IAEA Nuclear Energy Series

No. NP-T-3.10

Basic Principles

Objectives

Guides

Technical Reports

Integration of Analog and Digital Instrumentation and Control Systems in Hybrid Control Rooms

IAEA
International Atomic Energy Agency

IAEA NUCLEAR ENERGY SERIES PUBLICATIONS

STRUCTURE OF THE IAEA NUCLEAR ENERGY SERIES

Under the terms of Articles III.A and VIII.C of its Statute, the IAEA is authorized to foster the exchange of scientific and technical information on the peaceful uses of atomic energy. The publications in the **IAEA Nuclear Energy Series** provide information in the areas of nuclear power, nuclear fuel cycle, radioactive waste management and decommissioning, and on general issues that are relevant to all of the above mentioned areas. The structure of the IAEA Nuclear Energy Series comprises three levels: **1 — Basic Principles and Objectives; 2 — Guides; and 3 — Technical Reports.**

The **Nuclear Energy Basic Principles** publication describes the rationale and vision for the peaceful uses of nuclear energy.

Nuclear Energy Series Objectives publications explain the expectations to be met in various areas at different stages of implementation.

Nuclear Energy Series Guides provide high level guidance on how to achieve the objectives related to the various topics and areas involving the peaceful uses of nuclear energy.

Nuclear Energy Series Technical Reports provide additional, more detailed, information on activities related to the various areas dealt with in the IAEA Nuclear Energy Series.

The IAEA Nuclear Energy Series publications are coded as follows: **NG** — general; **NP** — nuclear power; **NF** — nuclear fuel; **NW** — radioactive waste management and decommissioning. In addition, the publications are available in English on the IAEA's Internet site:

http://www.iaea.org/Publications/index.html

For further information, please contact the IAEA at PO Box 100, Vienna International Centre, 1400 Vienna, Austria.

All users of the IAEA Nuclear Energy Series publications are invited to inform the IAEA of experience in their use for the purpose of ensuring that they continue to meet user needs. Information may be provided via the IAEA Internet site, by post, at the address given above, or by email to Official.Mail@iaea.org.

INTEGRATION OF ANALOG AND DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS IN HYBRID CONTROL ROOMS

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHRAIN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA
VIETNAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world''.

IAEA NUCLEAR ENERGY SERIES No. NP-T-3.10

INTEGRATION OF ANALOG AND DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS IN HYBRID CONTROL ROOMS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2010

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
September 2010
STI/PUB/1470

IAEA Library Cataloguing in Publication Data

Integration of analog and digital instrumentation and control systems in hybrid control rooms. — Vienna : International Atomic Energy Agency, 2010.
p. ; 29 cm. — (IAEA nuclear energy series, ISSN 1995–7807 ; no. NP-T-3.10)
STI/PUB/1470
ISBN 978–92–0–107710–3
Includes bibliographical references.

1. Nuclear power plants – Control rooms. 2. Nuclear power plants – Management. 3. Control systems. I. International Atomic Energy Agency. II. Series.

IAEAL 10–00651

FOREWORD

The IAEA's activities in the area of nuclear power plant operating performance and life cycle management are aimed at increasing Member State capabilities in utilizing good engineering and management practices as developed and transferred by the IAEA. In particular, the IAEA supports the improvement of nuclear power plant performance, plant life management, training, power uprating, operational license renewal, and the modernization of instrumentation and control (I&C) systems of plants.

The issue of the integration of analog and digital I&C systems in hybrid control rooms was suggested by the IAEA Technical Working Group on Nuclear Power Plant Control and Instrumentation (TWG-NPPCI) at its meetings in 2003 and 2005. The subject was then approved by the IAEA and included in its work programmes for 2006–2009.

The purpose of this report is to help nuclear utilities in planning control room and other human system interface (HSI) changes, making appropriate use of modern technologies. These technologies would aid in managing ageing and obsolescence, and facilitate improvements in plant performance and safety. This report covers a broad spectrum of potential changes to the control room ranging from the replacement of a few obsolete components with newer digital devices to a fully computerized control room.

New digital technologies offer significant opportunities to improve access to and presentation of information to the user, e.g. operators, maintenance staff and management. However, this technology should be used prudently. In some cases, modernization is undertaken to resolve ageing and obsolescence or to meet regulatory requirements for license renewal. The integration of new technologies during main control room (MCR) modernizations should be performed cautiously and all affected aspects of plant maintenance, and operation should be carefully considered, paying particular attention to the human factors elements of these aspects.

This report describes a formal, well planned approach to modernization, which involves all stakeholders from the utility, design organizations and regulatory authorities. A modernization plan should be based on a long term vision and take into account plant performance data, experiences in similar plants and evolving I&C technologies.

While the modernization of MCRs, resulting in hybrid technologies, is often conducted in response to ageing and obsolescence, it is important to keep in mind that one must also plan for the eventual maintenance and/or replacement of these new digital systems.

In the case where the modernization of the control room will be done in several incremental steps over several outage cycles, the utilities need to develop a migration path that defines how the incremental activities will lead to the final end point vision of the control room and HSIs. It is important to remember that the control room and HSIs must be fully operational and support safe operation of the plant under all conditions at each step of the modernization programme.

The IAEA wishes to thank all participants and their Member States for their valuable contributions.The Chairpersons of the meetings where this report was drafted were J. Naser and B. Rasmussen (USA) and J. de Grosbois (Canada). The IAEA officer responsible for this publication was O. Glöckler of the Division of Nuclear Power.

EDITORIAL NOTE

This report has been edited by the editorial staff of the IAEA to the extent considered necessary for the reader's assistance. It does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

The majority of instrumentation and control (I&C) equipment in nuclear power plants in the world was designed at least 30 to over 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 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. License extension means that plants must be supported longer, which will increase obsolescence issues. In addition, older technology limits the possibilities for adding new beneficial capabilities to the plant systems and interfaces. New technology provides the opportunity to improve plant performance, human-system interfaces (HSI) functionality, and reliability; to enhance operator performance and reliability, and to address difficulties in finding young professionals with education and experience with older analog technology. Finally, there may be changes in regulatory requirements that could necessitate modernization activities.

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 currently a major issue for nuclear power plants worldwide. A number of nuclear power utilities are committing to major modernization programmes. The need for this modernization will accelerate as plants age, obsolescence issues increase, plants receive license renewals, and features that digital technology offers are needed to increase cost effective electricity production. As an integral part of the I&C modernization programme at a nuclear power plant, the control room and other 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.

Plant personnel play a vital role in productive, efficient, and safe generation of power. Operators monitor and control the plant to ensure it is functioning properly. Test and maintenance personnel help ensure the equipment is functioning properly and restore components when malfunctions occur. Personnel performance and the resulting plant performance is influenced by many aspects of plant design, including the level of automation, personnel training, and the interfaces provided for personnel to interact with the plant. These interfaces include alarms, displays, and controls that are located in the main control room (MCR) and numerous local control stations situated throughout the plant. HSIs are also located in support facilities.

The plant I&C and HSI modifications can impact the role of personnel, the tasks to be performed and the way they are performed, and the knowledge, skills and training required of personnel. As part of modernization, HSIs are becoming more computer based, incorporating features such as soft controls and computerized procedures, touch-screen interfaces, sit-down workstations, and large screen overview displays. Computer based technologies are integrated into control rooms that were largely based on conventional technology resulting in hybrid control rooms.

While plant modernization can greatly improve personnel and plant performance, it is important to recognize that, if poorly planned, designed or implemented, there is the potential to negatively impact performance and reduce human reliability; resulting in a detrimental effect on safety and cost effective power production. Human factors engineering (HFE) is needed to ensure that the benefits of the new technology are realized and problems with its implementation are minimized. A discussion of some of the issues that arise when HFE is not properly addressed is given in the control room guidelines developed by the Electric Power Research Institute [8].

1.1.1. Definition of hybrid

The term hybrid system denotes any system that is built on heterogeneous technological solutions. Examples are combining hard and soft controls, different generations of analog and digital equipment, and different control system technologies.

1.1.2. Drivers and constraints

At certain intervals, the process industry at large experiences major changes in technological solutions. One important example of this is the change from analog to digital I&C. The potential benefits of implementing digital technology include more efficient operations and maintenance, leading to improved power plant availability and safety through the avoidance of transients, forced outages, and unnecessary shutdowns. New digital systems provide the opportunity to give personnel information they did not have with conventional systems. Improved instrumentation and signal validation techniques can help to ensure that the information is more accurate, precise, and reliable. In addition, data processing techniques and the flexibility of computer based information presentation enable designers to present information in ways that are much better suited to personnel tasks and information processing needs to achieve more efficient, cost effective power production.

The modernization of the existing MCR may be motivated by the need to enhance the safety and availability of the NPP. The utilities' MCR modernization approaches can be decided considering the purpose of the modernization, the available budget and schedule, licensing requirements, operators' request, degree of existing systems' ageing, remaining lifetime, etc.

The most common constraints result from licensing and regulatory compliance, technology available in the marketplace, the space in the MCR and I&C rooms and project internal constraints, such as budget and schedule.

1.1.3. Overview on possible solutions

The modernization approaches can be typically categorized into three different types in terms of complexity and degree of modification as follows:

— Type 1 — Component-by-component replacement approach.

This is the simplest approach to replace the old instruments and controllers on the control panels with new ones on a one to one base. The new instruments and controllers may be driven by digital devices such as microprocessors; however their functions are almost identical to the old ones.

— Type 2 — Hybrid (can be a goal or a step towards end vision) approach.

This approach takes the mid way between the Type 1 and Type 3 approaches. The instruments and controllers in the MCR will be replaced with new ones. Some of them may be integrated into video display units (VDUs) as a shared indicators and controllers. Some VDUs will be added in the MCR for enhancing the functionality, efficiency and safety of the operation.

— Type 3 — Fully computerized control room approach.

This is the most comprehensive modernization approach by which all the existing devices and panels in the MCR will be replaced by fully computerized VDUs on the compact workstation type operation consoles. Not only the indications but also the control functions can be accomplished on VDUs using soft controls. Future expansion of functions and capabilities should be considered in the implementation of modernization.

Most modernizations are either Type 1 or Type 2. Type 3 is conceptual with respect to modernizations and is more likely to apply to new plants.

The advantages and disadvantages of the three different approaches can be summarized as follows:

	Type 1	Type 2	Type 3
Advantages	Minimized budget and schedule for the MCR modernization. Minimized effort for the verification and validation (V&V) and retraining of existing operators. Minimize the cable replacement.	Expand the functionalities of MCR with relevant budget and schedule. Save efforts for the V&V and retraining of the operators compared with Type 3. Easy to get licensing for the new MCR by adding current licensing requirements and less software V&V.	Maximize the addition of new functionalities to enhance the performance and reliabilities of operation by utilizing advanced information technologies. Easy to accommodate future system changes due to the flexible nature of software.
Disadvantages	No improvement of MCR functionalities. Hard to implement new licensing requirements issued since the initial operation of the nuclear power plant.	Hard to satisfy both conservative and progressive requirements for MCR modification.	Maximized budget and schedule for the modernization and licensing. Maximized operator retraining efforts.

1.2. SCOPE AND INTENDED USERS

This report is focused on topics related to the use of multiple technologies in a hybrid MCR in order to achieve a consistent and harmonized operational environment.

The scope of this report covers a wide spectrum of control room and HSI modernizations from small additions of digital technology through like for like replacements to a more substantial replacement of multiple panels in the MCR. The new control room may include HSIs that are computer based and may incorporate features such as soft controls, computer based procedures, touch-screen interfaces, sit-down workstations, and large-screen overview displays. In addition, more advanced information technology which may be incorporated in future plants are discussed in [1].

In many, if not most cases, modernized control rooms will be the result of incremental steps over several fuel cycle outages. The resulting control room and HSIs at each of the incremental modernization steps will be a combination of different technologies resulting in a hybrid control room. As an example, after each modernization step, the amount of analog technology may decrease and the amount of digital technology may increase. This means that the HSIs will keep changing until the modernization programme is completed.

The guidance provided in this report will help utilities, their suppliers, and their contractors to plan, design, and execute MCR modernizations to achieve the desired benefits and avoid the potential downfalls.

1.3. REPORT STRUCTURE AND RELATION TO OTHER PUBLICATIONS

1.3.1. The IAEA Nuclear Energy Series publication structure/hierarchy

This section describes the publication structure relevant to the I&C area to assist the reader in illustrating how this introductory reference publication links the IAEA literature related to I&C and how they are categorized.

This report was prepared as part of the IAEA Nuclear Energy Series (NES) introduced in 2007. The NES has three levels:

— Level 1 — Nuclear Energy Basic Principles and Objectives;
— Level 2 — Nuclear Energy Series Guides;
— Level 3 — Nuclear Energy Series Technical Reports.

The Level 1 publication (Nuclear Energy Basic Principles) describes the rationales and vision for the peaceful use of nuclear energy and it represents the foundation for all other publications in the series. Following the Basic Principles, the Nuclear Energy Series Objectives publications describe what needs to be achieved in the following four areas:

— General;
— Nuclear power;
— Nuclear fuel cycle;
— Radioactive waste management and decommissioning.

The Level 2 publications (Nuclear Energy Series Guides) describe how to achieve the objectives related to the various specific topics under the above four main areas.

The Level 3 publications (Nuclear Energy Series Technical Reports) provide a detailed technical background on specific nuclear energy topics. An example of the latter is NP-T-1.1, entitled On-line Monitoring for Improving Performance of Nuclear Power Plants Part 1: Instrument Channel Monitoring (2008).

The current report is published as a Nuclear Energy Series Technical Report in the subcategory of Operation of Nuclear Power Plants (NP-T-3.10).

Before the introduction of the NES, the IAEA published its I&C related reports as Technical Documents (TECDOCs), and in the Technical Reports Series (TRS). I&C related examples are IAEA-TECDOC-1402 Management of Life Cycle and Ageing at Nuclear Power Plants: Improved I&C Maintenance (2004), and Technical Reports Series No. 387, Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook (1999).

The other series where publications related to I&C can be found is the IAEA Safety Standards Series. In general, this series covers nuclear safety, radiation safety, transport safety, waste safety and also general safety. The categories within the series are Safety Fundamentals, Safety Requirements and Safety Guides. An example of the latter is Safety Guide No. NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants.

1.3.2. Organization of this report

This report contains five main sections referred to as the main body of the report, followed by references and a glossary.

Section 1 gives the background and overview of the scope of the report, and defines the objectives and the intended audience of the report. Section 2 presents a comprehensive description of the factors influencing strategic decision making, planning and project management. In Section 3, a technical description of the components and systems that can be the subjects of modernization projects is given. Section 4 describes the steps and various options of project management and execution, including project life cycle, licensing, human factors, testing, V&V, and training. Recommendations given in the main part are summarized in Section 5 as conclusions.

2. STRATEGIC DECISION MAKING, PLANNING AND MANAGEMENT

2.1. ASSESSING AND MITIGATING AGEING AND OBSOLESCENCE

The life cycle planning process should include a plan to maintain and update I&C systems. There are many reasons why I&C systems cannot be expected to last for the whole life span of the plant. Both ageing and obsolescence processes need to be taken into consideration.

Ageing concerns refer to the fact that the reliability of I&C systems and equipment deteriorate with time, either due to physical wear or material degradation mechanisms of the individual component. These may be related to environmental stresses, usage, or simply the passage of time. Maintenance and equipment replacement strategies must, in some way, compensate for this effect. Implementing various provisions (or combination of provisions) such as ‘run to fail’, corrective maintenance and preventive maintenance, and replacement or upgrade are examples.

Obsolescence occurs for a number of reasons. These may include situations where equipment is no longer supported or available from suppliers, becomes difficult or expensive to maintain, or functionality and performance lags far behind current expected industry norms.

The strategic decision making for I&C maintenance and upgrade plans must ensure that the maintainability of systems is adequate to facilitate meeting the reliability and safety goals of the plant. This typically requires careful planning regarding assessment, replacement, monitoring and maintenance of I&C systems, to avoid problems relating to ageing and obsolescence. IAEA-TECDOC-1402 [2] provides more guidance on these issues.

The lead-time required to implement I&C modernization projects is often on the order of years. This is because resources, budget, and opportunity windows (i.e. outages) for installation are limited, Failure to adequately predict and plan I&C systems maintenance, replacement, or upgrade initiatives may have adverse consequences on overall plant performance, operability and economics.

2.2. FACTORS INFLUENCING DECISIONS ON I&C UPGRADES

2.2.1. Business drivers and constraints

The introduction of new I&C solutions may bring many benefits. However, NPPs tend to be conservative and slow to adopt new I&C technology and solutions due to the cost of equipment qualification, system development and installation, the impact of changes on an operating plant, and licensing cost and risk. As a result, most NPPs lag behind other industries in terms of I&C systems modernization. In many cases, this may have serious consequences in NPPs that impact production reliability and safety, and the problem may become especially acute for plants looking at life extension. Many factors must be considered and will influence MCR upgrade and/or equipment replacement decisions. These may include any of the following:

- The age and planned life of the plant, including life extension;
- The overall scope and cost of the project;
- The urgency and timing of MCR system or equipment replacement or upgrades. This may depend on the risk of I&C system safety function degradation and plant performance degradation;
- The ownership and management support;
- The ability of the project management to justify the cost of the project;
- Availability of key technical and human resources;
- Availability of appropriate technological solutions;
- Outage window (opportunities for installation);
- Licensing of replacements or upgrades.

2.2.2. Economic considerations and cost justification

Investment in nuclear power plant I&C and MCR upgrades to improve performance or to reduce costs often involves various technical options with different costs, benefits, and risks. These different options may result in different system and plant performance outcomes that in turn affect overall plant profitability. The option selected should reflect the optimum technical and financial decision consistent with the utility's overall business strategy.

When comparing alternatives, the scope of benefits and costs included in the analysis may include the following:

- Capital costs. These are one-time project expenditures made to obtain the desired financial benefits and normally occur over a fixed period of time (i.e. the project duration). These costs can include: design costs, manufacturing costs, training costs, installation and commissioning costs, documentation costs, licensing costs, validation and testing costs, unusual transition costs, etc;
- Life cycle costs and benefits. The decision to undertake nuclear plant upgrades usually involves not only capital costs but also costs and benefits incurred over much longer periods. Economic justification in this context must consider longer term issues, such as operations and maintenance (O&M) benefits or cost of the replacement system and possibly for the whole plant;
- Strategic costs. The effects of current decisions upon the cost of subsequent upgrades.

For each alternative, the specific benefits and costs associated with it have to be quantified. Capital costs are usually known or can be estimated. Strategic costs are often estimated based on reasonable assumptions, and these should be stated. Life cycle costs related to equipment are often more difficult to obtain and are sometimes overlooked or are inaccurately portrayed. Specific methods exist to help overcome the difficulties in the calculation of life cycle costs.

The decision as to whether to replace or upgrade a given I&C system must be evaluated in the larger business context of plant refurbishment. The objective of plant refurbishment is to ensure long term continued operation of the plant. It is also important to ensure that refurbishment investments are made at the most financially opportune time (e.g. in or out of the main outage). Some of the key factors in the replacement decision include:

- The risk of lost production due to the replacement system not being in an adequate state of readiness for installation during the refurbishment outage, or unexpected replacement system failures, both resulting in additional outage time;
- The risk of higher than expected project capital costs or overall life cycle costs;
- The risk that the chosen alternative will not meet the required extended plant life and could require further costs of additional system replacements;
- Risk of complex licensing issues and unexpected delays.

2.3. ASSESSMENT AND FEASIBILITY OF ALTERNATIVE MCR UPGRADES

Prior to establishing a strategic plan, an engineering technical feasibility assessment is necessary to properly identify and evaluate the viable approaches or solutions to the various I&C/MCR issues that need to be addressed. The feasibility studies should include the following:

- Identification and documentation of the technical and business requirements for each change, including a clear technical rationale or justification of the need for the changes;
- Identification and documentation of the feasible technical approaches to be considered and the development of clear evaluation criteria, including determination of the relative importance of each criterion. Criteria should include factors such as:
  - Impact of the change on operations, including indirect consequences such as the need for operator retraining, replicating the modifications in the full-scope training simulator, requirement to update engineering design drawings, effort required to update operating manuals and procedures, etc.

  - Risk associated with the change (safety, schedule, production outages, human factors, licensing etc.);
  - Performance and reliability considerations including failure-modes considerations, maintainability, etc;
  - Possibilities to introduce functional improvements during the change or in future and their strategic importance;
- Evaluation and assessment of the identified alternatives against the established requirements;
- Ease of maintenance and/or replacement of the new digital equipment (hardware, software, configuration data).

Clearly, to understand, document, and evaluate these issues will require consideration from the utility staff and suppliers on many aspects of the problem and expertise from design, operations, maintenance, safety and licensing, human factors, and training. It is important to ensure that adequate experience and expertise is available to address these issues. Any MCR changes will require the simultaneous consideration of many priorities and constraints across multiple disciplines. Most MCR modernization projects are complex and challenging and a proper technical assessment of alternative solutions will require a multi-disciplinary team approach. Systematic risk identification and mitigation are necessary to understand the relative risks and benefits of each alternative.

2.4. MCR POINT VISION

An important element of all strategic plans is a long term strategic vision. As an example, control room upgrade projects often refer to an end vision of the control room as the unifying idea that gives a direction to all incremental updates of the upgrade project, facilitating that individual upgrades take place in an organized manner. An end point vision for the control room defines the functionalities and 'look-and-feel' of the control room at the end of the modernization period.

