considered in relation to modification processes;
5. Identified or proven good practices to deal with modifications in regulation and in safety management;
6. Identification of topics which deserve further attention from the CSNI and its working groups.

Different types of sessions, including breakout group discussions, will be organised during the workshop on these subjects.

4 EXPECTED PARTICIPATION

A wide participation of NPP owners and operators, NPP designers and vendors, industry associations, regulatory organisations and their technical support organisations, national laboratories, and public interest representatives in NEA member countries will be welcomed.

5 ABSTRACTS AND PAPERS

A concise abstract between 100 and 300 words in length and the title of the intended paper should be submitted before 15 May, 2003 to the following addresses (4 copies):

Workshop chairs

<table>
<thead>
<tr>
<th>Mr. Daniel TASSET</th>
<th>Mr. Didier WATTRELOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRSN/DES/SEFH</td>
<td>IRSN/DES/SEREP</td>
</tr>
<tr>
<td>B.P. No. 17</td>
<td>B.P. N° 17</td>
</tr>
<tr>
<td>F-92262 FONTENAY-AUX-ROSES CEDEX</td>
<td>F-92262 FONTENAY-AUX-ROSES CEDEX</td>
</tr>
<tr>
<td>FRANCE</td>
<td>FRANCE</td>
</tr>
</tbody>
</table>

Tel: +33 (0)1 58 35 84 03  
Fax: +33 (0)1 58 35 88 40  
E-mail: daniel.tasset@irsn.fr  
Tel: +33 (0)1 58 35 78 33  
Fax: + 33 (0)1 46 54 35 60  
E-mail: didier.wattrelos@irsn.fr
Authors of approved presentations should send a master copy of their paper to the NEA secretariat before 15 September, 2003 so that pre-prints of the papers can be made available for participants at the beginning of the workshop.

6 DEADLINES

Deadline for abstracts: 15 May, 2003
Programme Committee meeting: 6 June 2003
Notification of authors: 20 June, 2003
Submission of full papers: 15 September, 2003
Workshop Registration: 15 September, 2003
Date of Workshop: 6-8 October, 2003

7 WORKSHOP ARRANGEMENTS

7.1 Proceedings
The proceedings of the workshop together with a specific chapter containing the summary and conclusions will be issued as a CSNI report. It will distributed after the meeting to the participants of the workshop, members of CSNI, CNRA, WGOE and SEGHOF.

7.2 Working language
The working language of the workshop will be English.

7.3 Hotel reservation
A list of hotels in the vicinity of OECD Headquarters (La Muette) exists at: http://www.nea.fr/html/general/oeccd-hotels.html.

7.4 Registration fee
There will be no registration fee for the workshop but the costs for refreshments and meals will be borne by the participants.

7.5 Social event
A social event hosted by IRSN is planned to be organised during the workshop.
7.6 Organising committee
The following persons form the organising committee of the workshop:

- Mr. Didier Wattrelos, IRSN (F)
- Dr. M. Maqua, GRS (D)
- Mr. Daniel Tasset, IRSN (F)
- Ms. H. Mcrobbie, CNSC (CAN)
- Mr. A. Vandewalle, AVN (B)
- Mr. Y. van den Berghe, AVN (B)
- Mr. Deutschmann, HSK (CH)
- Mr. T. Taylor, IAEA
- Mr. S. Tamao, NUPEC (J)
- Dr. P. Pyy, NEA
- Mr. F. van Iddekinge, VROM (NL)

7.7 Meeting information
Practical information on the workshop will be made available on the NEA website: http://www.nea.fr/html/nsd/workshops/modifications/welcome.html.