While it is important that a long term strategy be developed with a specific end vision, technology is advancing rapidly, making it impossible to formulate a fixed end vision. Therefore, it is important to keep in mind that there are typically two sides to an end vision. One is primarily technology driven while the other is related to operational performance and plant safety. For example, the information technology side of I&C: such as software tools, operating systems and engineering tools. None of the recent developments could have been predicted just a few decades ago. The end vision should also be connected to the remaining operational life of an NPP. In some cases, significant modernization is not needed because of the short time remaining till decommissioning.

Thus, the end vision needs to be re-considered and updated on a regular basis. Keeping a watchful eye on developing technology and evaluating its relevance to the existing company strategy must be part of all strategic plans. Because the end vision is dynamic, specifications of the new I&C and HSI systems must be as formal as possible (technology independent).

An end point vision may consist of minor changes where only a few systems are modernized and done in a consistent manner, or may consist of a large, comprehensive modernization of all control rooms (main and secondary) and applicable I&C systems.

The end point vision of the control room includes the configuration, the functional capabilities, the display types, the level of automation, types of electronic procedures, color and symbols to be used, alarm schemes and presentation, etc. of the control room. The operational concepts include how the plant is operated under normal and abnormal conditions; including loss of equipment or displays and how the operators are expected to interface with each other, etc.

A multi-disciplinary team for developing an end point vision should include: operations, maintenance, training, human performance, I&C design engineering, human factors engineering, systems engineering, procurement and licensing.

Typical technologies available to consider for inclusion in the end point vision are:

- Workstations;
- Large display screens;
- Soft controls;
- Automation;
- Computerized procedures;

- Computerized operator support systems (including alarm management);
- Intelligent processing including advanced alarm systems;
- Failure management.

2.4.1. Operating philosophy

An important part of the end point vision is defining an operating philosophy for the updated control room. Namely, how the plant will be operated under normal and abnormal conditions, and how the operators' roles and responsibilities may change with the modernized control room and HSI equipment. This includes consideration of operation under conditions of failed or degraded I&C systems or HSI (e.g. failure of workstation displays).

The operating philosophy includes the makeup of the operating crew, roles and responsibilities, skills and capabilities of reactor operators and equipment or auxiliary operators. The operating philosophy also defines how the operating crew is expected to handle anticipated and unanticipated transients and how to operate during outages. It may also provide information from previous reviews of the human factors aspects of the control room. For example, overall control room arrangement, relationships and ordering of controls and displays, number of personnel normally in the control room and maximum numbers during situations of augmented manning, use of procedures, and communication among the crew members and with outside personnel.

When developing the operating philosophy, consider how the flexibility of new computer based HSIs can affect the assignment of tasks to individual crew members. For example, the current assignment of tasks may have been based in part on limitations related to the fixed locations of controls and displays in the existing control room. Computer based HSIs allow needed controls and displays to be brought to the operator at a workstation, enabling the design of information displays and control screens that are more compatible with operator functions, possibly allowing a more effective assignment of functions and tasks to individual operators.

2.4.2. A doctrine of use of digital systems

In relation to the licensing principles, it is important to provide the doctrine (main rules) of digital systems use (or non-use), during accidental, abnormal and normal operation.

We can distinguish two types of means: those for which a classification is required and unclassified means.

Some unclassified means can be used during abnormal or accidental operation. It can be the case for users not directly involved in accidental operation, in particular to apprehend the situation finely or to simulate different issues to manage the crisis. In this case, the operation doctrine must be particularly clear.

The rules must describe the context of use of each digital system, including the actors, the plant mode, and if there is a redundancy with conventional means, their priority of use.

2.4.3. Failure management (in plant/HSI)

Engineering must also take into account degraded operation; from the interface with the process to the interface with operators.

At the level of interface with the process, it is necessary to describe how a whole of information that are usually not available in conventional technologies can be or could be 'sent'.

For example:

- Discrepancy;
- Run time limit;
- Quit of position limit delay;
- Position default;
- Non equivalence monitoring (a changeover contact of a limit switch can not have double 0 or double 1);
- Voltage (125 or 48 V) loss;
- Local MMIHSI racked in;
- Test key in test position;
- Drawer unlocked;
- Electrical fault (thermal protection feature, short circuit);

- Blown power fuse;
- Re-opened mechanical switches;
- Drawer racked out;
- Insufficient arc blowing gas pressure;
- Operating cycles number exceeded;
- Operating time exceeded;
- On/off data flutter (shattering), etc.

On the one hand, work consists of describing information to present in the MCR. On the other hand, it is necessary to describe, for the one that will be retained, the principle of MMIHSI to apply — to visualize them — to operate the corrective treatments if necessary.

At the level of the treatments carried out in the automation system (loop controllers and group controllers), it is also necessary to describe their operation in degraded mode, even in case of total loss of their power supply. We have to define, for these degraded modes of automatic operation, how the process is managed (state of the valves and the pumps in the event of loss, restart, etc.), how the information of failure is sent to the control room and also actions that the operators must carry out when such failures appends.

Finally, it is necessary to study the consequences of partial loss or total loss of the MMIHSI level in order to define the rules of operation during the failure time, and when the computerized system starts up again.

2.5. MCR MODERNIZATION PLANNING

Main control room modernization activities are typically performed in an incremental manner rather than in a single step; thus, a migration path should be determined. The modernization plan should describe the migration path and include the following considerations:

- The interface boundaries between the MCR and I&C systems as well as the interfaces with other plant systems and equipment.
- Operating and maintenance staff training and plant simulator upgrades for the modernized systems;
- The size and duration of the incremental steps, depending on the utility's goals and regulatory constraints;
- The modernized HSI should be fully operational at the end of each step so that the plant can continue to operate effectively:
  - Any temporary HSI equipment or administrative controls that may be needed during the transitions also should be identified. Examples include temporary alarms needed during transitions that take the primary alarm system out of service, and temporary indications or augmented operator surveillances needed while monitoring systems are being replaced;
  - Temporary communications may also be required. It is important that any temporary HSIs are developed and evaluated using an appropriate human factors engineering process, verifying that the operators can perform the required tasks satisfactorily during the transitions. This is particularly important when changes are made at power, but also can be needed during an outage when some level of monitoring is still required (e.g. moving fuel, fuel storage pool, radiation monitoring);
  - It is also important to remember that changing conditions, such as reductions in funding, can mean that any intermediate step may be the last step for a long time. Therefore, the control room and HSI configurations at every step must be adequate to operate the plant under all possible conditions indefinitely.
- System validation and documentation (including operating procedures and qualification) at each step of the modernization;
  - Parallel operation of the old and new systems to verify the proper operation of the latter system before it is commissioned for operation in the plant.
- The need to periodically revise the plan to reflect the current configuration of the MCR as it changes with each incremental step.

2.5.1. MCR panel migration strategies

Careful consideration should be given to potential advantages of a phased approach to MCR panel modifications. Various implementation approaches are possible, and each station must consider a range of site specific issues and constraints. The EPRI document entitled Interim Human Factors Guidance for Hybrid Control Rooms and Digital I&C Systems [3] provides the following guidance on approaches to migration of the control panels, and in any given situation, a combination of these approaches may be appropriate:

- Migrate by I&C system. As the instrumentation and control systems are updated, also update the associated HSI (controls, displays, alarms, etc.) for that I&C system. Note that this does not necessarily correspond to plant systems or functions. The I&C system may be one or more cabinets full of analog circuit cards that serve various functions for a portion, but not all, of one or more plant systems. Updating the HSI driven by the analog controls in these cabinets would not modernize the other portions of the HSI for the affected plant system (e.g. component controls such as pump and valve controls, indicators or recorders driven by instrumentation that does not go through the analog cabinets).
- Migrate by plant system or function. For example, upgrade all of the HSI for the feedwater system, or for a function such as reactivity control or inventory control.
- Migrate by physical location in the control room or plant. Modernize the controls, displays, and alarms on a location by location, or panel section by panel section basis.
- Migrate by HSI element. Modernize the displays in one or more steps, the alarms, the controls, and so forth, across systems and across the control boards or panels. Although this is not practical on a large scale, it can be followed for some portions of the control room changes.

The same EPRI document points out that any temporary HSI equipment or administrative controls that may be needed during the transition should be identified and factored into an overall implementation plan. For example, the need for temporary alarms during transitions that take the primary alarm system out of service, and temporary indications or supplemental operator monitoring systems needed while existing monitoring systems may be out of service. Temporary HSIs will need to be developed and evaluated using an appropriate HFE process such that the operators can safely perform required tasks during each of the change out phases.

2.5.2. Involvement of the affected parties

For any plant upgrade project to be successful, it needs to be accepted by all parties that are affected by the change. Acceptance presupposes involvement in the processes that leads up to the change, e.g. a new I&C solution. In most cases the affected parties will include:

- Plant management (including senior management);
- Project group (project management and engineering);
- Drawings production group;
- Design organization or project engineering firm;
- Key suppliers (critical equipment or systems);
- Operators, field workers (e.g. electricians), maintenance staff etc.;
- Work management and outage planning group;
- Training and training simulator support group;
- Safety authorities.

Involvement of all affected parties is important during project development as well as implementation. This will ensure that the suppliers meet the expectations of the project and the end users are comfortable with the solution, and reduce risk in the licensing process.

2.6. KNOWLEDGE MANAGEMENT AND PRESERVATION

A strategy for the development of I&C solutions of any given plant must be intimately connected to the knowledge preservation and in-house re-training strategy of that plant. IAEA-TECDOC-1510 [4] addresses the factors that are important for knowledge management in nuclear industry operating organizations.

IAEA-TECDOC-1399 [5] states that staffing and workforce plans must be compiled that "provide a standardized and consistent methodology for overall human resources planning driven by strategic and business goals." While some of the knowledge preservation can be done using formal means such as documents and databases, hands on training and mentoring is essential to accomplish knowledge preservation. Knowledge transfer and preservation requires long term planning, typically taking several years. Competence relating to existing elements of I&C solutions that will be retained must be preserved, while competence relating to new solutions must be worked up.

Knowledge preservation is often an uncertain undertaking since it relies to a certain degree on tacit knowledge. Tacit knowledge cannot easily be documented or described. Sometimes the staff uses tacit knowledge without realizing that they depend on it. Therefore, there is a risk that the organization might lose competence without realizing it before it's too late.

Other important considerations are related to maintaining an adequate skill, experience, and expert knowledge base or capability in the organization (or perhaps in conjunction with external consultants and suppliers) that ensures I&C systems important to production or safety can be reliably maintained. Ageing I&C equipment and systems, particularly computer based systems present technology specific and system specific challenges to operating facilities.

2.7. CONFIGURATION MANAGEMENT

Configuration management and change control systems are important parts of any modernization project, especially in safety related applications. Changes in the control room will typically be implemented in stages; therefore a high quality configuration management system should be in place during the whole project. Proper configuration management processes should be set up at the design stage of the modernization project and they should be carried out in sufficient detail during and after each major step of design and implementation.

Configuration management programmes ensure that the design, construction, testing, and operation, of the physical facility are in accordance with the design requirements as expressed in the design documentation, and to maintain this consistency throughout the operational life cycle phase, particularly as changes are being made. An important objective of the configuration management programme is to ensure that accurate information, consistent with the control room physical and operational characteristics, is available, in a timely manner, for making safe, knowledgeable, and cost effective decisions. Management ownership and management support of the configuration management programme are essential to assure that changes and processes are implemented correctly. Specific training on configuration management objectives and processes should be provided to all personnel to assure that they can effectively carry out their work.

IAEA-TECDOC-1335 [6] presents a comprehensive review of configuration management requirements and applications in nuclear power plants.

2.8. COORDINATION OF I&C AND HSI MODERNIZATION ACTIVITIES

The control room modernization plan should be done in conjunction with the development of an I&C system modernization plan. Although there is some flexibility in choosing the level of modernization for the HSI, the degree to which it can be modernized clearly depends on the level of I&C modernization. For example, upgrading to compact workstations providing plant-wide access to controls and information requires an I&C communications and control architecture that allows access to multiple systems and functions across the plant.

The I&C modernization plan will be a major driver of the HSI changes. However, the interaction goes both ways. Human factors and operations considerations, and the plant's choice of a control room end point vision and method for migrating toward the end point vision can have a significant impact on the I&C modernization plans. It is important that an overall operating philosophy be defined for the modernized control room and the plans for individual I&C modernizations and HSI changes consider how this operating philosophy will evolve over time until the end point is reached.

3. MCR MODERNIZATION OPTIONS FOR COMPONENTS AND SYSTEMS

There are many options afforded by digital technologies leading to a multitude of possible systems and components which may be replaced or upgraded during a modernization project. The specific items to be included in a modernization project depend on the specific goals and life cycle plans of the NPP. This section briefly describes the most common systems, components and functional elements which may be upgraded or included during an MCR modernization.

3.1. ANALOG INSTRUMENT REPLACEMENTS (FORM-FIT-FUNCTION REPLACEMENT)

This is the simplest approach to replace the old instruments and controllers on MCR panels with digital instruments, on a one to one basis. The existing ageing analog components are replaced with digital counterparts that have the same functions as the existing analog components. The new digital components may have additional, auxiliary functionality; however, their basic functions are similar to the old ones.

The problem of common mode software failure is important in retrofits of digital components into existing plants. Where programmable, digital components are substituted for analog components, independence of components may be compromised due to the use of the same software for each of the independent components. The safety evaluation may need to be revised to account for common cause software failure. Extensive discussions of these issues are presented in IAEA Nuclear Energy Series, Protecting Against Common Cause Failures in Digital I&C Systems [7].

3.2. SOFT CONTROLS

Controls are the devices through which personnel interact with plant functions, processes, systems, components, and variables. From an HSI standpoint, controls are classified as hard or soft. Hard controls are physical hardware devices, such as j-handles, position switches, and pushbuttons, which are typically mounted on control panels. Soft controls are user input devices presented as displays on a computer screen. From an I&C standpoint, hard controls may be either hardwired directly to the equipment being operated or they may provide input through software. Soft controls only provide input through software and cannot be hardwired to equipment. In the strict sense, when a hard control is linked to software, it is a soft control in that it can be flexibly used to provide different types of control modes and options that are defined based on the current software configuration. Thus it is important to recognize that software control of plant equipment can be implemented using hard or soft interfaces.

The main elements of a soft control are:

- Selection display. The display from which a soft control is selected;
- Control display. The display with which the control action is taken. In addition to providing for control input, this display may provide information about relevant parameter values, the control logic, constraints, and feedback related to the control actions;
- Display devices. The devices on which the soft control display are presented. It may be a video display unit or other display device;

— Input devices. The devices used to interact with the soft control. Typically these are computer-input devices, such as a keyboard, mouse, and touch screen.

Soft controls offer a great deal of flexibility and when properly implemented can greatly enhance the users understanding, execution, and monitoring of the control action. Soft controls are especially attractive when the end point vision for the control room modernization programme involves the following types of modifications:

— Transition to computer based workstations with seated operators;
— The consolidation of controls;
— The integration of controls with relevant displays and other information;
— An increased level of automation;
— Computerized procedures implemented;
— Increased flexibility in the presentation of controls and displays.

Perhaps the greatest benefit of soft controls is the ability to significantly enhance the information needed to fully understand a control action. A display of the control logic can be made available at the interface. The control display can be designed to indicate any prerequisite conditions for the control action (e.g. the presence of any interlocks or alarm conditions associated with the actions). The soft control display can precisely provide feedback about the effects of the control action so that the user can monitor its progress. Soft controls can be designed to perform different functions, depending on the current control mode, thus providing greater flexibility. They can also provide checks on user inputs and provide more informative feedback to users about the acceptability of their inputs to protect the system against incorrect user control inputs.

Soft control can be integrated into other displays, such as task displays and computerized procedures so that the control is available to the user precisely where it is needed. Soft controls can also be grouped into sets of controls that are needed together for user actions.

Soft controls can be used to consolidate a large amount of panel space into a single VDU. Further, new controls can be added to the control room without the need to add additional panel space or to rearrange already existing controls. This feature makes operations from a seated workstation possible. This also enables control to be easily modified.

A special case of soft controls is spatially dedicated and continuously available (SDCA) soft controls. These soft controls are spatiallydedicated on VDUs so that they are continuously available to users. These are especially important for controls that need to be accessed immediately. These SDCA controls are always in the same position so that there is no need to navigate the screens to find them, which would add to the time required to take the necessary action.

While the benefits of soft controls are many, their main drawback is that under some circumstances they require additional time and workload to operate. This mainly happens when they have to be retrieved by navigating through multiple screens on a VDU; thus, a great deal of consideration should be made in designing control screens for operating soft controls, especially if multiple controls are being consolidated into a single VDU terminal.

One of the first considerations in choosing an approach to the design of controls is whether the controls should be soft controls or hard controls. This decision is not one that can be based on human factors alone. I&C criteria for reliability, diversity, isolation, separation, transient response performance requirements, and defense-in-depth must also be considered [8].

3.3. OVERVIEW DISPLAY PANELS

Conventional control rooms have specific characteristics that have evolved over many years of design that contribute to crew performance. They typically feature hardwired controls and displays (and perhaps a lesser number of computer based controls and displays) that are installed on large control panels shared by crew members. Because they have fixed locations on the control panels, access typically does not require unusual display space navigation skills. Control room with computer based workstations may result in the following types of new concerns:

- Difficulty maintaining awareness of overall plant status. This concern may be aggravated in a computerized control room due to the fact that only a portion of the total plant information is visible at one time through the limited viewing area of an information display screen;
- Difficulty and time delay associated with accessing computer based controls and displays. Concerns may result because controls and displays must be retrieved through navigation of the computer display space;
- Difficulty maintaining awareness of crew member actions. Operator actions performed at a computer based workstation may be less identifiable when compared with actions performed at a conventional control panel. In addition, because a single control could have multiple locations in the computer display space, it may be possible for multiple operators to perform tasks involving the same control without being fully aware of each other's specific control actions and intentions;
- Difficulty communicating. Expressing ideas face to face is important to crew performance. This may be difficult in a computerized control room because of physical separation/isolation. This concern may be further aggravated by the fact that operators have individual views of the display system and may not be viewing the same portion (e.g. page) of the system when they attempt to collaborate.

To minimize these concerns and enhance the crew interaction, an overview display panel (ODP) should be designed. The ODP is important to facilitate communication, coordination, and cooperative problem solving and allow multiple personnel to simultaneously view the same information when they are in the control room or throughout the plant. Generally, ODP provides a plant level overview and safety information to the operating staff via an SDCA display. In all plant modes, the ODP should perform the following functions:

- Support the operator’s plant level situation awareness. Operator tasks often require detailed diagnostics in very limited process areas. However, maintaining continuous awareness of plant-wide performance is necessary. The dedicated ODP can be viewed from anywhere in the control room and its simplicity and fixed format makes it easily understood at a glance. Therefore, it provides an operator a continuous indication of plant performance regardless of the detailed nature of the task that is undertaken;
- Support the operator’s crew coordination. The proper coordination and direction of the control room operating staff is important during all modes of plant operation. The ODP provides a common mental model of the plant to facilitate common plant visualization among all plant operational groups. This promotes a more effective communication process among plant personnel. This display function assists the operator in maintaining awareness of the intentions and actions of the other operators so that separate activities can be coordinated and operators can monitor each other's activities to correct errors or promptly lend support when needed;
- Support personnel communication and collaboration. This group view display function assists the operators in actively participating in the same task through the sharing of information, ideas, and actions. This is achieved by providing the operators with a common frame of reference and tools for communication;
- Support the operator’s shift turnover. Proper transfer of information from one shift to another is essential to plant operation. Special provisions to make the turn-over convenient can reduce the potential for operator errors;
- Critical functions are maintained by success paths, which are key portion of plant systems that are used to maintain or restore the critical function parameters within specified limits;
- Support the operator’s maintenance of critical safety functions and associated success paths. Critical functions and success path alarms are used to aid the operator in quickly identifying the location of important alarm information;
- Support the operator’s safe shutdown operation;
- Support the presentation of any computerized display (control displays, informational displays, etc.) at the operator’s request;
- Provide detailed plant information to the operator in a direct manner. The ODP should provide for the display of the operational status, e.g. flow or no-flow, energized or de-energized, on or off, open or close, etc. of a limited number of essential components controlled or monitored by the MCR.

It should be noted that the ODP contributes to improved team performance in advanced plant designs. In addition, prior research has shown that digital systems have a significant impact on crew teamwork and coordination. For example, the availability of improved monitoring, decision support, controls and automation, frequently alters the crew's role more toward system supervisors. This is because the digital systems perform many of the lower level activities associated with data gathering and processing. Thus, the crews are freed from these lower level activities. This has often resulted in a shift to less teamwork, less communication, and more difficultly for crew members to monitor each other's activities. When the digital systems are lost, the crew must shift its activities to accomplish the lower level responsibilities that the digital system performed. In this case, the type of teamwork needed is more similar to conventional control rooms. More detailed discussions on the human performance issues related to digital control systems are presented in the EPRI report on Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance [8] and NUREG-0700 Human-System Interface Design Review Guidelines [9].

3.4. ALARM SYSTEM

The operators' task of monitoring the plant operating condition and detecting problems is demanding due to the large number of individual parameters and conditions involved. Therefore, operators are supported in the task by alarms. MCR modernization offers the opportunity to make major improvements in a plant's alarm system. Computer based alarms provide increased capabilities that can make them more effective and provide added features not practical with conventional, hardwired alarm technology. Because the alarms are one of the primary means by which abnormalities and failures come to the attention of plant personnel, there is a major operational incentive to make them as effective as practical.

Alarms provide automated monitoring capability that alert operators via visual and auditory displays when parameters deviate from specified limits. The general functions of alarms are to:

- Alert the operator to a system or process deviation;
- Inform the operator of the nature and priority of the deviation;
- Guide the operator's initial response to the deviation;
- Confirm whether the operator response corrected the deviation.

While monitoring and detection is the primary purpose of alarms, in most plants they are used for other purposes as well, such as:

- Providing an overall assessment of plant status, mostly by the presence or absence of alarms in key systems;
- Determining the availability of systems and components, mostly by the absence of alarms;
- Diagnosing transients and events;
- Supporting testing and maintenance (e.g. surveillance tests).

Alarms generally display information by means of arrays of alarm tiles. These panels are often supplemented by dedicated video displays of parameters related to specific systems or functions. In addition, many plants have alarms for other systems in the control room. For example, separate alarms are often provided on auxiliary panels such as radwaste processing; heating, ventilation and air-conditioning (HVAC), switchyard equipment, or a fire alarm panel. Detailed information about alarms is often provided in alarm messages provided via a printer or other logging device. The existence of an incoming (i.e. new, not acknowledged) alarm is typically associated with an audio signal as well as flashing of the visual indication (e.g. alarm tile). The audio and visual indications may persist until the alarm is acknowledged by the operator. Clearing conditions (i.e. parameters re-entering the normal range) are typically indicated by a different audio signal and different flash rate.

While alarms play an important role in plant operation, they have also posed challenges to the operators. Common problems include:

- Too many alarms which creates alarm overload such that operators cannot process all of the alarm information;
- Too many spurious or nuisance alarms, which contributes to alarm overload and may cause operators to discount alarm information;
- Poor distinction between alarms and normal status indications, which can make it difficult to distinguish normal from abnormal conditions.

MCR modernizations offer the opportunity to improve alarms. Computer based alarms can provide increased capabilities designed to improve alarm effectiveness. They can handle more complex logic than can be implemented in hardwired alarms, and provide more flexibility in the display of alarm information. Some examples of how the added capabilities can be exploited are as follows:

- Processing logic can be used to eliminate nuisance or irrelevant alarms and reduce the number of alarms that occur in a transient;
- Separate alarms can be integrated into process displays to improve their association with related components, systems and functions;
- Alarms can be integrated into other displays, such as electronic procedures and soft control displays, or presented on common or group view displays to help focus and coordinate the control room staff;
- Alarms can not only be integrated into the displays, but once this is accomplished, alarms can be used as part of these other HSI resources to provide, for example, alarms for entry conditions in emergency operating procedures (EOPs);
- Computer based alarms can also allow operators to add features, e.g. operator-defined set points to help in monitoring;
- Alarm response procedures can be provided electronically, thereby providing rapid access to detailed information about the alarm without the need to consult books of procedures;
- Alarms can be designed with management facilities allowing personnel to sort alarms by time and by system, and to interrogate the alarms to obtain detailed information about those that are of specific interest.

At the same time, existing alarms have some advantages that should be retained as systems are upgraded to modern digital technology, including the following:

- The fixed positions and patterns of existing alarm tiles provide an advantage in quickly assessing the state of the plant and in recognizing particular transients.
- Hard copy alarm message lists have an advantage over lists produced on a computer-driven display in that messages do not scroll quickly off the screen.

It is important that new alarms be designed and implemented to take advantage of each technology and provide the needed improvement in effectiveness for operators.

It is also important to recognize that introduction of new, digital control and monitoring systems often results in a tendency to create many more alarms, because of the ease with which alarms can be generated from process information in a digital system. Further, self-diagnostic features in a digital alarm system can add many detailed alarms on problems or failures within the alarm system itself. Proliferation of alarms can make the alarm overload problem worse and add to the administrative burden of managing the alarms and alarm response procedures. Care should be taken to ensure that new alarms serve a documented need as new alarms result in the need to create, learn and follow associated alarm procedures.

General considerations for alarm modifications should be considered within the context of the overall I&C modernization programme. These considerations include identifying what additional alarms will be needed and which of the current alarms may need to be modified. They also address the extent to which modifications will be made to the alarms. For significant modifications, the designer will need to consider such fundamental questions as:

- How alarms will be defined;
- How alarms will be prioritized;
- How the numbers of alarms can be reduced;

- How alarms will be displayed to operators and how they will be integrated into other displays;
- How alarms will be coded for priority, status, and other relevant information;
- Where the alarms will be located (e.g. overview panel, control panels, workstations);
- What control and alarm management features will be made available;
- How alarm response procedures will be designed, modified, and implemented;
- What are the HFE principles to be applied;
- Not all modernization projects will require an extensive upgrading of the alarms or provide a practical opportunity for such major changes.

As the expanded functionality of alarms is considered, it is important to distinguish between them and other operator aids. The concept of an alarm can be expanded in time to provide alerts and early warning of equipment failure based on more intelligent condition monitoring for predictive maintenance purposes. Similarly, as plant data analysis becomes more intelligent, it can be applied to fault data in order to analyze the pattern of failures to diagnosis the event.

3.5. COMPUTER BASEDBASED PROCEDURES

Procedures in nuclear power plants are typically paper based procedures (PBPs), including both text and graphic formats, that present a series of decisions and action steps to be performed by plant personnel (e.g. operators and technicians) in order to accomplish a wide variety of tasks from administration to testing to plant normal and abnormal operation. Computer based procedure (CBP) systems, also known as computerized procedure systems (CPS), were developed to assist personnel by computerizing paper based procedures with the objective of increasing the likelihood that the goals of the procedures would be achieved more efficiently and with less likelihood of human error.

Computerization can be applied to any procedures, for example:

- Emergency operating procedures (EOPS);
- Abnormal operating procedures;
- Normal operating procedures;
- Test and surveillance procedures;
- Maintenance procedures;
- Administrative procedures.

CPS may provide different levels of functionality, ranging from the simple translation of traditional procedures into software representations for viewing on a VDU, to systems that integrate process and equipment information and alarms with procedure steps, and then provide control and automation features to aid the execution of tasks.

Computer based procedures have the potential to greatly support crew performance. Computerizing tasks such as data gathering, monitoring of steps of continuous applicability, and keeping track of procedure navigation paths allows the crew to devote more attention to achieving the goals of the procedure. Since these tasks also demand considerable communication and are a potential source of human error, CPS have potential to improve performance. Computerization can also allow users to access varying levels of detail, tailor information displays based on context, support simultaneous use of multiple procedures, and facilitate the administrative aspects of maintaining the technical accuracy of procedures [8].

The following are among the general challenges for introducing computerization of procedures:

- Level of authority and supervisory control. CPS usability is enhanced if the system provides automated features to secure necessary authorizations and places operators in control of the pace and path of the procedure;
- Level of automation of individual procedure functions. When procedure functions are automated, the CBP system needs to provide the user with the basis for CPS actions and the path of the procedure;

- Cognitive workload. While a CBP system is supposed to reduce cognitive demands on the operator, cognitive overload may be the effect if the system is poorly designed. Computerized procedures should be designed consistent with the view that the user of the procedure supervises both the plant and the procedure;
- Keyhole effects and navigation. All screen based systems may induce keyhole effects and navigation problems unless this is considered in the design.

For further information on usability issues with CBP systems, the reader is referred to EPRI 1010042 [8], NUREG-0899 [10] and NUREG-0711 [11]).

Concerns that can be attributed to effects of a hybrid MCR and possible mitigating measures include the following:

- A hybrid set of procedures. Since procedures or procedure related material is so comprehensive it is usually not feasible to computerize the whole set of procedures. Usually, the most important procedures are computerized first. This creates a situation where the operator must use different kinds of procedure interaction schemes, some which are used with PBPs, and some which are used with CBPs. Even though the whole set of procedures could be computerized, the operator would probably need some kind of fallback on PBPs in case the computerized system should go down. To this end, computerized and paper based procedures should apply a common operational strategy;
- Hybrid crew member communication schemes and responsibilities. Computerized procedure systems may perform activities previously performed by crew members. This may change the way crew members handle plant situations and the frequency and types of communication they engage in. This may easily result in two different ways to manage the work in the MCR, one that is used when a CBP is being used, and another one that is used when a PBP is being used. In order to design usable CBPs, one will need to analyze these effects to ensure the CBPs are appropriately integrated into plant operations and that any changes to individual crew member responsibilities are addressed.

3.6. COMPUTERIZED OPERATOR SUPPORT SYSTEMS (COSS)

Computerized operator support systems (COSS) provide early warning of failure to increase asset availability, which provides benefits such as increased revenue, reduced maintenance expenses and improved operational efficiency. The methodology provides an approach to focus on equipment and failure modes that deliver the maximum benefits. COSS assists operators and maintenance personnel in supporting their monitoring, situation analysis, and decision making activities and may provide the following capabilities:

- Provide access to data historians and electronic technical data sheets;
- Monitor plant processes and other equipment, variables, and predict future plant data and information. Future process data may be computed based on process models. The data and information may be presented in forms that enhance user’s situation awareness and understanding;
- Calculate signals and values that cannot be measured. Calculations may be based on existing measurements and a model of the process. Results may be presented independently or integrated with measured data. This can be very useful, for example in case of loss of electric power supply, to automatically calculate which equipment is still available;
- Perform logic based diagnostics based on measurements, stored data and information, and a process model;
- Evaluate the effects of different actions on future plant states to support decision making using an appropriate plant model with user input of control actions, or without user input to recommend control actions (this feature is not typically available within current systems but may be in the future as advanced COSS are developed);
- Dynamic function diagrams which display current or historical data within the configured function diagrams (this feature is not typically available within current systems but may be in the future as advanced COSS are developed).

While additional more complex functions can be implemented within the COSS, one must also consider the maintenance and life cycle costs of the system. Certain key technical and cost issues should be considered when designing a COSS:

- What are the technical requirements for design, development, implementation, and maintenance? A COSS may have different requirements than the traditional HSI reflecting the fact that it may be dependent on and require interfacing to I&C systems, plant data, and plant databases;
- What are the technical issues to be solved in installing and integrating a COSS into the control room? COSS may require access to sensor data, and calculated data from several sources;
- Will the expected benefits justify the cost of design, development, installation, and maintenance, or acquisition of an off-the-shelf system? If the COSS is not safety related, does the expected increase in plant availability and/or the prevention of equipment damage justify the cost?

Where practical, the COSS should be fully integrated and consistent with the HSIs. The appearance and functionality of the COSS should follow the same design conventions as other HSI resources (e.g. use the same nomenclature, abbreviations, etc. as the general information display system).

3.6.1. Outage support systems

Separate displays.
Verifying compliance with plant mode specifications.

3.6.2. Communication between outage support systems and MCR

Outage support systems are central to managing and coordinating all outage activities on a strict schedule, including interactions between all relevant personnel, supplier representatives, and safety personnel. In the USA, some utilities have established a separate outage control room. The main purpose of outage support is to separate the outage tasks from the current plant operations in the MCR so that the operations crew can focus on process control. It is also important to ensure that the new digital systems have the ability to interact with the outage support systems.

There are also potential important gains, in a good coordination between re-qualification of the circuits after maintenance and the lining up operation activities.

3.6.3. Safety monitoring displays

During outage it is especially necessary to ensure that the plant state is compliance with the operation technical specifications. For each system of the plant, it is necessary to know if it is available or not, in a safety point of view. Such a monitoring can be done through computerized aids.

As a first step, for each system of the plant, it is necessary to translate its operation specifications constraints into logical equations. This must be done for each standard operation state of the plant. Then, a computerized aid can evaluate the equations in real time, in order to monitor the respect of the technical specifications. In case of non respect of the specifications, the computerized aid warns crews of the new operation situation. Specific overview displays can be designed, representing the standard plant states, the systems, the available systems requested and the real state of the systems.

Such a computerized aid normally has two levels of interface: an overview of the status of the systems in relation to the operation specifications, and a level of detail that allows operators to access details of the equations underlying synthesis information. Viewing the importance of such aids concerning safety monitoring, a specific quality process must be put in place both to validate process inputs and the equations monitoring the systems availability.

3.6.4. System performance evaluation systems

During normal plant operation conditions, operators of most plants around the world rely on various tools to monitor and assess actual plant performance, based on specific performance indicators. The need is to have accurate and reliable performance indicators on the basis of which relevant maintenance actions and corrections of operation settings can be decided: the end goal is to have the plant running at the maximal allowed power output, and at the optimal thermal efficiency. Various systems have been built worldwide for such a purpose: usually they were not built from plant commissioning, but rather designed later after a few cycles of experience feedback and gradually installed.

The relevance of a planning and performance management system(PPMS) lies in its ability to detect and localize the smallest possible losses of performance, as soon as possible. This will allow the plant operators to adjust settings or make early corrections, thus minimizing losses. The features of these systems vary greatly, mainly on the following features:

- The process data from the sensors: the sensors are either the process control sensors, or some additional test sensors (which are of higher accuracy than the process control sensors);
- The data acquisition system: it may be continuous (e.g. as a data historian allows), or periodic (daily, weekly, monthly), or on demand;
- The process modeling tool: the data provided by the sensors and data acquisition system has to be processed on a plant thermodynamic model that will diagnose the differences between expected parameters and actual parameters. The results can be given in MW, electrical or thermal;
- The operator–PPMS interface: the results may be given as lists of basic data, or may be more sophisticated (such as providing trending figures on main components, recommending prioritization of actions, access to data archives...). The PPMS may or may not be located in the control room.

The evolution of the PPMS may be impacted by I&C renovations: e.g. when a digital I&C system is installed it may include digital instrumentation/sensors and digital communication, thus generating higher accuracy of process data and ultimately a more accurate and a faster diagnosis from the PPMS.

Another field of ‘performance monitoring systems’ is emerging from the collaborative work managed by the Nuclear Energy Institute (NEI) in the USA, with the Electric Utility Cost Group (EUCG) and the Institute of Nuclear Power Operations (INPO). The work aims at defining a standard nuclear performance model (SNPM) to improve benchmarking effectiveness between nuclear plants: this work has been in progress since 2002 and describes plant processes, cost definitions and key business performance indicators (KPIs). SNPM’s main processes are: plant operation, work management, configuration management, equipment reliability, materials and services, and various enabling processes.

3.7. OTHER POSSIBILITIES

3.7.1. Remote plant data display

The information available in MCR can be also accessible in other places in the plant for field operation, maintenance, management and outage monitoring. The benefits of remote displays are:

- Limitation of disturbing activities in MCR;
- Facilitation of communication between MCR and field operation;
- Facilitation of maintenance;
- In case of accident, regulatory and/or other authorities can proceed in parallel to recover the accident with MCR operators;
- Availability of plant data for experts.

3.7.2. Integration of communication with field operation

The modern I&C systems and HSI have an opportunity to share information outside the MCR, especially for field operation.

Personal digital assistant (PDA) technology, wireless networks, wireless sensors and codings systems are available on the market. These technologies can be applied to upgrading I&C systems for field operation. The nuclear context should also be taken into account when these technologies are used for nuclear plant, especially to guarantee a certain level of quality of systems and data manipulated.

PDAs can take pictures, view videos and record messages.

These devices can recognize equipment near where they are. For example placing radio frequency identification tags on equipment so that the PDA can recognize it. With this recognition, many applications are possible. For example, the visualizing of technical documents on the equipment, downloading field procedures into the PDA, following the realization of the field procedure with the PDA, and verification of the field activities done.

Wireless sensors can be used for the measurements difficult to access or temporarily placed. The PDA could then collect this measurement data, and distribute them as well in the MCR or retransmit it to maintenance teams. PDA can send directly field information to the MCR, permit communication with operators, track field activities from the MCR.

3.7.3. Live documentation

The plant operating parameters of the systems can be monitored online, directly into document forms.

This technology allows plant personnel to have user configurable on-line plant documentation. The fields in the documents can be referred to as either process data or synthesis data calculated by the I&C system. An application might be the monitoring of the technical specifications for each system of the plant, such as 2-D or 3-D computer aided design (CAD) drawings, schemas representing isometrics.

3.7.4. Link with computerized maintenance systems

One of the benefits of digitalization is to be able to merge process and maintenance and information.

For maintenance activities, an important coordination has to be managed between the operation team and the maintenance operators. This coordination consists especially in managing clearances. It is performed by a dedicated member of the operation team.

Today, with conventional technology, clearances management involve a specific database, printing sheets that have to be hanged on the equipments that have to be set in safe position and macaroons that have to be placed around the switches buttons, indicating to the operators that it is forbidden or impossible to operate an equipment.

With digital technologies, it is now feasible to establish a link between the clearances management system and the I&C system, in order to digitally inform the operator that an equipment is not available du to a clearance.

4. PROJECT EXECUTION

4.1. DETAILED ENGINEERING PLAN

4.1.1. Project life cycle

MCR modernization projects should use a documented design process to govern changes and modifications. A structured design process provides a means to trace requirements from the early stage of design through to the final detailed design and to verify and validate the end product. The design process for a modernization project generally includes requirements specification, overall architecture design, detailed design and analysis, installation, acceptance testing and operation. MCR modernization may involve a single system or multiple plant I&C systems. Thus, in general, the life cycle for a modernization project comprises a sequence of activities that are necessary to develop multiple I&C systems involving programmable digital devices in an integrated environment. The project life cycle is illustrated at the overall plant or project level in FIG. 1 and at the level of an individual I&C system in FIG. 2. The system life cycle depicted in FIG. 2 provides additional detail on the activities necessary to realize individual systems; these activities are shown grayed out in FIG. 1. In addition to the eight main system life cycle activities, FIG. 2 shows 11 support activities.

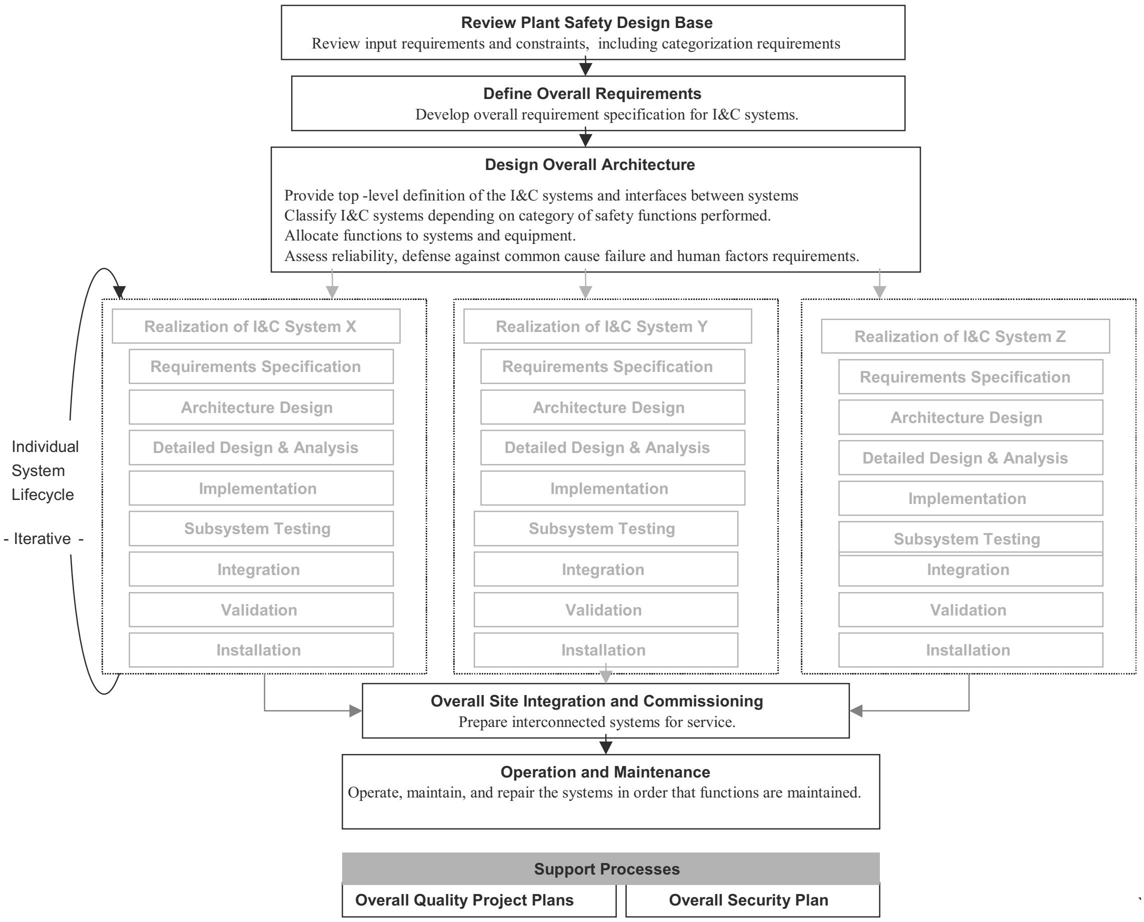

Review Plant Safety Design Base
Review input requirements and constraints, including categorization requirements
Define Overall Requirements
Develop overall requirement specification for I&C systems.
Design Overall Architecture
Provide top -level definition of the I&C systems and interfaces between systems
Classify I&C systems depending on category of safety functions performed.
Allocate functions to systems and equipment.
Assess reliability, defense against common cause failure and human factors requirements.
Individual System Lifecycle
- Iterative -
Realization of I&C System X
Realization of I&C System Y
Realization of I&C System Z
Requirements Specification
Architecture Design
Detailed Design & Analysis
Implementation
Subsystem Testing
Integration
Validation
Installation
Overall Site Integration and Commissioning
Prepare interconnected systems for service.
Operation and Maintenance
Operate, maintain, and repair the systems in order that functions are maintained.
Support Processes
Overall Quality Project Plans
Overall Security Plan

FIG. 1. Life cycle for overall I&C development.