For any additional information, please contact the NEA secretariat (notice to send abstracts to all four involved parties as indicated before):

Dr. Pekka T. Pyy
OECD Nuclear Energy Agency
Le Seine St Germain
12 Boulevard des Iles
F- 92130 Issy-les-Moulineaux, France
Tel: +33 1 45 24 10 54
Fax: +33 1 45 24 11 29
E-mail: pekka.pyy@oecd.org
Joint CSNI WGOE/SEGHOF Workshop
"Modifications at Nuclear Power Plants – Operating Experience, Safety Significance and Role of Human Factors"

Registration / Abstract Form

See also the on-line version at: http://www.nea.fr/html/nsd/workshops/modifications/registration.html (it goes to chairs & secretariat automatically)

In response to the announcement and call for papers we inform you of the nomination of

<table>
<thead>
<tr>
<th>Title, Name, Surname:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Position:</td>
<td></td>
</tr>
<tr>
<td>Organisation:</td>
<td></td>
</tr>
<tr>
<td>Address:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Tel:</td>
<td>Fax:</td>
</tr>
<tr>
<td>E-mail:</td>
<td></td>
</tr>
</tbody>
</table>

Title of my presentation (abstract to be added, if any):

Please return the registration form by September 15th 2003, at the latest, to (do not forget to send your eventual abstract to the workshop chairmen by May 15th):

Dr. Pekka T. Pyy
OECD Nuclear Energy Agency
Le Seine St Germain
12 Boulevard des Iles
F- 92130 Issy-les-Moulineaux, France
Tel: +33 1 45 24 10 54
Fax: +33 1 45 24 11 29
E-mail: pekka.pyy@oecd.org

(In case you want to use this MS Word form, a normal email or any other means (and not the on-line registration/abstract form at: http://www.nea.fr/html/nsd/workshops/modifications/registration.html), please, make sure that all the information is included)
Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Cooperation and Development shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original Member countries are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), the Republic of Korea (12th December 1996) and the Slovak Republic (14th December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full Member. NEA membership today consists of all European Member countries of OECD as well as Australia, Canada, Japan, the Republic of Korea, Mexico and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its Member countries in maintaining and further developing, through international cooperation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency (IAEA), with which it has a Cooperation Agreement, as well as with other international organisations in the nuclear field.
CSNI

The NEA Committee on the Safety of Nuclear Installations (CSNI) is an international committee made up of senior scientists and engineers, with broad responsibilities for safety technology and research programs, and representatives from regulatory authorities. It was set up in 1973 to develop and coordinate the activities of the NEA concerning the technical aspects of the design, construction and operation of nuclear installations insofar as they affect the safety of such installations. The Committee's purpose is to foster international cooperation in nuclear safety amongst the OECD Member countries. CSNI's main tasks are to exchange technical information and to promote collaboration between research, development, engineering and regulation organisations; to review the state of knowledge on selected topics of nuclear safety technology and safety assessments, including operating experience; to initiate and conduct programs to overcome discrepancies, develop improvements and reach consensus on technical issues; to promote coordination of work, including the establishment of joint undertakings.

SEGHOF

The OECD Committee on the Safety of Nuclear Installations (CSNI) established a Special Experts' Group in Human and Organisational Factors (SEGHOF) in 2000. The main missions of SEGHOF are to improve the current understanding, to advance the utilisation of methodologies for human and organisational factor assessment and to address emerging safety issues in order to maintain and to improve the safety of nuclear installations in Member countries. SEGHOF constitutes a forum for exchange of information, methods and experience about safety-relevant human and organisational issues and programmes in Member countries. SEGHOF has continued, and built upon, the work of its predecessor, the Expanded Task Force on human and organisational factors (ETF) which has existed since 1984.

WGOE

The main mission of the CSNI Working Group of Operating Experience (WGOE) is to analyse and develop insights from operating experience, in particular the safety significance of operating events, and to communicate these insights to CSNI, CNRA (Committee on Nuclear Regulatory Activities) and government and industry bodies. The functions of the WGOE include the review and analysis of operating experience from nuclear power plants and fuel cycle facilities, the development of improved techniques and methods for the review of operating events, the operation and maintenance of operating experience data bases (common cause failures, computer-based control systems important to safety, human performance) and Incident Reporting System (IRS) with IAEA.