One or more governing procedures should be provided for each life cycle activity to identify the necessary outputs and describe in detail the engineering process requirements for completing the activity.

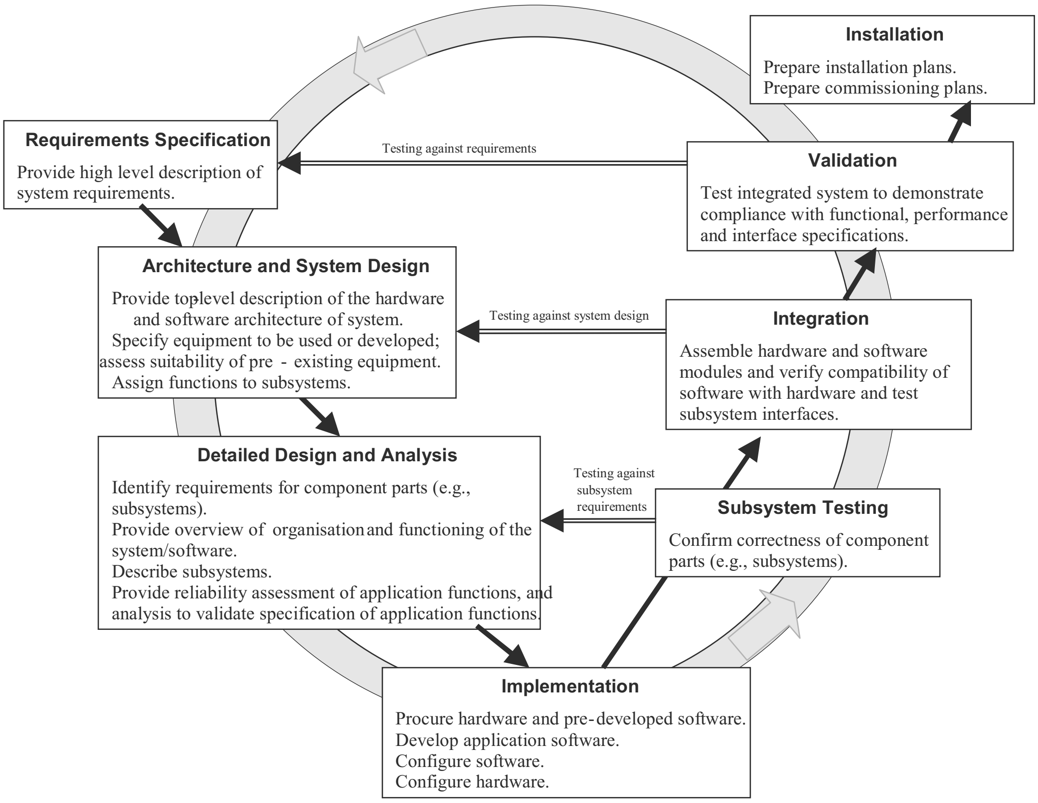
The overall life cycle addresses the life cycle requirements of I&C systems important to safety for the NPP as a whole. It includes the activities that are necessary to derive, from a plant wide perspective, the functions important to safety and to determine the architecture to meet these requirements. These are the first three activities shown in the strategic and conceptual studies discussed in Section 2.3 may be considered part of these activities as they set the context for their completion.

The overall life cycle also includes testing and commissioning the interconnected systems, as well as operation and maintenance of these systems in the context of maintaining plant safety, quality of control and ease of operation. The procedures governing overall design and development should address the process requirements necessary to support operation and maintenance.

At the system level, life cycle activities include requirements specification, architecture and system design, detailed design and analysis, implementation, sub-system testing, integration, validation and installation. Additional details of each activity are provided in FIG. 2.

4.1.2. Specific concerns of project implementation

(a) Project team. Based on the modernization size, the plant management should set up a specific organization including HFE specialist and operating personnel having operations experience to successfully perform the modernization project. The project team may be divided into three groups, as follows:


Installation
Prepare installation plans.
Prepare commissioning plans.
Requirements Specification
Provide high level description of system requirements.
Testing against requirements
Validation
Test integrated system to demonstrate compliance with functional, performance and interface specifications.
Architecture and System Design
Provide toplevel description of the hardware and software architecture of system.
Specify equipment to be used or developed; assess suitability of pre - existing equipment.
Assign functions to subsystems.
Testing against system design
Integration
Assemble hardware and software modules and verify compatibility of software with hardware and test subsystem interfaces.
Detailed Design and Analysis
Identify requirements for component parts (e.g., subsystems).
Provide overview of organisation and functioning of the system/software.
Describe subsystems.
Provide reliability assessment of application functions, and analysis to validate specification of application functions.
Testing against subsystem requirements
Subsystem Testing
Confirm correctness of component parts (e.g., subsystems).
Implementation
Procure hardware and pre-developed software.
Develop application software.
Configure software.
Configure hardware.

Support Processes

System QPP	System Maintenance	Change Management	System Operation	System Security	
System Verification	Qualification	Configuration Management	Safety Manual	Non-conformance	Procurement

FIG. 2. Life cycle diagram for a system development.

— A group to coordinate the project and interact with the supplier;
— A second group concerned with design and V&V;
— The third group would adjust the configuration of existing equipments as a consequence of the new HSIs.

The project team should include operations and maintenance personnel. This team should have sufficient knowledge and skill to develop a thorough understanding of the new design and provide clear solutions for problems identified in its implementation. For a large modernization project, the project manager could set up the project team as integrated, working together, with shared responsibilities between utility and supplier clearly identified in an organization chart.

(b) Schedule and work plan. In case of incremental modernization, it is necessary to have a clear understanding of the end point vision of the MCR at each step in the modernization. The plant management should ensure that the project team keeps this vision in mind, particularly in case of the introduction of a fully computerized MCR. This could be done by holding regular meetings with the project team during the detailed design phase and each step of modernization, in relation to the criteria identified in the long term strategic plan. A main constraint in the success of a modernization project, which should be mastered, is the limited availability of the plant (generally only during the plant outage) for the integration and on-site tests of HSIs.

The project is usually split into main activities from design to commissioning (see discussion of project life cycle in Section 4.1.1). Some of these activities can be realized in parallel while others must be done sequentially. A detailed schedule describing these activities, including the utility's resources and the critical dates, must be developed. The project manager and the plant manager need to agree on this schedule and work plan within the context of the constraints of the power plant (operation and safety). This is particularly critical for installation activities during power operation.

(c) HFE programme plan. An HFE programme plan should be prepared during planning/conceptual design development. This plan should include the goals and scope of the modification, HFE activities, schedule, HFE personnel involved and their responsibility. The implementation of the HFE aspects of the plant modification should be fully integrated into the overall plant engineering process to ensure timely and complete interaction with other engineering activities. Applying a comprehensive HFE from the earlier stage of design helps ensure that a design considers impacts on all affected HSIs and the modernization does not create human performance problems. Since HFE is an essential engineering discipline along with I&C, mechanical or electrical, it should be well implemented to verify the design adequacy and correct design flaws and errors.

During basic and detail design, there should be design guides including human factors engineering principles expressed in concrete, easily observable terms. The design guide should be detailed enough to permit use by design personnel and easily understandable to achieve consistency of the design. In addition, an experienced operator from the utility should be involved in the project to gain benefit from their knowledge and get an acceptance for the HSI design. Close interactions between the utility and the supplier on the HSIs would give the most confidence to the modernization and will provide efficient training for the utility staff who will later be responsible for the operation and maintenance of the plant. However, both the utility and the supplier have to evaluate the interface with the existing facilities, which are not included in the modernization project. Cable routing and wiring connection should be carefully checked and necessary steps should be taken so the remaining and the new equipment work together. As this is a time consuming and costly activity, it should be properly prepared before the outage. The amount of interfaces to the existing power plant should not be underestimated, which can cause major impact on cost and schedule.

4.1.3. Licensing

(a) Interaction with licensing authority. It is important to keep the licensing authority informed of all tasks of the modernization project before the submittal of the safety report in order to identify potential issues and reduce licensing risk.

Plant management should ensure that a formal basis for the interaction with the licensing authority is established (list of documents, report to the project team, schedule, etc.) to help ensure regulatory compliance. A dedicated, single point of contact with the licensing authority should ensure that no deviation from the agreed licensing requirements occurs from the beginning of the licensing process to the end of the project (except as formally agreed, should the need arise).

(b) Regulatory documents. An objective of this guidance report is to provide guidance that may be applicable when making digital I&C changes that affect the control room or otherwise impact human functions and tasks. Relevant guidance is included in many documents, including federal regulations, regulatory guides, regulatory review guidance, standards, and industry guidance documents. It is important to distinguish the three types of information provided in these documents:

- Regulatory requirements. These are mandated by law, and thus must be complied with. For example, in the USA, the primary federal regulation that governs changes to a nuclear facility is 10 CFR 50.59. However, there are additional regulatory requirements that must be complied with when making changes to the control room or other HSIs. Examples of these are requirements on the application of human factors engineering in the design, requirements on specific HSI design features such as post-accident monitoring capabilities, requirements for qualified HSIs, and operator licensing requirements, In some instances, the regulations invoke the requirements of a standard (e.g. some IEEE standards are invoked) and thus those requirements become mandatory as well.
- Regulatory expectations. The regulatory requirements typically are written at a relatively high level. However, in the USA, the NRC has issued a number of NUREG reports and Regulatory Guides that describe in more detail what the regulator considers to be acceptable methods for meeting the regulatory requirements. The provisions outlined in these documents do not represent hard requirements unless the licensee commits to them formally. However, they do characterize the regulator’s expectations, so it is important to be aware of them. Also, any deviations from the approaches described in these documents are likely to receive extra scrutiny during a review by the regulator.

- Guidance. In many cases there are also industry guidelines available which, when followed, can help the licensee ensure that regulatory requirements and regulator's expectations are met for a given topic area.

(c) HFE design process. Application of human factors engineering principles and use of an appropriate HFE design process are fundamental to ensuring that changes to the control room and other HSIs are safe and effective. The regulator review of such changes will most likely focus on the HFE process used. One way to help ensure that this does not cause a problem is to obtain regulatory review of the plant's HFE programme as early as possible in the modernization process. Any issues that arise from that review can be addressed, and the programme can then be applied with confidence and referenced in any licensing activities for subsequent modifications.

4.1.4. Evaluation of hybrid HSI issues

There are a number of hybrid HSI issues that should be addressed when designing and evaluating interim HSI configurations. The issues pose potential human performance problems associated with the HSI employing a mixture of older (typically analog) and more modern, digital technologies. The issues will need to be addressed as part of detailed HSI design and development, and modification of training programmes, and may impact licensing.

Many of the hybrid HSI issues are not new, as existing plants have dealt with a mix of analog and digital technologies for some time. For example, in many plants the operators currently work with a combination of analog and digital or computer-driven displays for monitoring plant variables, including safety parameter display systems and post-accident monitoring systems. Plant computers provide graphical displays that are used under normal and emergency conditions along with conventional meters and indicators. However, as plants further modernize their control rooms over time, there will be a significant increase in the number of digital HSIs that will be used and thus hybrid issues will be more pronounced, particularly as soft controls are introduced alongside conventional controls.

The issues that are mentioned below are just some of the issues that may arise with control rooms containing hybrid HSIs. It is important that the project team:

- Specifically identify the hybrid issues that need to be addressed at each step in the migration to the end point vision;
- Assess the risks associated with them, as well as, the likelihood of a problem resulting from the hybrid situation, and potential consequences to plant safety and availability;
- Determine how they will be addressed.

This may affect planning of the activities involved in the modifications, and in some cases it could lead to changes in the designs to accommodate specific hybrid HSI concerns.

In addition to the issues which relate to potential differences between older analog and newer digital HSIs, there are other aspects of HSI design that also can introduce differences in the interfaces the operators use. An example is the use of both qualified and non-qualified HSIs. These should be considered along with the hybrid analog-digital issues discussed here.

High level issues related to overall plant operation are described first, followed by specific issues related to individual hybrid HSI elements.

High level hybrid HSI issues. HFE evaluations should address the potential impact of hybrid HSIs on operator tasks, and how this might affect plant safety. For example, the following hybrid issues [8] should be addressed:

- Inconsistencies in design or operation between different systems (e.g. one system still analog, the other system converted to digital) or between different sections of the interface, when these must be used together or alternately to perform operator tasks. Examples of operator tasks that may be affected and specific issues include the following:
    - Abnormal and emergency operating procedures, where in performing these procedures the operators must transition across a technology interface (e.g. move from analog to digital technology or vice-versa). Operator confusion at these transitions may lead to errors or delays, and thus impact on plant safety. HFE evaluation should be performed to identify transitions between interface technologies, the risks should be assessed and HSI design modified as appropriate.

- Other risk important operator actions or tasks, such as assessing the status of the critical safety functions, operator actions credited in the licensing basis, and those identified as risk significant in the probabilistic safety analysis. HFE evaluation should be performed to identify transitions between interface technologies, the risks should be assessed and HSI design modified as appropriate.

— Increased training burden in ensuring operators remain proficient with old interfaces that are retained, while gaining proficiency in use of new interfaces. Sufficient resources and time must be made available to ensure that training is accomplished effectively.

— Compromises in design to accommodate old and new technologies. For example, attempts to set lighting levels high enough to make remaining analog gauges readable but not too high for recently installed VDU displays.

Low level hybrid HSI issues. At a more detailed level, there are a number of specific issues or concerns related to various aspects of hybrid HSI designs. For example, hybrid HSIs need to be examined for the following types of hybrid HSI elements:

— Duplicated indications, where there are both analog and digital indications of the same variable.

— Duplicated controls, where both analog and digital controls are provided for the same function.

— Control tasks that require the use of analog and digital controls at different steps in the same task.

— Deactivated controls and/or indications (i.e. controls/indications left in place but non-functional).

— System/functional groupings of controls and indications in hybrid designs.

— Differences in the level of automation between analog and digital implementations.

— Hybrid alarm systems, or different implementations of alarms between analog and digital systems.

— Hybrid procedure implementations, where some procedures are converted to computer based format but others are not.

— Differences in failure modes between analog and digital HSIs.

The above are examples only. It is important for the design team to identify hybrid issues applicable to the plant-specific design at each step in the modernization programme and to ensure that the issues are adequately addressed.

4.1.5. HSI failure analysis

HSI failure analysis is very important to the design of digital systems and is a significant input to licensing. For changes that impact the control room or other HSIs, the failure analysis should include consideration of HSI failures and potential human errors in using the HSI (including both operator and maintainer errors).

Failure analysis should address:

— Impact of HSI failure on operations. Issues to consider are differences in failure modes between the old and new systems/components, failure effects on indications to the operators, potential for resulting operator error, training requirements, and testing and validation.

— Impact of HSI failure or degraded functionality, including loss of data to update displays, loss of alarms, display failure, loss of entire workstations including control capability, etc.

— How the operators will handle situations where an I&C and/or HSI problem has been detected (e.g. through self-diagnostics) but the system is still functional.

— Human error in using new HSIs, particularly issues such as new types of errors possible and new error consequences. It should be determined whether such issues have these been evaluated to show how they would be detected and corrected, and has adequate response capability been demonstrated.

When considering the potential loss or degradation of HSIs resulting in significant loss of control, monitoring and/or alarming capability, the following issues should be addressed:

- What failures or modes of degradation are credible and should be considered in the design? How frequently would these be expected to occur? Plausible common cause failures should be considered as well as single failures in determining what situations need to be evaluated.
- What is the impact of the HSI failure situation on ability to meet technical specifications and limiting condition of operation (LCO)?
- What controls, alarms, indications should be provided as a backup for each situation? What criteria should these be designed to meet? For example, should they be sufficient to monitor steady state conditions and detect any need to trip? Should they be designed to allow maneuvering the power level? Should they be sufficient to meet the technical specification surveillance requirements within the time required to restore HSI capability? There are several approaches that may be considered when there is a significant loss of HSI capability, including the following:
  - Shut the plant down using the remote shutdown panel. Adequacy of this approach has already been addressed in the plant's licensing basis. Although it is probably acceptable from a regulatory standpoint, this may not be the safest approach.
  - Provide enough backup HSI to allow the operators to hold the plant at power for a fixed timeframe. After that time, the plant would be tripped.
  - Hold at power indefinitely (no predetermined timeframe). As long as there is no transient, simply hold present power level until repairs are made. Shut down if a transient or a situation requiring trip occurs.

  Other options having greater functionality, such as the ability to maneuver power level, may also be considered.
- What is the impact on the emergency plan and declaration of emergency action levels? At a minimum, it is important to be aware of the potential to have to make notifications of unusual events when failures occur.

4.2. CONSIDERATION OF HUMAN FACTORS

Human factors should be integrated into the plant change process at various levels, from project management, to verification and validation, to end users. Where appropriate to the complexity of the change to the operator interface, the use of a multidisciplinary design team is recommended. At a minimum, a modification design team should include personnel familiar with each aspect of the system(s) being modified. Each modification should be carefully evaluated to ensure that it does not have negative impacts on other plant HSIs, whether existing or planned. The design basis should be fully documented.

The implementation details for the human factors-related activities should be included in the project plan for the modification and should not be confused with the generic procedures that are applied to all modifications. Implementation plans should include the goals and scope of the modification; an updated list of the HFE modification personnel involved and their responsibilities. Additional required items are a description of the procedures that will be invoked and how the HFE activities will be tailored to the specific modification; as well as the schedule for planning, design, V&V, procurement, installation, training, etc. The portions of the project plan that address HFE should document which HFE activities are applicable, and the scope or nature of the activities to be undertaken in each case based on a graded approach and the scope and nature of the modification. An initial assessment of the scope of HFE activities should be performed and documented as early as possible in the conceptual design phase.

Details of HFE activities should be included in the integrated budget, schedule, and implementation plan for the modification. A modification plan is used to integrate activities, coordinate the efforts of plant personnel and contractors, and ensure that resources will be available when needed to support each activity.

After the activities are defined and integrated into the plan, the planning team can assign responsibilities and allocate resources to ensure that the modification will be performed on time and within the budget.

During modification planning, some level of function analysis and allocation should be performed to define the performance requirements for new equipment, such as response times and information availability. The scope of the analysis should include all functions for which the existing equipment is used and functions for which the new equipment will be used. In most modification projects, major high level functions and their requirements may not change substantially; however, some modifications may change the allocation of functions between human and machine. These types of changes can have broad effects on crew coordination, procedures, training, and the amount of information needed at the workstation.

Functional requirements analysis ensures that all functional requirements that must be met after the change is implemented are identified. While this analysis does not reach the level of detail needed to specify components, it is needed to perform a task analysis and to develop V&V criteria. It can also be used to identify changes in the operators' responsibilities for a given function.

Note that it is very important to pay particular attention to modifications that affect functions that are identified as important to nuclear and personnel safety and plant availability or that change the allocation of those functions. The following section describes the function analysis and task analysis in more detail

4.2.1. Function analysis

NUREG-0700 [9] states function analysis is to define and to evaluate the functions and actions to be performed by the operator in the MCR, and to verify that operator procedures are adequate to guide the operators during operation of plant systems and verify effective performance during system operation. IEC 60964 [12] states that function analysis should hierarchically identify goals for the control room design covering all operational states and accident conditions. NUREG-0711 [11] states that function analysis is the identification of functions that must be performed to satisfy plant safety objectives; to prevent or mitigate the consequences of postulated accidents that could damage the plant or cause undue risk to the health and safety of the public. Therefore, function analysis should be conducted to:

- Determine the objectives, performance requirements, and constraints of the design;
- Define the functions that must be accomplished to meet the objectives and required performance;
- Define the relationships between functions and plant process (plant configuration and success path) responsible for performing the function;
- Provide a framework for understanding the role of controllers (whether personnel or system) for controlling the plant process.

The term function can refer to a high level plant function, such as critical safety function, or merely the functioning of an individual piece of equipment. An NPP is a large complex system which is composed of interrelated subsystems that have their own subsystems, and so on, until some lowest level of an elementary component is reached. Intra-component (components may be composed of human–software–hardware) linkages are generally stronger than inter-component linkages.

Figure 3 shows a hierarchically linked complex system with various subsystems. The space structure can represent structural hierarchy, and the dynamic system presentation can represent functional hierarchy, behavioral hierarchy, goal/condition hierarchy and event hierarchy.

Structural hierarchy is difficult to represent all information of a complex system. Therefore, functional hierarchy can correctly express the role of each component of system as well as describe all information of system. High level functions are usually achieved through some combination of low level function, and may require human actions. Human involvement may be needed at any or all levels of functional structure.

Functional hierarchy can represent the hierarchically tree structure from top objectives, such as power production and maintain safety, to function, sub function, system, and components. Figure 4 shows conceptual functional hierarchy.

4.2.1.1. Use of function analysis

Figure 5 shows a typical control room engineering process. An iterative approach to function decomposition is recommended as opposed to one full comprehensive analysis. Function analysis, at first, should be considered to be a higher level analysis supporting the conceptual design. Task analysis is overlapped with function analysis and is analyzed for the more detailed level of operational analysis. The VDU based display will have specific task oriented display, procedure based display, physical process flow based display and function based display. Function analysis will support well organized hierarchy display of function. Function analyses are required to support the following control room design activities:

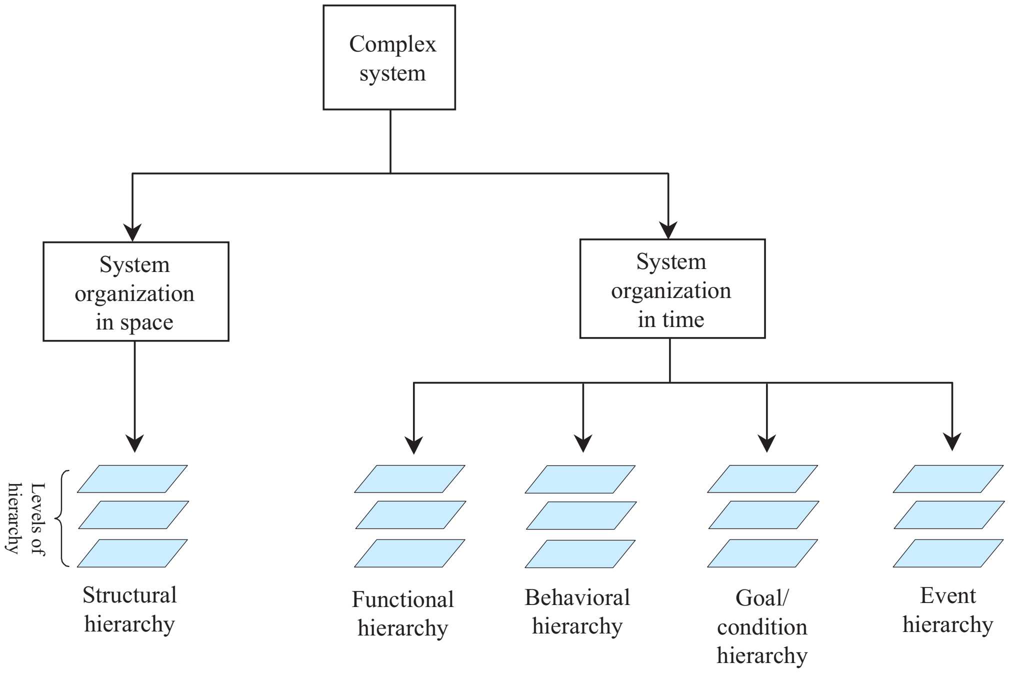


FIG. 3. System hierarchy structure linked with complex interface.

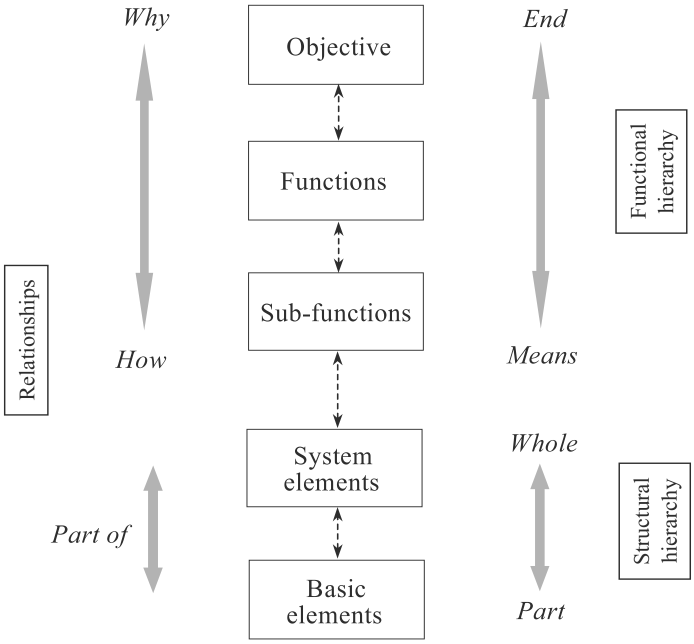


FIG. 4. Conceptual functional structure hierarchy.

- — Support a hierarchical structure for the function allocation between machine (automatic) and human (manual);
- — Support or guide overall control room design configuration by using a high level functional decomposition;
- — Support a partitioning or assignment of panel layout for controls, displays and alarms;
- — Support of grouping of each panel components;
- — Support function based display design of VDU based display;
- — Function analysis should support the task analysis which will be performed at a later stage of the design;
- — Support of verification and validation.

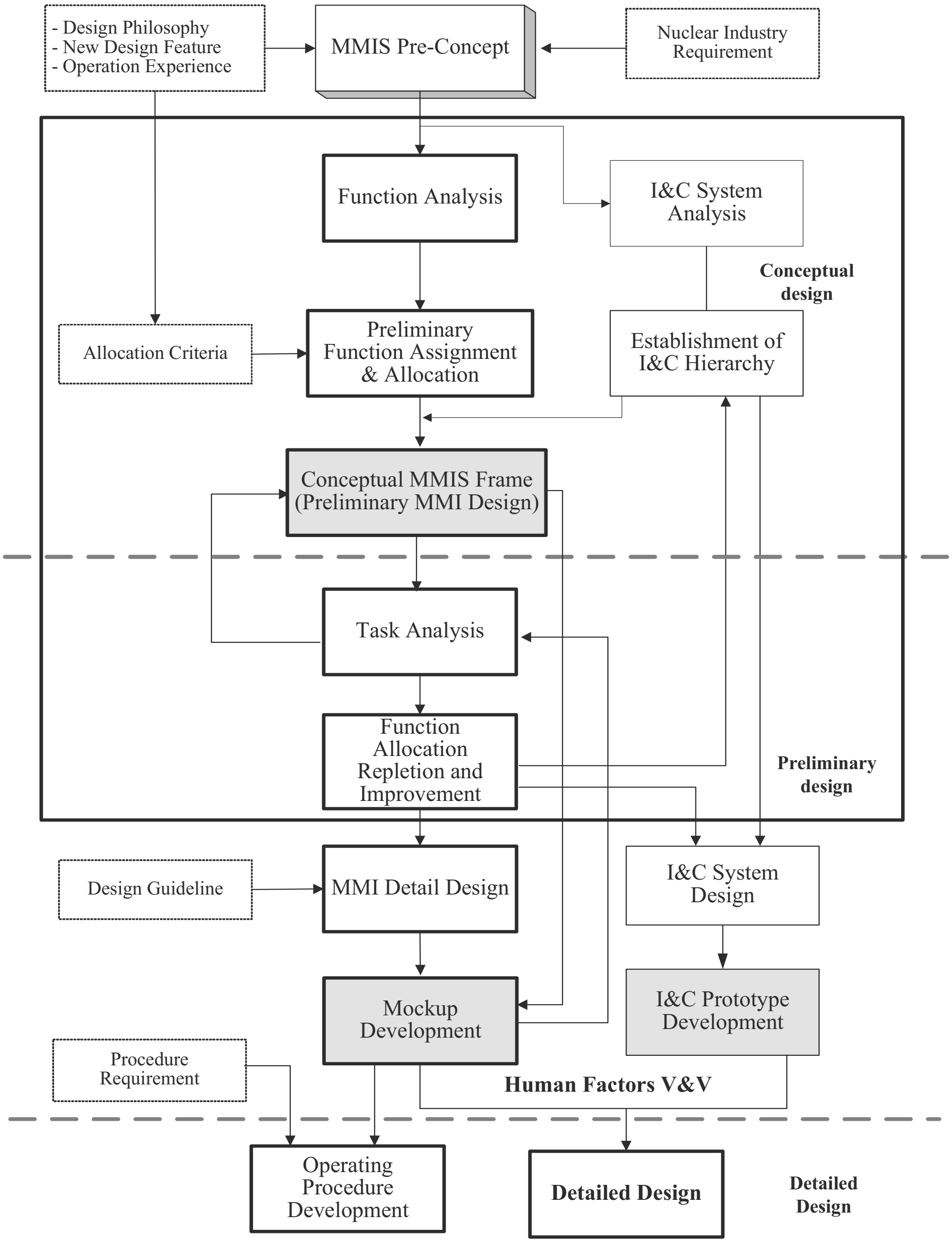


FIG. 5. Typical control room engineering process.

4.2.1.2. Incorporation of function analysis into modernization

Function analyses should be revised and updated for all modernizations:

- — That are safety significant;
- — Affect the role of human;
- — Likely to change existing safety functions;
- — Introduce new functions for systems supporting safety functions;
- — Involve unclear functional requirements that may be important to safety.

The scope of function analyses are to be restricted to functions related to modernization. One of the design goals of the plant modernization may be function changing and modification of level of automation. However, high level plant function and thermo-hydraulic functions are seldom; modernization programmes often modify plant systems and HSIs. Therefore, the modernization may affect the allocation of new and existing functions to human. Additionally, modernization can change the level of automation of the original design, which may result in the change of allocation of human tasks, and in turn affect the roles and responsibilities of human. The automation can involve an entire process control sequence or it can be applied to the generic activities involved in decision making. The operator's role is shifting away from directly controlling plant systems and toward monitoring automated systems and sometimes intervening in case of incorrect functioning. A change in an operator's role due to modernization should be examined within the context of its effects on the operator's overall responsibilities.

Because the whole function analysis and allocation process should be iterative, analysis can begin at the earliest stages in the modernization planning. Function allocation can be refined as more information. For the performance of function allocation, rules and priorities should be defined. Generally, function allocation rules are the following four categories.

— Mandatory required by regulatory requirements;
— Technical feasibility of automatic implementation;
— Cost effectiveness;
— Cognitive usefulness/continuous situation awareness.

From the above rules, allocation should first be considered whether it is mandatory, required by regulatory requirements. If it is not, determine whether the function is automatic or not. If it is automatic, an evaluation should be performed as to whether there is some need for human involvement. If not, a specific reason for human involvement, full automation is suggested. If some function is not considered automatic, then it can be re-evaluated based on technical feasibility of automatic implementation and cost effectiveness (see Fig. 6).

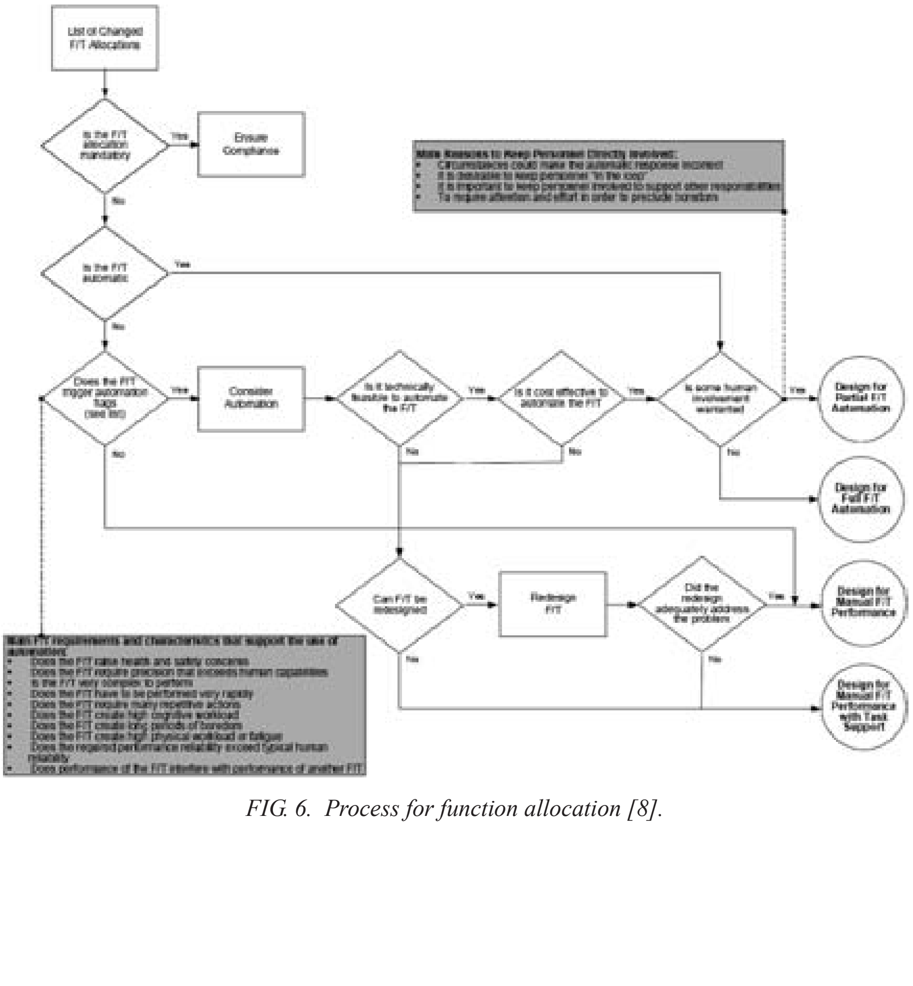

List of Changed F/T Allocations
Is the F/T allocation mandatory
Yes
Ensure Compliance
No
Main Reasons to Keep Personnel Directly Involved:
Circumstances could make the automatic response incorrect
It is desirable to keep personnel "in the loop"
It is important to keep personnel involved to support other responsibilities
To require attention and effort in order to preclude boredom
Is the F/T automatic
Yes
No
Does the F/T trigger automation flags (see list)
Yes
Consider Automation
Is it technically feasible to automate the F/T
Yes
Is it cost effective to automate the F/T
Yes
Is some human involvement warranted
Yes
Design for Partial F/T Automation
No
No
No
No
Design for Full F/T Automation
Can F/T be redesigned
Yes
Redesign F/T
Did the redesign adequately address the problem
Yes
Design for Manual F/T Performance
No
No
Design for Manual F/T Performance with Task Support
Main F/T requirements and characteristics that support the use of automation:
Does the F/T raise health and safety concerns
Does the F/T require precision that exceeds human capabilities
Is the F/T very complex to perform
Does the F/T have to be performed very rapidly
Does the F/T require many repetitive actions
Does the F/T create high cognitive workload
Does the F/T create long periods of boredom
Does the F/T create high physical workload or fatigue
Does the required performance reliability exceed typical human reliability
Does performance of the F/T interfere with performance of another F/T

FIG. 6. Process for function allocation [8].

4.2.2. Task analysis

4.2.2.1. Overview of task analysis

The functions allocated to human define their roles and responsibilities. Human actions are performed to accomplish these functions. Human actions can be further divided into tasks, which are a group of related activities that have a common objective or goal. Task analysis is the identification of requirements for accomplishing these tasks, i.e. for specifying the requirements for the displays, data, processing, controls, and job support aids needed to accomplish tasks.

Task analysis is a means to ensure that necessary operator tasks can be successfully performed. The approach functionally decomposes the physical plant and its operations so that procedural tasks and decision processing can be analyzed independent of particular hardware implementations. As such, the results of task analysis are identified as inputs in many HFE activities, e.g. it should provide input to the design of HSI, procedures, and personnel training programmes.

For the plant modifications that are likely to affect risk-important human actions, cause existing human actions to become risk important, or create new actions that are risk-important, the tasks analyses should be revised and updated to reflect requirements of the modernization. The function allocation analysis identified tasks associated with modification that are new or modified due to change in the level of automation.

The scope of analyses should include tasks involving the modification and its interactions with the rest of the plant, including those resulting from functions addressed in the function analyses and function allocation. For maintenance, tests, inspections, and surveillances, attention should be given to risk-important actions that are new or supported by new technologies (e.g. new capabilities for on-line maintenance). For example, if the critical functions are automated, the analyses should consider all human tasks including monitoring of the automated system and execution of backup actions when the system fails.

The task analysis for modernization should identify the design characteristics of the existing HSIs that support the performance of experienced personnel (e.g. support high levels of performance during demanding situations). These design characteristics should be considered in developing new design requirements. That is, the new design should have features performing similar functions, or should eliminate the need for them by performing these functions differently. All task demands, considering the new design features, should be adequately addressed by the new design requirements.

4.2.2.2. Description of task decomposition

Task decomposition is an information collection tool, which is used to systematically expand upon the basic description of the activities, which must be undertaken in each task activities. Hierarchical task analysis is a method of decomposing higher level function to the information and controls that human need to perform his tasks (Fig. 7). Depending on the complexity of the tasks or function, there can be many levels. The high level function is broken into sub-functions. The sub-functions can be broken into tasks. The tasks can be broken into task steps. The steps can be further broken into activities. Activities are the lowest level of analysis and describe behaviors such as monitor reactor control system temperature.

High level function is normally operating procedure. Sub-functions are high level statements of the operation's general purpose in performing a related set of tasks. They specify a basic operating goal (e.g. maintain reactor control system heat removal) from the operator's perspective. Each sub-function statement represents one or more tasks with a single main purpose, and may be comprised in different situations by different sets of tasks. Tasks level analyzes operator behaviors in terms of a generic, closed loop information processing model as follows:

— Plan: Evaluate, calculate and decide (etc.) on a result or course of action based on collected or otherwise known information;

— Do: Perform the act or manipulation specified;

— See: Collect information or monitor the results of output and transmit the results back to the input; this either verifies success or cues further processing and corrective action.

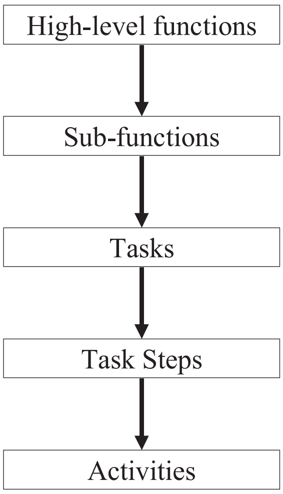


FIG. 7. Hierarchical structure.

Tasks in a sequence tend to cycle through these categories, although well-designed and skillfully performed tasks do not necessarily show distinct categories. The benefit of this framework is that it directs the analyst's attention to the necessary components of deliberate, rule based (i.e. procedural) behavior.

The task steps level of this analysis specifies critical details that may be associated with each task activities.

4.2.2.3. How to incorporate in modernization

Task analysis provides detailed information needed to perform tasks. The results of tasks analysis are used as one of the inputs in the staffing analyses. However, the operational staffing for modernization is not likely to change. The task requirements are also an important input in HSI design. It is even more effective VDU based HSI design than conventional analog panel design because of the high degree of freedom in designing the alarms, displays, and controls to be much more task specific. Therefore, it is very easy for task requirements to directly be developed into task oriented displays, such as a startup task display. Even if displays are not task oriented, the information can be used to determine what should be displayed and how information should be grouped.

Figure 8 shows the structure of a function based display using task analysis results and function decomposition. A few goals can be extracted from the procedure, and these goals can be broken into more detail functions. These functions also can be decomposed into tasks as mentioned in Section 4.2.2.2. Figure 9 shows the display design model of a function based display.

Also, task requirements and sequence information are significant inputs in procedure development. In fact, draft procedures can be written directly from the task analysis when new tasks are issued from function allocation.

For modernization, the initial task analyses are usually performed from the existing well-established procedure used with the existing system. System designer procedure to changing function also may be utilized as a starting point for analysis of tasks. Finally, the task analysis should be performed in conjunction with the development of modified procedures. Task analysis information is also an input for trainers since the analysis identifies what skills and abilities need to perform the tasks. For a new plant design, the skills, knowledge and abilities identified from the task analysis can be reflected in crew selection and development of a training programme. For modernization, the necessities of change of existing training programme should be defined based on the results of task analysis, and this should reflect modification of a training programme.

4.2.2.4. Documentation

Adequate documentation should be produced to verify human factors involvement in control room design. These documents are prepared in such a way that later review or outside audit would be able to interpret them and verify their purpose and content. The task area data may be stored on a database system to allow manipulation and updating of information. As additions are made to the database, existing portions of the analysis will be updated to

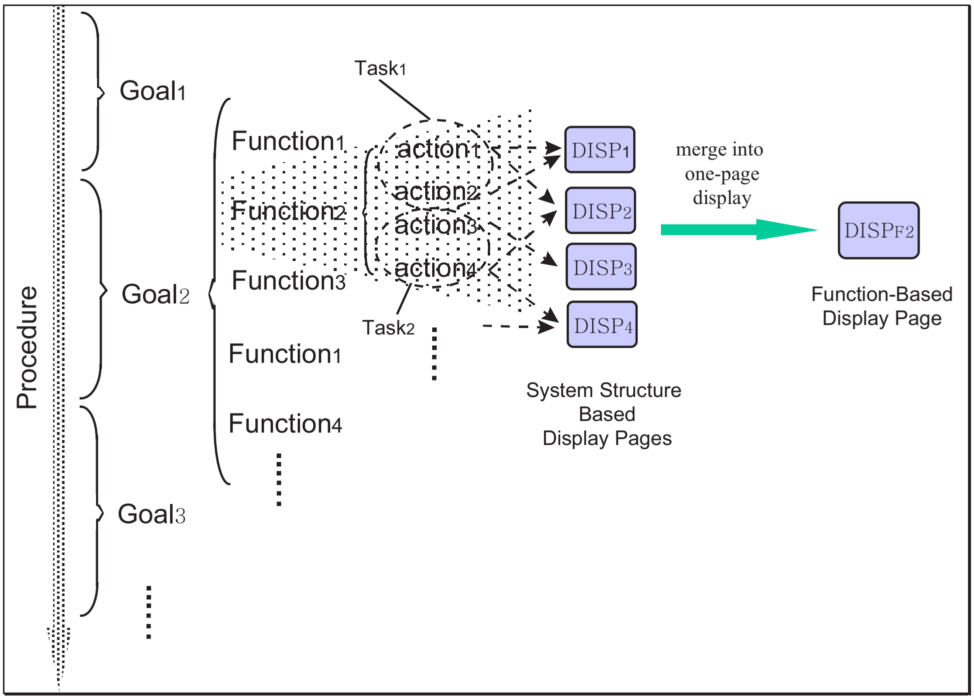


FIG. 8. Function based display structure.

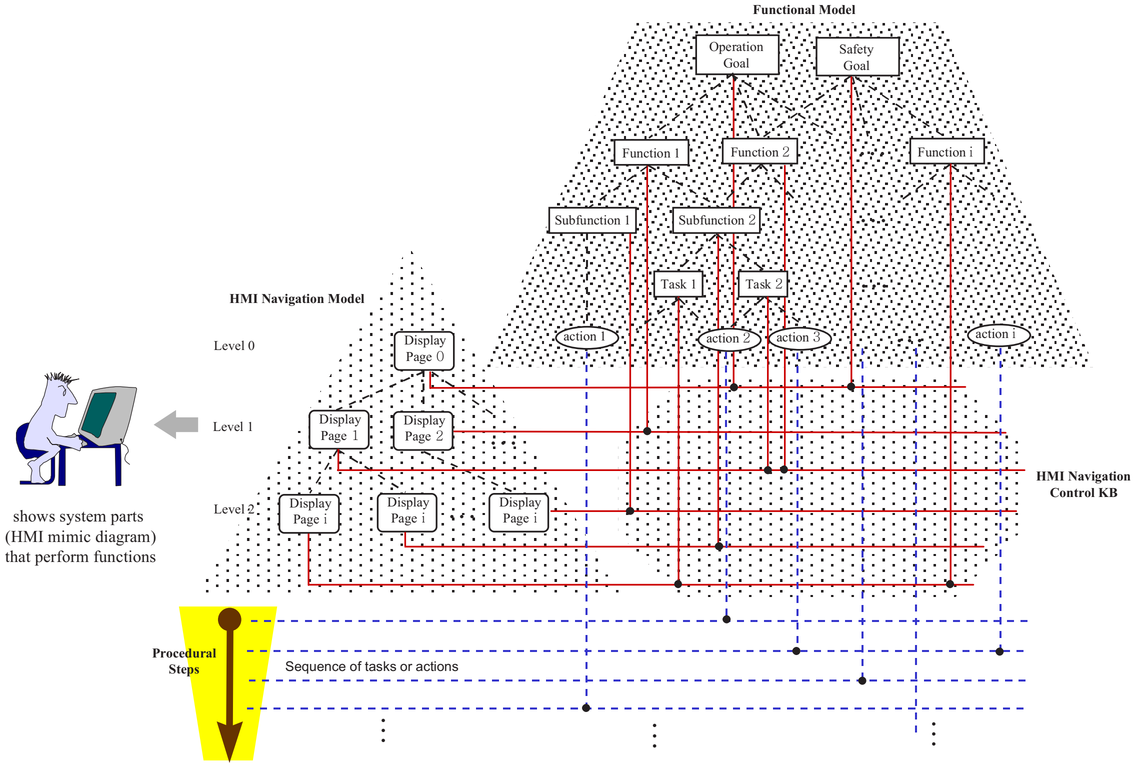


FIG. 9. Function based display design model.

reflect any changes to the task area. This will ensure internal consistency of the final task area results and provide input to the HSI design. When completed, the task area database will incorporate all event sequences, and the related results from the analysis of those sequences.

4.2.3. Human factors issues in modernization

The hybrid HSI, using a mixture of conventional and advanced technology, may enhance system performance and reduce human reliability, but may also spawn new types of human errors. The trends of hybrid HSI design are:

- Extension of automation of plant control functions;
- Development of computer based alarm system;
- Development of information and display system;
- Use of soft control, development of computerized procedure system;
- Development of computerized operator support systems (COSS).

The great extension of automation can affect operator situation awareness and operator's vigilance in monitoring because the operators gradually trust in automation, and may not positively intervene/participate in the operation loop. The great degrees of automation and computerized HSIs are also associated with workload and crew performance.

Also, modern digital technology enables plant automation to enhance human activities and reduce human error. Tasks that are difficult or tedious can be automated thus freeing humans to perform more supervisory activities, as well as reducing the likelihood of human error. Newer approaches to automation reflect greater cooperation between automatic systems and plant personnel. Opportunities exist to use differing levels of automation in an effort to combine human and automated system capabilities in a complementary manner. In addition, automation is being applied to more than plant control functions, i.e. functions such as monitoring and fault detection, situation assessment and response planning. In light of these developments, designers are faced with decisions as to what to automate and how the personnel interaction with automation should be designed. Historically such decisions were mainly based on available technology. That is, a function that could be cost effectively automated was automated. Tasks that could not be automated were performed by personnel. However, this was not the best approach from the standpoint of human performance or for overall safety and productivity. Thus, new approaches are needed to optimize overall plant performance by allocating functions between personnel and automation such that the strengths and weaknesses of each are considered.

The computerized HSIs can provide flexibility for designer/operator and give an expanded range of data available to the operator. They reduce the workload associated with gathering, integrating and interpreting parameter information needed to work through the emergency response procedure.

4.2.3.1. Poor automation causes poor personnel performance

Automation is often employed to achieve more reliable and precise control. This is positive from a reliability standpoint, since personnel are considered one of the more unpredictable components in the system. Thus, automation can enhance overall system reliability by removing or reducing the need for human action. However, it is also important to understand the effects of poor automation design on personnel. These effects are summarized below:

- Change in the overall role of plant personnel. Automation changes the roles and responsibilities of personnel and, if not evaluated, can result into tasks that are difficult for personnel to perform;
- Understanding automation. Automation can add to the overall complexity of the plant. If personnel do not develop an understanding of automation, it is difficult for them to properly monitor and supervise its actions;
- Situation awareness. When functions and tasks are performed by automation, it is sometimes difficult for personnel to remain aware of the status of its functions;
- Workload and skill. Automation shifts personnel workload from that associated with direct control to that associated with monitoring. When functions and tasks are automated, it can impact the ability of personnel to skillfully perform them because the skills are much less used;
- Trust and complacency. Since automation works very well most of the time, personnel develop a trust in it. When that happens they can sometimes become complacent and not monitor its performance effectively;

- New types of human errors. Interactions with automation lead to new types of errors that must be dealt with, such as mode error (acting as though an automatic system is in one mode when it's actually in a different mode).

These effects are the result of poor automation design. Thus, in addition to designing automation itself, it is important to design the human-automation interaction. A clear focus on identifying the impact on human roles and responsibilities can support the design of more effective automatic systems that avoid many of these issues. Design methods can help ensure that the benefits are achieved and the challenges are avoided. These methods are discussed in the following sections.

4.2.3.1.1. Defining the relative role of humans and automation

The role of personnel is defined as the integration of the functional responsibilities they perform to achieve the plant's missions and goals. This role is the result of the functions that have been allocated to personnel, including those associated with their role in the monitoring and supervision of the automated systems.

Once plant functions and tasks are defined in sufficient detail, they can be allocated to (a) personnel (e.g. manual control), (b) system elements (e.g. automatic control) and (c) combinations of manual and automation (e.g. shared control). Function and task allocation seeks to enhance overall productivity, reliability and safety by exploiting the strengths of personnel and systems, including improvements that can be achieved through the assignment of control to these entities with overlapping and redundant responsibilities.

Improvements to function allocation methods are needed to make the results more useful in the engineering design process. The following are areas where improvements are needed:

- Integration of multiple analysis factors;
- Expansion in allocation options;
- Consideration of human role in automated processes;
- Analysis of functions in a realistic context;
- Use of multiple sources of data.

EPRI report 1011851 [13] describes a method for function allocation that addresses these needs. While the methodology can be applied to new plants, new systems introduced into existing plants, and plant modernization programmes, it includes special considerations for the latter.

The objective of this analysis is to specify the roles and responsibilities of plant personnel performing plant functions and tasks, and how those roles may change as a result of the planned modification. The methodology:

- Evaluates functions and tasks that may be impacted, either deliberately or inadvertently, by the changes made to plant systems as part of the plant modernization project;
- Evaluates the suitability of full automation, partial automation and manual function and task performance;
- Identifies the design consequences of allocation decisions;
- Provides a basis for allocation decisions.

The analysis is performed iteratively as the design evolves. Allocations may be qualitatively performed in the beginning for higher level functions and later more quantitative assessments are made for the detailed tasks.

4.2.3.1.2. Providing HSIs that support human-automation interaction

The analysis of the reasons personnel are challenged by poor automation design provides a basis for the development of guidance for designing better HSIs. Even when a process is fully automated, personnel must still monitor its performance, judge its acceptability, and when necessary, assume control. HSIs have generally been lacking in their ability to support these personnel task demands. Automated systems have often been designed with inadequate communication facilities, which make them less observable and impair the operator's ability to track their progress and understand their actions. These lessons learned offer a basis for the development of guidelines to support better personnel-automation interaction. The guidelines in Reference [12] are generally oriented to providing the enhanced ability of personnel to monitor and supervise automation, and greater cooperation between human and autonomous agents.

Thus, the design of the automation itself and the HSIs that support it must provide the basic functionality to enable:

- Personnel to monitor automation, especially goals, status and potential degraded conditions;
- Personnel to supervise automation, such as to redirect automation's goals, redefine task sharing, or to assume manual control;
- Automation to communicate with personnel by sending messages or through alarms;
- Automation to monitor personnel, especially goals and activities that impact automations functioning.

The lessons learned also emphasize the importance of supporting and reinforcing human interaction with automation through procedures and training. For example, procedures and training are needed to support personnel in the event of degraded conditions or loss of the automated system. Training is also needed on the monitoring and supervision of automation.

4.2.3.2. Automation complexity increases operator's mental model

The increased automation can make it easier to perform control actions because the increased level of automation simplified many steps in the process. However, it is more difficult for the operator to understand the structure of the automated system and how it works. Automation can increase the complexity of the plant and problems can arise because the operator lacks a good mental model of the behavior of the automated system. As the plant became more automated, the operator would be required to understand the complex software algorithms. Operators need to understand how information is processed by the automated system so they can determine whether the result is relevant to the task situation and whether the automated system is operating properly. The lack of an appropriate mental model can result in operator actions that produce unexpected consequences, such as improperly planned intended actions and unintended operator actions.

4.2.3.3. Poor situation awareness, workload

It has been stated by many researchers that the increased automation has been frequently associated with loss of operator vigilance and situation awareness.

Automation can remove the operator from direct control of the plant and reduce monitoring workload during the periods of stable plant condition. However, the operator may be required to employ high cognitive workload and alertness for the monitoring of the plant variables and detection of transients/anomalies. Moreover, it is difficult to maintain the situation because automation generally leads to excluding the operator from the control loop. Therefore, human interactions with a highly automated system can cause poor situation awareness.

4.2.3.4. Impacts on staffing requirements and the role of the crew

Initial staffing levels may be established based on experience with previous plants, staffing goals, initial analyses and government regulations. However, HSI modernizations may affect the number of operators and their required skills and expertise. Staffing requirements should be changed for control room modernizations that are significant to plant safety, affect the role of the operators or their tasks and are likely to change staffing requirements. The scope of the staffing analysis should cover demands resulting from the modernization and its interactions with the plant.

The number of control room (CR) operators may be affected by factors that increase workload or compromise the operator's performance. Even if the operator's functions are unchanged, their tasks may alter the required staffing levels. Additional operators may be needed if the frequency or difficulty of tasks increase and they cannot be performed effectively by current staff.

The knowledge, skill, or abilities of staff may be affected by any modifications. For example, an advanced modification may require an operator to have a more sophisticated understanding of thermo-hydraulics which may currently be lacking. Also, the design of HSI may require operators to have special skills in human computer interactions.

Increases in automation result in a shift of the operator's function from that of a direct manual controller to a supervisory controller and system monitor.

Personnel roles can be defined as the integration of the responsibilities that operators and other personnel perform in the fulfillment of the mission of plant systems and functions. Responsibilities are defined with regard to a spectrum of control modes. The focus of the role is on the operator's control authority and responsibility in the specific context of the plant functions and systems in which the operator is a part of the control loop.

Operators have monitoring and decision making responsibilities as well and these activities are facilitated by various levels of automation. However, the concept of the role is focused on control loop characteristics. The operator's role should be deferred as the total integration across plant functions and systems of the operator's responsibility and not at the individual system level, in isolation of other systems.

Since the operator's role is defined in terms of plant functions and systems and the operator's responsibility in each, the notion of ‘change’ in an operator's role can result from changes to either plant functions and systems, allocation of function, or both.

Function allocation seeks to enhance overall plant safety and reliability by exploiting the strengths of personnel and system elements, including improvements that can be achieved through the assignment of control to these elements with overlapping and redundant responsibilities.

4.2.3.5. Crew communication

As indicated before, automation and advanced control and display capabilities can reduce operator workload under normal operating conditions. However, they may increase workload in other situations.

Crew coordination and teamwork in advanced HSIs is an important aspect of NPP operation. The conventional CR has characteristics that support operators ability to observe each other and maintain awareness of each other's actions. However, computer based CRs may present special challenges to crew coordination and affect the ability of crew to maintain awareness of each other's activities.

4.2.3.6. Mode errors

Automated systems may have various modes that the inputs used and outputs provided are different. Operator inputs may have different effects depending upon the characteristics of each operating mode. Automated systems should be designed to inform the operator of its current operating mode, mode transition points, limits on operator actions, and circumstances in which operators need to assume control.

4.2.3.7. Inconsistencies between conventional and new HSI causing problems

In case of automation and hybrid HSI modernization, such as flat panel displays design and soft control using computer system, the HSI may contain different user interface for presenting information with conventional interface and different mechanisms for accessing and controlling it. This may affect the overall consistency of the HSI. When an operator lacks the knowledge to operate the interface, the operator may derive an inappropriate action sequence. For high level automation and advanced HSIs, it may be difficult to determine the appropriate level of operator knowledge. Operators of highly automated plants may require much more training due to the complexity of the plant design than operators of less automated plants. However, such training can result in operators acquiring knowledge that does not have an obvious relationship to their operational responsibilities and, thus may not be readily applicable to operational tasks.

4.2.3.8. Issues to HSIs

(a) VDU alarms
- Display of alarm information: Typical conventional alarm tiles are an example of spatially-dedicated, continuously-visible alarm display. Variable alarms displays are not presented in a fixed location and are usually presented according to some logic such as time or priority. A message list using a VDU is an example of this type of display. A conventional alarm display is more superior to a variable display during over crowding alarm condition in aspect of rapid detection and enhanced pattern recognition;
- Alarm message design;
- Use of auditory cues;
- Alarm system control and management;
- Alarm system integration.

(b) Information and display system
- Information design and organization;
- Display management and navigation;
- Volume of information;
- Density of display information.

(c) Soft control
- Time delays and control stability;
- Input and feedback methods for continuous-variable inputs;
- Confirmation and warning messages;
- Sequential plant control and interface management tasks;
- Access to one versus multiple input fields at one time;
- Interaction of soft controls with automation;
- Soft controls and display space;
- Keyboards versus incremental input devices;
- Consistency of soft controls in hybrid HSIs.

(d) Computerized procedure system
- Role of plant personnel in managing procedures;
- Team performance;
- Situation assessment, response planning and operator error;
- Level of automation of procedure functions;
- Keyhole effects and use of multiple CPS;
- CPS failure in a complex situation.

(e) COSS (computerized operator supporting system)
- Task relevance of the information provided;
- Level of explanatory detail;
- The complexity of information process;
- Integration of the rest of HSIs, and etc.

4.2.4. Other design considerations

4.2.4.1. Displays

During the modernization of the MCR, VDUs can replace all or part of the previous instruments and controls on the control panels. Displays on the VDUs not only provide information but are also used for the control of the NPP as a form of soft control for the operators in the fully computerized MCR. Therefore the display design is very important for the efficient and reliable functioning of the modernized MCR. The hierarchy and configuration of the displays should be well structured such that the operators in MCR will not have any difficulties or cognitive burden in finding information or navigating to other displays.

The display should contain all the plant information that is available to the operators in a structured format and be designed to aid operational activities of the plant by providing trends, present value, controls, categorized listings, messages, operational prompts, as well as alert the operator to abnormal processes. Generally the display types to be included are system mimic display, critical safety function display, computerized procedure system (CPS) display, global display, soft control display, alarm display and operational aided display (function or task based display)

With respect to computer based displays, the primary form of information presentation in many plants is typically system oriented mimic displays. While system oriented mimics are well suited to some personnel tasks, they may not be effective for other important activities that personnel perform. An example is the task of plant startup. Crews need access to information about many different systems. Thus for startup, when only system oriented displays are available, operators need to access many different displays to retrieve needed task information. Analysis is needed to decide how to display the information and what information to display. System engineering approach is commonly used for specifying information requirements. Task analysis is applied to identify the specific alarm, indication and controls needed for personnel to perform their tasks. Whatever methods are used, information requirements analysis must be performed to identify the needed displays and their information contents.

The display navigation is important for personnel to access the required information. A poor navigation can cause added mental workload including the probability of human error. Simplifying the navigation action can reduce the demands imposed on cognitive resources, especially central cognitive processes (e.g. determining relationships between the current and desired locations) and response processes (e.g. manipulating the navigation control). Moving from one location to another on the display page requires time. It may be affected by such factors as the number of steps in a navigation move, the length of the navigation moves, and the display system's response time. As the length of time increases there is an increased likelihood that the information held in working memory will be lost. Therefore, the amount of time needed to complete a navigation move should be minimized. Minimizing the navigation distance can reduce the amount of time that information must be held in working memory, thereby reducing cognitive demands on the operator. One approach may be to provide broad, shallow menu structures rather than narrow, deep ones. However, the former may be impractical if the total number of menu items is large and the display devices have limited space for presenting them. In such cases, additional navigational mechanisms should be considered such as direct keyword retrieval. Other features for reducing navigation distance should be used such as navigation shortcuts (e.g. buttons for jumping to the top of the menu or major branches without accessing intermediate nodes) and buttons for accessing previous displays. The followings are examples of general guidelines for the design of the displays:

- Display screen partitioning for HSI functions. A standard display screen organization should be evident for the location of various HSI functions (such as a data display zone, control zone, or message zone) from one display to another;
- Distinctive HSI functional organization and display elements. The HSI functional zones and display features should be visually distinctive from one another, especially for on-screen command and control elements (which should be visibly distinct from all other screen structures);
- Hierarchy of titles. Where displays have several levels of titles (and/or labels), the system should provide visual cues to aid users in distinguishing among the levels in the hierarchy;
- Normal value reference index. Displays should contain reference(s) to the values of normal operating condition(s);
- Critical value reference index. A reference index should be included in a display when the user must compare displayed information with some critical value. Limit marks should be used for each critical plant parameter displayed;
- Freeze feedback. If a display has a freeze capability, the display should have an obvious reminder that it is in the freeze mode;
- Data overlays. Displayed information which temporarily overlays and obscures other display data should not erase the overlaid data;
- Physical overlays. Overlays should not distract or interfere with the observation or interpretation of displayed information;
- Correspondence mapping. There should be an explicit mapping between the characteristics and functions of the system to be represented and the features of the display representation, i.e. changes in the appearance of the display form should have a one-to-one relation with the plant states it represents. These changes should result from explicit rules relating the physical form of the display and it's meaning to the plant state represented;

- Coherence mapping. The characteristics and features of the display used to represent the process should be readily perceived and interpreted by the operator;
- Display of goal status. The information system should provide for global situation awareness (i.e. an overview of the status of all the operator's goals at all times) as well as supplying details about the current specific goal;
- Failure recognition. Information system failure should be indicated;
- Display failure indications. Displays should be designed so that a loss of power or signal to the display or display circuitry is readily distinguished from the range of possible readings for the displayed parameter.

4.2.4.2. Safety console design (sometimes not needed for hybrid solutions)

The safety console is a backup panel to the computerized HSI. In the complete loss of computerized HSI, the operators should have diverse means to maintain the NPP in the safe condition. The extent of the diverse HSI capability that is needed depend to a great extent on how the plant wants to respond to loss of the normal HSI. A variety of options are possible, including:

- Immediately shut down the plant;
- Maintain the current state for a specific period of time (assuming the reactor is at power and no secondary event has occurred) and monitor plant safety functions for the need to shut down;
- Support power maneuvers;
- Handle plant upsets and emergencies.

Dedicated control switches needed for the safe shutdown and engineered safety features operation should be installed on the safety console. Those are safety qualified and have hardwired connection to the controllers to avoid loss of functioning due to the data link failure. The safety console should also have qualified information displays and/or indicators needed for the safety controls and monitoring of safety parameters. The safety console should also accommodate the qualified minimum inventory controls for performing the emergency operating procedures. The safety console may have the displays and controls used in support of maintenance activities and instrument testing during normal operations and shutdown conditions. The safety console should be designed to meet the licensing requirements to cope with the common mode failure of information systems.

If, in future, next generation plants have no hardwired devices in the control room and this concept is accepted, this document will be revised accordingly.

4.2.4.3. Control room environment/layout

The MCR environment should be adequately designed, configured, and maintained to support the operators' comfortable and efficient task performance. The followings are examples of general guidelines that can be considered for the modernization of the MCR:

- Lighting and illumination: An acceptable illumination level should be determined to allow easy performance of all operator tasks based on conservative assumptions about the reflectance of the task background, the age of the operator, and the criticality of the task being performed. VDUs, traditional control/display, and paper documentation usually require different lighting environments within the same control room area. With respect to computer driven displays, glare may be a greater concern than the level of illumination. To meet varying lighting requirements, specific illumination level for particular areas, such as workstations, individual control and display devices, and areas used for reading and writing should be considered and be adjusted by dimmer switches located at the control room;
- Uniformity: The level of illumination should not vary greatly over a given work station;
- Supplemental light: Supplemental lighting should be provided for personnel performing specialized visual tasks in areas where fixed illumination is not adequate;
- Color: Surface colors should be recognizable under both normal and emergency lighting conditions;
- Ambient illumination and VDUs: The ambient illumination in the VDU area that is necessary for other visual functions (e.g. setting controls, reading instruments) should not degrade the visibility of signals on the VDU;

- Use of colored ambient illumination: Colored ambient illumination should not be used if color coding is used in the workplace;
- Emergency lighting: A control room emergency lighting system should be automatically activated and immediately available upon failure of the normal control room lighting system. Failure of the normal control room lighting system should not degrade operability of the emergency lighting system;
- Glare and reflectance: Glare increases the probability that an individual will misread a display or will fail to notice displayed information. Glare can also produce discomfort. To minimize the glare and reflection, VDUs can be equipped with shields, or the display faces themselves treated to diffuse reflections. In addition to this, following guideline should be considered to minimize reflections;
  - Noise levels: Background noise should not impair verbal communication between any two points in the primary operating area;
  - Availability of indications and controls: Control rooms should have all the controls and displays needed to detect abnormal conditions and bring the facility to a safe condition, as required by availability analysis;
  - Accessibility of instrumentation and controls: The operators should not need to leave the controlling workspace to attend to instrumentation on back panels during operational sequences which require continuous monitoring or timely control actions. Actions that must be taken promptly to assure plant safety should be capable of being performed directly from the control room;
  - Field of view: Operators at desks/consoles in the controlling workspace should have an unobstructed view of all controls and displays on the consoles and the large display panels.

4.2.4.4. Cyber security considerations

As main control rooms increasingly employ computer based digital technologies and interconnected networks, computer security plays a vital role in ensuring safe operation. Computer or cyber security objectives are commonly defined as protecting the confidentiality, integrity, availability of electronic data or computer systems and processes. In order to achieve this, it is important in the early design and engineering phase of the modernization project to establish a programme (or upgrade an existing one) aimed at protecting computer systems, networks and other digital systems that are critical to the safe and secure operation of the facility and for preventing theft, sabotage and other malicious acts.

Due to the high concentration of information and human-system interaction, the cyber security of control rooms and other interface systems is one of the most important components of the overall plant security (computer and physical) programme. Cyber security is built from the consideration of possible threats and the development of a design basis threat defined within the context of cyber security. The tools for identifying threats and building barriers include both technical tools, such as intrusion detection, virus scanners, firewalls, and encryption, as well as administrative tools, such as the application of security zones, security management systems, access control, (i.e. passwords and biometric identification).

Four categories of possible cyber attacks have to be considered:

(a) Unauthorized access to information (loss of confidentiality);
(b) Interception and change of information, software, hardware (loss of integrity);
(c) Blocking data transmission lines and/or shutting down systems (loss of availability);
(d) Unauthorized intrusion in data communication systems or in computers (loss of reliability).

The possibility of these events occurring increases as digital data flowing in and out of main control rooms are used by other IT systems, such as production and corporate networks, engineering workstations for maintenance management and monitoring activities.

4.2.5. System failure analysis

4.2.5.1. Failure modes and effects analysis

Failure modes and effects analysis (FMEA) is a systematic methodology to evaluate a system (hardware, software or process) for possible ways in which failures (or risks) can occur [20–21]. For each of the failures identified, an estimate is made of its occurrence, severity, and detection. An evaluation is made of the necessary action to be taken or ignored. The emphasis is to minimize the probability of the failure or to minimize the effect of failure.

A FMEA programme should start when a new design or an upgrade is initiated. It is recommended that FMEA must begin as early as possible even though all the facts and information are not yet known. After the FMEA begins, it becomes a living document and a dynamic tool of improvement, regardless of the beginning phase, it will use information to improve the system or design. It is continually updated as often as necessary.

FMEA is one of most important early preventive actions in design. This early warning and preventive technique provides the designer with a methodical way of studying the causes and effects of failures before the design is finalized. The FMEA provides a systematic method of examining all the ways in which a failure can occur, and will identify corrective actions required to prevent failures. Therefore a good FMEA will:

- Identify known and potential failure modes;
- Identify the causes and effects of the each failure mode;
- Rank the identified failure modes according to risk priority number;
- Provide for problem follow-up and corrective action.

FMEA can be applied to improve reliability of digital protection and control systems of the digital upgrade or new digital I&C design [26], for the analysis of operational system software [27], or for the safety assessment of a new digital safety system [28]. Software FMEA has been applied for software safety analysis for safety software in the digital protection system [29].

FMEA is applicable at various levels of system decomposition from the highest level of block diagram down to the functions of discrete components or software components. FMEA is applicable to all levels of system design, but most appropriate for lower levels where large numbers of items are involved and functional complexity exists.

The FMEA is a team function; therefore the makeup of the team must be cross-functional and multi-disciplined for each FMEA.

Different types of FMEA exist based on the system life cycle. For I&C system designs, ‘System (or concept) FMEA’ and ‘Design FMEA’ can be considered. System FMEA is used to analyze systems and subsystem in the early concept and design stage. A System FMEA focuses on potential failure modes between functions of the system caused by system deficiencies. Design FMEA is used to analyze products before the designs are released to manufacturing. A design FMEA focuses on failure modes caused by design deficiencies.

4.2.5.2. Other considerations for FMEA

Where FMEA is applied to a system incorporating features designed to prevent or mitigate human errors, the failure modes of such features need to be evaluated with consideration of a reasonable range of human error modes.

When FMEA is performed on the hardware design of a system that has hardware and software, the FMEA may have repercussions on the software in the system. The findings of the FMEA may be dependent upon the software elements and their nature. When this is the case, the interrelationships between hardware and software need to be clearly documented because any subsequent software revision may require repetition of the FMEA assessment.

4.2.5.3. Potential benefits of FMEA

FMEA provides the following potential benefits:

- Provides rigour in identifying single failures and their consequences;
- Facilitates design to avoid or mitigate failure modes which have unacceptable or significant effects;
- Helps avoid costly modifications by early identification of design deficiencies or critical failures;
- Provides criteria to compare design alternatives;
- Provides means to assess/verify robustness of design and ability to meet reliability criteria, and thereby provides an input to assignment of appropriate quality assurance level;
- Provides a logical model for evaluation of the probability of anomalous operating conditions of the system;

— Provides input to other types of system failure analysis and the preventive maintenance strategy and schedule for the system;

— Facilitate or support the determination of test criteria, test plan and diagnostic procedures.

4.2.5.4. Limitations of FMEA

FMEA is very efficient when it is applied to the analysis of elements that cause a failure of the entire system or of a major function of the system. However, FMEA may be difficult and tedious for the case of very complex systems [21]. This is because of the large quantity of detailed system information that needs to be considered. If maintenance and operational issues are included, analysis difficulty will be increased.

Some component failure modes of the system that is under study may be unknown and systematic (e.g. software) failure may not be included.

Errors in the analysis can occur when FMEA attempts to span several levels in hierarchical structure if the system design has redundancy.

Any relationships between individual or groups/causes of failure modes cannot be effectively presented in FMEA, such cases as hardware/software interaction and human interactions are involved, since the main assumption of such analysis is independency of failure mode.

Systems are examined one part at a time. FMEA does not provide a measure of overall system reliability. Also the ability of FMEA to fully analyze CCF is quite limited.

4.2.5.5. Related tools

FMEA is a useful design tool. However, it should be supplemented by other methods or tools, if required. This is particularly in the case when problems need to be identified and solutions need to be found in situations where multiple failures or sequential effects need to be studied.

Failure mode analysis (FMA) is a systematic approach to quantify the failure modes, failure rate, and root causes of known failures. Usually the FMA is based on historical information. In this sense, the FMA is a diagnostic tool because it concerns itself with only known failures. Because of the ability to utilize historical data and known failures, the FMA is used primary on current system as opposed to the FMEA that is used on new design or upgrade design.

Functional flow diagram (FFD) is a high level block diagram that illustrates the physical or functional relationships as well as interfaces within a system or sub-system under analysis. The block diagrams used in FMEA are for identifying the relationships between system level major functions and sub-functions, or logical flow and interrelationships of individual functions.

Failure modes, effects and criticality analysis (FMECA) is a systematic approach to analyze the failure modes and effects from a criticality perspective [22–23]. The aim of FMECA is to rank the criticality of components that may result in unsafe failure through single-point failures, in order to determine which components are critical to safety and identify any measures needed to strengthen the safety of the design.

Failure modes, effects and diagnostic analysis (FMEDA)

A failure modes, effects and diagnostic analysis (FMEDA) [24–25] is an extension of traditional FMEA/FMECA to include quantitative failure rate data and assess capability for on-line diagnosis and alarming or mitigation of failures. While FMEA is a structured qualitative analysis method, FMEDA is a systematic quantitative analysis method.

FMEDA is crucial to achieving and maintaining reliability in complex systems and systems that may not be fully exercising all functionality under normal circumstances, such as a low demand emergency shutdown system.

FMEDA analyzes failure modes at a component level, determines which failures lead to a safe condition and which lead to a dangerous condition, identifies which dangerous failures will be diagnosed, causing the device to be forced to a safe condition. FMEDA provides detailed failure rate data and safe failure fraction (SFF), the fraction of all failure modes that lead to a safe state of the system, either directly or via failure detection and mitigation. Such data is needed for safety integrity level (SIL) qualification.

Software safety impact assessment (SSIA) is a technique for assessing the impact of functional failure of software modules on the capability of the system to perform its safety functions.

The technique classifies software module failures as *safety direct*, meaning software functional failure may degrade the performance of one or more system safety functions; *safety indirect*, meaning software functional failure may degrade the performance of one or more safety functions only if it occurs with a second software functional failure or a hardware failure; or *non-interfering*, meaning that no functional failure, in combination with any second failure, may degrade any system safety function, or lead to another failure.

Fault tree analysis (FTA) is a system failure analysis technique that identifies all possible combinations of component failure events that can result in the occurrence of the top-level system failure event. FTA results in a logical model that is readily presented graphically. The tree shows the logical branches from the system failure at the top of the tree to root-cause basic failure events at the bottom of the tree. The logical model facilitates calculation of the probability of the top event, given failure rate data for the basic failure events. Software is available to automate the entry of the logical model and the above calculation. The availability of an FMEA facilitates performing FTA.

4.2.5.6. Hazard and operability study

4.2.5.6.1. Overview

Hazard and operability (HAZOP) is a structured and systematic technique for examining a defined system/design to identify potential hazards in the system/design, and to identify potential operability problems with the system/design. The information developed is also of benefit in determining appropriate remedial measures.

HAZOP identifies deviations from the system intent utilizing a core set of guidewords. IEC 61882; Hazard and Operability (HAZOP) studies-Application guide [47], provides a guide for HAZOP studies of systems utilizing the specific set of guide words defined in the standard.

HAZOP studies can be used during the design phase of a new system, a facility upgrade, as well as periodically during the operation phase.

4.2.5.6.2. Relation to FMEA

Failure mode and effects analysis is a component-centred approach while HAZOP is a system-centred approach. FMEA starts with a component failure, and investigates the consequences of the failure on the system. HAZOP starts with identification of possible deviations from the design intent, and then finds the potential causes of the deviation and measures to reduce consequences. FMEA develops information useful in performing a HAZOP analysis, but HAZOP results do not facilitate FMEA.

4.2.5.6.3. HAZOP limitations

HAZOP analysis is subject to the following limitations:

- HAZOP does not reveal possible interactions between hazards as it examines them one at a time;
- The success of a HAZOP study depends greatly on the ability, knowledge and experience of the study leader and team members;
- HAZOP only considers parts that appear on the design representation. Activities and operations that do not appear on the representation of the design are not considered.

The study of a complex system should not depend entirely upon a HAZOP study since there is no guarantee that all hazards will be identified because of the above limitations. Therefore, other relevant studies should be coordinated.

4.2.5.6.4. Software HAZOP

A software HAZOP is a hazard and operability study of software functions based on a detailed review of software functionality in terms of postulated functional failure modes. For each software failure mode, the effect on the system is assessed using static analysis methods. The software HAZOP complements and verifies the results of SSIA assessment, particularly key assumptions regarding failure modes and the isolation or inter-dependence of software modules.

The software HAZOP should be done with the software developers, both to make the process efficient and to improve understanding by the development team of any issues and required modifications that may result from the analysis.

HAZOP analysis proceeds on the basis of guide words that are used to guide a systematic assessment of each software module.

IEEE 7-4.3.2-2003 [14] Annex D provides guidance. Part 7, Section C.6.2 of IEC 61508 [52] provides additional references for 'Software HAZOP' or 'Computer HAZOP' methods.

4.2.5.7. Common cause failures

4.2.5.7.1. Significance of common cause failure

Common cause failure is a dependent failure that is the result of one or more events (or causes or stresses) that cause coincident (or within a short time interval) failures of two or more distinct channels in a multiple channel system, leading to the system failure [30–31]. The common cause can be heat, humidity, chemical corrosion, shock, vibration, electrical surge, electrostatic discharge, radio interference, unexpected sequence of events and human errors.

An example of CCF is when all of the pumps for a fire sprinkler system are located in one room. If the room becomes too hot for the pumps to operate, they will all fail at essentially the same time, due to the heat in the room. A high temperature can fail the three redundant processors in a safety system. An electrical surge can fail redundant input/output (I/O) modules.

The terminology on CCF has changed over the years. Common mode failures only were considered in failure analysis. Later, the definition of CCF was introduced referring to a slightly wider group of failures superseding common mode failures. The term 'dependent failures' was introduced to supersede and encompass common cause, common mode failures and cascade failures. Cascade includes all dependent failures that are not common cause failures. Common mode failures are a subset of common cause failures, whilst dependent failures encompass both common cause and cascade failures [31].

Common cause failures are real and a high common cause failure rate can effectively reduce or even negate the benefits of redundancy. This common cause failure has significant impacts on system reliability and safety [32].

The significance of CCF is that a single cause defeats the redundancy employed to improve the reliability of safety functions, and NPP operating experience has shown that CCFs are contributors to plant risk and economic consequences [31].

4.2.5.7.2. CCF analysis for I&C systems design

Safety-related I&C systems should be carefully designed and configured to reduce the possibility of CCF so as to reduce the risk of a CCF that disables multiple trains or systems.

CCF is a major contributor to risk and a critical factor for digital I&C system in NPPs [33]. Risk analysis can provide valuable information to reduce CCF. Therefore, close cooperation between I&C designer and risk analyst is needed.

CCF analysis methods

With collected event data, CCF models, such as, β-factor (BF) model, multiple greek letters (MGL) model, α-factor (AF) model, basic parameter (BP) model and binominal failure rate (BFR) model have been used to analyse CCFs within PSA tasks. The CCF models using simulation data are evaluated and compared in NUREG/CR-5044 [34].

CCFs are rare events and individual power plants present limited experience. There is a significant variability among plants due to differences in coupling mechanisms and defences. Therefore careful review and screening of event data with the plant design and the PSA models is required for CCF analysis.

CCF data collection and analysis

There are several international efforts to collect and make available CCF data. Under the OECD/NEA International Common cause Data Exchange (ICDE) Project [35] CCF data is systematically collected and analysed in several countries. The ICDE project overcomes previous difficulties in integrating CCF data collected in different countries due to inconsistent criteria and methods. Eleven countries are participating in this project. Reports and data analysis are available for components, such as, pumps, diesel generators, motor-operated valves, batteries, etc.

A CCF database and analysis are available from US NRC to aid system reliability and risk-informed application. The US NRC has produced several reports on CCF issues [36]. For example, CCF data Collection, Classification and Coding in the NUREG/CR-6268 [39]. This report presents an overview of CCF analysis methods for use in the US commercial nuclear power industry and summarizes how data is gathered, evaluated, and coded into the CCF system, and describes the process for using the data to estimate probabilistic risk assessment common cause failure parameters. CCF information of the safety-related performance of the reactor protection system and circuit breaker at US commercial reactors are presented [40–41].

For the analysis of CCF, a comprehensive review should include identification of the root causes, coupling factors, and defenses in place against them.

If failure data of a system is not available for CCF analysis, the load-strength interference model for data mapping and prediction of CCF probability [37] or a stress-strength failure model to simulate failures could be used [38].

4.2.5.7.3. Software common cause failure

When multiple components use software to provide similar functionality, there is a danger that design diversity may be compromised. AECB (currently Canadian Nuclear Safety Commission: CNSC) draft regulatory guide [42] and USNRC position [43] address the possibility of common caused software failure and require taking steps to reduce that possibility. Design diversity and functional diversity are recommended to protect against software common cause failures. It is also recommended to use different hardware and different real-time operating systems instead of relying solely on different programming languages, different design approaches meeting the same functional requirements or different design teams.

The USNRC emphasizes that quality is one of the key defences against software CCF [44]. While the specific probability of failure due to a software design flaw cannot be determined on a quantitative basis, there are established methods for software development and qualification that, when followed, provide reasonable assurance that the likelihood of failure due to software is sufficiently low. Engineering evaluations (e.g. likelihood of failure due to software, and risk of software CCF) of the quality and design process determines if there is reasonable assurance that the likelihood of failure due to software is sufficiently low. In the evaluation, 'sufficiently low' means much lower than the likelihood of single failures and comparable to other common caused failures that are not considered in the updated FSAR (updated Final Safety Analysis Report) (e.g. design flaws, maintenance errors, calibration errors) for the digital upgrade. If there is reasonable assurance that the likelihood of failure due to software is sufficiently low, then the upgrade would not require license agency's review on the basis of software common cause failure.

4.2.5.7.4. Recommended design approaches to minimize CCF

Diversity design

Diversity is a concept in which different units are used together in a redundant configuration. Channel, component and engineering diversities can be used for diversity design. The use of different components using different technologies from different manufacturers can increase common cause strength if the design responds differently to a common cause. However, design diversity does not eliminate all common cause failures [45].

Method for performing Diversity and Defence-in-depth Analysis of Reactor Protection Systems NUREG/CR-6303 [46] identifies 6 diversity strategies for digital I&C systems at NPPs. The six diversity strategies are design, equipment, functional, human, signal and software diversities.

Diversity of computers may be achieved through the use of separate computer functional specifications, computer hardware, computer languages, etc. to minimize the possibility of CCFs [14].

Defence-in-depth design

NUREG/CR-6303 [46] and NUREG-0800 [48] provide guides for the defence-in-depth design. These guides describe an acceptable process for performing a diversity and defence-in-depth analysis to demonstrate that vulnerabilities to CCFs are adequately addressed. From this analysis, if a safety function is subject to a CCF, backup systems or any means necessary for accomplishing the required safety functions should be identified. Manual operator action may be credited for responding to events in which the protective action subject to a CCF is not required for at least the first 30 minutes and the plant response is bounded in acceptance criteria.

A loss of capability in redundant components caused by a digital system CCF (H/W and/or S/W CCF) is considered the result of a design deficiency, manufacturing error, maintenance error, or an operator error. Since digital system CCFs are not classified as single failures by IEEE STD 379-2000 [50] postulated digital system CCFs is a single failure in design basis evaluations. Therefore, digital system CCFs as single failure in design basis evaluation analysis is not required for digital safety system design. Best estimated techniques can be employed in performing analysis to evaluate the effect of digital system CCFs coincident with design basis events [49].

Redundancy with isolation

If redundancy of a system increases, system downtime will be decreased. However, it is recommended to reduce the probability of common stress on the redundant systems to reduce CCF rate.

A way to reduce the CCF rate is to reduce the chance of redundant systems/units being exposed to the same cause/stress. When redundant units are physically separated/isolated, there is less coupling between systems/units and less likelihood of a common stress. Programmable electronic systems that have redundant equipment physically separated will be less susceptible to environmental common cause failures simply because the common environment has been reduced.

Robust design

Higher strength (robust) designs with lower failure rates will have lower CCF rates [51]. A device of greater strength can survive a larger stress. Stressors can be electrical (voltages, surge/currents, electromagnetic fields, etc.), mechanical (shock, vibration), physical (temperature, humidity), chemical (corrosive atmosphere) or human (abuse, operational errors, maintenance errors).

Diagnostic test

Digital I&C system with redundant channels can carry out diagnostic testing functions during on-line operation [52–53]. The channels can have a high diagnostic coverage within the channels, monitor other redundancy channels, have a high repetition test rate, and monitor sensors and/or actuators.

A large fraction of CCFs do not occur concurrently in all of the affected channels. Therefore, if the diagnostic tests are performed with sufficient high repetition rate, a large fraction of CCFs can be revealed and, hence, avoided before they affect all available channels.

Not all features of a redundant system will be affected by diagnostic tests. However, diagnostic tests can make the diversity or independence more effective.

The diagnostic tests are not required as the same level of quality assurance as the main control or protection functions of the system. However, the diagnostic tests should have an appropriate integrity commensurate with the target safety integrity level.

4.2.6. Use of commercial off-the-shelf products

Procured commercial off-the-shelf (COTS) digital I&C equipment can offer reliable and cost effective alternatives to custom-designed or nuclear-grade products. To use a digital COTS I&C equipment for a nuclear application, a qualification process (or dedication process) must be performed to demonstrate the COTS product is suitable for the application, adequate product documentation for safety and evidence of correctness of the product design are available.

Approaches to the qualification of pre-existing digital COTS equipment for use in nuclear safety applications vary somewhat in each country. A common approach has been based primarily on the assessment of the product design (i.e. a design review) and the process by which it was developed (i.e. a development QA audit). This has typically been done against appropriate reference standards and guidelines.

4.2.6.1. Dedication of commercial grade item

The US Nuclear Regulatory Commission (NRC) regulations under 10 CFR Part 50, Appendix B [54], Quality Assurance Programme, define two types of components: 'Basic component' and 'Commercial grade item'.

A basic component means a structure, system, or component thereof that affects its safety functions necessary to assure:

- The integrity of the reactor coolant pressure boundary;
- The capability to shut down the reactor and maintain it in a safe shutdown state; or
- The capability to prevent or mitigate the consequences of accidents, which could result in potential offsite exposures.

A commercial grade item means a structure, system, or component thereof that affects its safety functions, which was not designed and manufactured as a basic component. In addition to that, a commercial grade item is:

- Not subject to design or specification requirements that are unique to those facilities or activities;
- Used in applications other than those facilities or activities;
- To be ordered from the manufacturer/supplier on the basis of specifications set forth in the manufacturer's published product description (for example, a catalogue).

Commercial grade item and COTS item are synonymous terms.

Many equipment manufacturers either disappeared from the market or abandoned their product lines that were designed and manufactured under the 10 CFR Part 50 Appendix B quality assurance programme. The operating NPPs faced a problem related to the availability of qualified equipment, components and spare parts.

The NRC has defined the special process of 'Dedication of CGI (commercial grade items)' to provide reasonable assurance that a commercial grade item will perform its intended safety related function when required (when installed in its intended environment, which must be carefully specified) and is therefore essentially equivalent to a basic component. The dedication of CGI has been widely used mostly for relatively simple electrical and I&C components and spare parts. However, difficulties persisted in upgrading or modifying safety related digital I&C systems of NPPs due to uncertainty regarding licensing and a lack of guidance for digital upgrade and lack of guidance for performing the qualification of CGI.

To resolve these difficulties and harmonize regulatory requirements, the Electrical Power Research Institute (EPRI) set up the following working groups:

- Use of Commercial Grade Digital Equipment in Nuclear Safety Applications;
- Programme to Pre-License and Implementation Programmable Logic Controllers in Nuclear Application.

The above EPRI working groups have produced the following documents, which have been accepted by the NRC:

— Guideline on licensing digital upgrade, EPRI TR-102348 [57];

— Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, EPRI TR-106439 [55].

Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, EPRI TR-107330 [56] was also released for qualification of a COTS PLC.

In summary, in the USA, the COTS product qualification process is based on a combination of US NRC requirements for commercial grade item dedication, and design and licensing requirements for digital systems. EPRI guidelines on evaluation and acceptance of commercial grade digital equipment are available.

Krško NPP (NEK), in Slovenia, has an experience of dedication of a digital controller for the chillers [58]. NEK reviewed the generic process for evaluation and acceptance of CGI and used a dedication method for programmable digital system in safety applications. NEK recommends preparing a dedication plan especially when performing the dedication of an equipment system that contains several complex components. The acceptance process method used by NEK for the dedication of a programmable digital system was a combination of ‘Special Tests and Inspections’, ‘Commercial Grade Survey of Supplier’ and ‘Acceptable Supplier/Item Performance Record’.

4.2.6.2. Qualification of commercial off-the-shelf products

In Canada, the requirements for nuclear quality assurance are defined by the Canadian Standards Association (CSA) nuclear (N-series) standards and the regulatory guides and standards of the Canadian Nuclear Safety Commission (CNSC). No specific guides or standards exist at present addressing product qualification of programmable electronic sSystem (PES) equipment, only general requirements that appropriate industry standards be applied. The standard CSA N-290.14 [60] issued in 2007 addresses the software aspects of Application Specific product qualification; however, it addresses requirements on the process for qualification rather than technical evaluation and acceptance criteria. It also does not address programmed hardware logic devices (e.g. field programmable gate arrays) and non-software related issues.

Over the past several years, new international nuclear I&C standards have emerged to address the functional safety of nuclear I&C systems. In particular, the International Electrotechnical Commission (IEC) has issued IEC 61513 [61], IEC 62138 [62], and updates of other I&C related standards. Collectively this family of standards provides comprehensive guidance and specific requirements for the design of safety-related I&C systems using the fundamental principle of graded requirements based on the safety significance of the functions being performed. Atomic Energy of Canada Limited (AECL) has received feedback from the regulator (CNSC), and customers alike, indicating a desire for new (and in some cases the upgrade or replacement of existing) plant safety-related I&C system designs to meet these new standards. This includes an expectation that any COTS PES equipment important to safety be qualified to the IEC standards.

In the above, the term ‘programmable electronic system’ (PES) is used to refer to any system based on computer technology, which may be comprised of hardware, software, and of input and/or output units. Examples of PES include microprocessors; micro-controllers; programmable (logic) controllers; smart sensors, transmitters and actuators; application specific integrated circuits (ASICs), and field programmable gate arrays (FPGAs). PES software may be either end user configurable or pre-configured at the factory.

PES products and components are increasingly being used in plant process equipment and components. PES are also found in control, safety, monitoring and test systems. PES technology is being used because of its cost effectiveness, reliability, and configurability. While the benefits of PES technology are significant and worthwhile, the problem of confirming that a PES can be used safely and demonstrating that it will meet the requirements of a specific application is often challenging. This confirmation process is known as application-specific product qualification (ASPQ).

PES components are finding their way into most plant I&C and process equipment. Although generally of high reliability, PES components are complex devices and are susceptible to random hardware failures, systematic design faults, and common mode failure. In addition to the vulnerabilities of software (e.g. the possibility of latent faults), most PES hardware is based on low voltage electronics, that if not considered in design, may be susceptible to electromagnetic interference (due to radiated radio-frequency electromagnetic field, magnetic field, electrostatic discharge, electrical surge, fast transient/burst and other disturbances). PES components are also often susceptible to human error and environmental conditions (e.g. temperature, vibration, humidity, dust, radiation etc.). Thus, in applications where failure of a PES may directly or indirectly affect the safety function(s) of the equipment or system of which it forms a part, consideration of the above failure modes becomes a concern.

ASPQ has become increasingly important as an enabling process to permit the licensing of economic digital upgrades or new plants using pre-existing ‘off-the-shelf’ commercial PES products and equipment. ASPQ is a means of evaluating and accepting PES products or components developed outside of a nuclear QA programme and is intended to address the concerns and risks associated with using the technology in a nuclear safety-related application. Provided these concerns and risks are appropriately addressed, PES technology has been shown to improve overall system reliability and safety of plant systems.

ASPQ can be challenging and difficult due to the range of issues that need to be addressed, the wide range of expertise required, the willingness of the manufacturer to provide extensive product information, the availability of evidence and the need to consider context specific requirements and the safety significance of the functions performed.

An ASPQ methodology that has been developed at AECL (Annex II and [59]) and successfully applied to qualify PES equipment intended for use in domestic CANDU® 6 and Advanced CANDU® Reactor (ACR-1000®) power plants and special purpose reactors at the Chalk River Laboratories.

4.2.7. Design for maintainability of the new system

The strategy of modernization step by step, application by application, system by system, can potentially generate a significant number of different types of HSI in control room, and also different technologies, which have to be maintained.

The systems of the past were often closed and inflexible software systems and therefore cause problems when new systems were integrated. Based on these experiences, open systems should be considered in the nuclear domain.

Consequently, it is important to make sure that a solution of modernization provides not only a short term problem solving to a problem but also flexibility, in the future, to be able to integrate other technology/solution while maintaining the existing development and maintenance method.

4.2.7.1. Open software solutions

An open software system is characterized by having a context independent interface that allows many different kinds of applications to interact with it. The bottom line is that open software system is a prerequisite for having system flexibility. Flexibility goes along different dimensions such as:

- Features for both exporting and importing information from the individual software system module, making use of the imported information in the software system to the extent this is appropriate or desirable;
- Features for configuration of the system module so that it can be used as part of many different work processes. This usually entails the configuration of the interface of the module, or the integration of the interface into the interface of other modules. It may also entail the configuration of different modes of the software module depending on certain contextual conditions.

It is important to note that an open system does not necessarily assume commercial operating systems or that the system itself is implemented as a commercially available system. Open systems are only qualified by the fact that they adhere to standardized encoding of the information that is sent to or received from the module.

It is also a quite common misconception that open systems preclude the existence of needed security mechanisms for protecting the system in question.

IAEA-TECDOC-1252 [15] (Section 4) sketches a general approach for establishing a sufficiently open, distributed and flexible system structure.

- Each I&C system should be able to communicate effectively with other internal and external systems;
- Safety systems and information should be isolated so that they cannot be corrupted by other systems or information modules;

- Access control should be implemented so as to assert data security;
- The HSI of each modernized I&C system should be consistent in the look and feel with the other modernized systems;
- Future migration to new hardware or technologies should be achieved without excessive downtime or a major conversion effort;
- Each modernized I&C system should be able to take advantage of additional functionality available with newer technologies and should also integrate smoothly with older systems in the plant;
- The migration to the new architecture might be scheduled in phases that are coordinated with other plant events such as plant outages.

Openness is a necessary condition for asserting flexibility in the future control room solution. Due to safety requirement it is possibly impossible to avoid introducing hybrid control room when digital technology is being taken into use.

Due to severe qualification requirements, safety classified systems (e.g. class 1E) must be kept as simple as possible. In order to implement the qualification requirement it might be impossible to use general purpose computer technology (for all foreseeable future). Still, as is the case today, the safety classified parts of I&C systems should be interfaced to the non-classified systems. For this purpose, standardized information exchange formats should be applied.

One example is the recent development of software solutions that assist in the implementation of administrative functions. State of the art systems are commercially available and are being used in the management of the plan, e.g. maintaining parts of the plant documentation, to manage the inventory and to plan outages. As a further example, engineering data management systems have been taken into use that help to manage documents; such as letters, reports, specifications, CAD-drawings, invoices, sales orders, photographs, phone interviews, video news clips, etc.

Still the MCR systems are not appropriately integrated with these systems even though they are, in parts, related to the same information. This might (at least in parts) be explained by the fact that the MCR application does not conform to the standards that some of the administrative systems are already using.

Another important paradigm shift that is currently taking place worldwide is the application of web technology. Many other industries (such as the oil industry) already apply this technology in many of their projects. The obvious reason for this is the expectation that much of the software development that will take place will be based on these standards. It is an open question what would be the consequences if the nuclear should disregard this trend.

The inability to share common information among systems entails the embedding of duplicated information in one or several systems. Obviously this leads to huge maintainability problems during the life cycle of the MCR and the plant.

One problem with hybrid solutions is that it is harder to ascertain openness and flexibility due to the added complexity in integrating the individual systems — it may even be impossible to obtain full flexibility and openness because of certain legacy systems. Added complexity might entail at least the following conditions:

- Training of operators as well as other technical personnel is more comprehensive. Qualification of systems will be more complex;
- Possibilities for errors both in operation and maintenance are increased;
- Possibilities that information must be duplicated.

If stepwise migration is applied in less than optimal solutions, it might be tolerated as a temporary solution. However these solutions might include non-consistent user interfaces that must be checked that they do not induce intolerable risks in given situations.

Due to the underlying dichotomy between operational and administrative plant systems, one seems to have, in certain cases, possibly for most plants, a more or less permanent hybrid condition (looking at the total amount of plant applications). This situation will persist until either a solution is found that solves the problem of qualifying the new type of technology or some kind of interfacing layer may be qualified (thus removing most of the problems of hybrid solutions).

Most of the safety related systems of the MCR do not have interface-flexibility that modern information systems have today. This will unavoidably lead to the situation where most MCRs of the future will be hybrid. However the recommendations to the utilities are to have a well-considered management to minimize this effect and try to use open standards for the information exchange between safety and non-safety classified systems. For all non-classified systems, mainstream standards and system solutions should be considered. This creates the best possibilities for asserting system flexibility in the future.

4.2.8. Methods and tools

There can be many methods and tools for the development, conduct of the validation activities and configuration management. The use of tools can increase the integrity of the development process for modernization, and hence reliability, by reducing the risk of introducing faults. The use of tools can also have economic benefits as they can reduce the time and effort required in the design process. Tools are either written or computerized. Their purpose is to facilitate the specification, analysis, design, development, and V&V of a system. When systems are designed, different types of tools are used. There are many different ways to collect data. Some ways are relatively easy to use; others are more difficult and costly. These methods are often used together.

Interviews may be used alone or in combination with other methods and techniques to obtain information from users. Interviews can be conducted in support of design activities, such as interviewing operators to determine desired improvements in the control room, or evaluation activities, such as conducting debriefings following the use of new HSIs. Interviews are one of the best methods to get user comments and opinions and to determine the root causes of difficulties and problems they encounter and how they can be improved.

A questionnaire is a method which can be used to collect a lot of information can inexpensively.

Observation involves users carrying out tasks in their actual work environment, such as the control room, mock-up or training simulator. The HFE analyst observes user activity as unobtrusively as possible and records information by taking notes or using checklists of expected user actions. If it is possible, videotaping is helpful and can make data collection more reliable since it provides an opportunity to replay the tape to observe behavior that was either missed the first time or to conduct a more detailed analysis of any specific problems.

In a walk-through, users perform selected activities and provide information to the HFE analyst either in response to questions from the analyst or as a narrative of their thoughts as they carry out their actions. When users verbalize what they are thinking as they performing the task or interact with the HSIs, they may reveal the strategies they use, the resources they require from the interface, and their expectations about how the resources will be made available. It will also draw attention to points in the interaction where the design of the interface does not complement the user’s goals.

There are also many tools for the HFE verification and validation of HSIs, such as static-mock-ups, prototypes, part-task simulators, full-scope simulators, and virtual reality simulators. These tools are categorized in the degree of HSI completeness, HSI physical fidelity, HSI functional fidelity, system model fidelity and timing and dynamics fidelity. Some of the tools are more important for the integration of information than others. Figure 10 shows a simple example tool to easily and effectively perform the task analysis. In addition, an equally valuable role of the real time part-task or full-scope simulator is in validation of the control logic and strategies programmed into these digital control systems under the HSI. Experience has shown that while human factor testing by employing simulators is key to project success, the validation of the new control system on the real time simulator will, by itself, justify the cost of all upgrades to the simulator and the time spent on testing. The value comes from reducing the programming errors in the control logic. Errors indentified by simulator-based tests can reduce the initial startup and can avoid potentially dangerous scenarios during abnormal plant operation.

To allow uniform processing as well as consistent data management throughout the various steps of the design, it is recommended to use different types of tools. The input information and source data for the tools used in the design process are, for example, the result of the different types of analyses performed in the early stages of the system life cycle, e.g. task analysis. Other sources of input data for the design tools are the results of the modeling. Tools are most efficient when they provide input for other tools used in later phases of the design process.

An example is when the engineering tools provide data in a format usable for the code-generating tool. It is also beneficial if the output from the task analysis and modeling is in such a format that it can be used directly by the engineering and software tools.

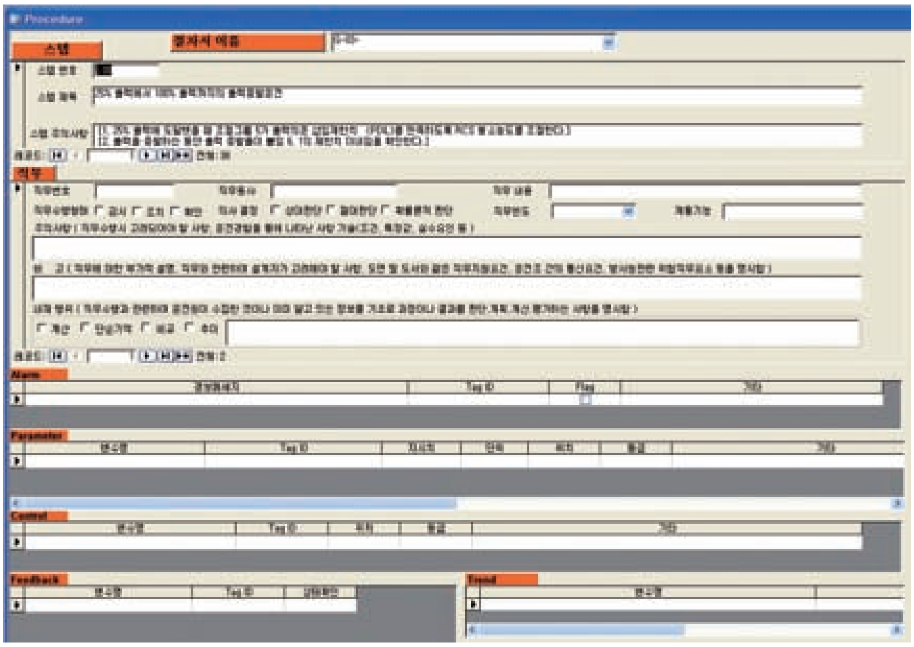


FIG. 10. Sample program for the task analysis.

The software tools should support all or parts of the following steps in the development and design of software:

- Programming;
- Code generation;
- Documentation of the generated code;
- Testing and analysis of the generated code;
- Maintenance of the code and its documentation;
- Translation of formalized specifications, e.g. into application software (translation to another level of abstraction).

Computer aided design (CAD) tools are used in the design of I&C systems. The CAD tools are used in order to support all aspects of the design of hardware (sensor installation, cabling, structure of boards in cabinets, etc.) and the interfaces between systems. Typical CAD tools are, for example, tools for drawing diagrams, tools for routing of cables, etc. It is beneficial if the CAD tools are able to interface to other tools used in the design process.

Computer aided system engineering (CASE) tools are very supportive of information integration. The main feature of CASE tools is their ability to keep track of practically all types of data describing the information system design, such as data items, database structures, data relations, data flows, processes, different attributes, comments, functions, etc.

The repository holding this information is unique for a project or a group of projects. This allows the CASE tool to organize cooperation between different project teams providing synergy effects. In order to benefit from the use of the CASE tool, it is necessary to implement it before modernization or new systems are implemented.

IEEE 7-4.3.2-1993 [14] identifies the need for abnormal conditions and events analysis (AECS) for software based systems. There are many techniques that can be used to support ACES analysis. One example is failure modes and effects analysis. It is used to identify as many as possible of the potential failures that can occur when a function is executed and the effects of this failure on the system. This methodology can be used in all phases of the development process. Tools exist to support failure modes and effects analysis in several phases of the project.

Various maintenance support systems are already in use at nuclear power plants worldwide. These provide support in scheduling maintenance activities and in maintaining spare parts. The integration of these tools with the plant information database provides additional opportunities for the modernization or new systems.

4.3. INSTALLATION

The MCR modernization project should be well planned based on the allowed budget and schedule. The design of the new MCR starts from the basic requirements of modification of the utility. The designer of the MCR modernization project should review the utility requirements precisely and finalize the design goals by coordinating with the utility, licensing organization, and system vendors to finalize the design plan and schedule. Normally the installation of equipment in the MCR will be scheduled around the plants operational schedule and planned outages. Completion of the work during the planned time is critical to the success of a modernization project. Three types of installation can be considered:

- Installation during plant operation;
- Installation of part of the system during power operation while the remaining work is done during plant outage;
- Installation during plant outage.

A risk management study can help management select the appropriate strategy. Special care should be taken when modifications are done during plant operation to avoid disturbances. Some disturbances can potentially lead to unplanned shutdowns, increasing the overall cost of the modernization. Proper identification of interfaces and affected safety system, wire routing and termination, power consumption of new equipment and the effect of the new equipment on existing systems are vital to the success of the modernization project.

4.3.1. Installation planning

Prior to the installation, the supplier has to develop an installation plan taking into account the existing environment (size of entrance door, equipment removal aisle, etc.) and plant operational mode (plant operation or outage). The installation and possible dismantling plan should include a detailed schedule of planned activities. It should also identify the required interface conditions of the remaining system to prevent inadvertent equipment operation. The planned activities have to be approved by the utility before the installation can proceed.

If the modification is done during plant outage, the installation plan must take into consideration outage activities. Certain activities may need to be closely coordinated with other outage activities to be carried out efficiently. Dismantling plan should carefully identify the interfaces between replaced and remaining equipments. Impact analysis on the remaining hardware should be carried out to mitigate potential problems. Early identification and mitigation of potential installation problems will reduce installation time during outages.

When modernizing the control room, a temporary control panel is required for continued plant operations. This temporary panel allows for the modernization project to proceed while ensuring that the plant can be safely operated. The utility should carefully review the required instruments and control devices for the temporary panel and provide the design information to the supplier for implementation. The utility may be able to reduce the number of the safety functions to be supervised from the temporary control panel. A change in the need of supervised safety function has to be approved by the licensing authorities. This can be done by analysis of the situation and writing a temporary safety specification for use during the modernization of the control room. It is also beneficial to add important service functions to the temporary control panel.

4.3.2. Installation execution

During the installation execution, it is important to constantly review and adjust activities to forecast potential delays. Interactions between the utility and the suppliers are important during this phase. Installation staff are managed by the supplier, who should interface directly with the utility representative to provide regular progress reports and contingency plans when necessary.

4.4. TESTING, VERIFICATION AND VALIDATION

Testing and evaluation of HSI designs should be conducted throughout the HSI development process and evaluations should be performed iteratively. Although the types of tests and evaluations performed will vary depending on the specific applicant's design process, the methodology used should be determined using the appropriate criteria. Aspects of human performance that are important to task performance should be carefully defined so that the differential effects of design options on human performance can be adequately considered in the evaluation of the HSI design. The following evaluation factors should be considered:

- Personnel task requirements;
- Human performance capabilities and limitations;
- HSI system performance requirements;
- Inspection and testing requirements;
- Maintenance requirements;
- Use of proven technology.

The development of simulators must be considered very early in the project as lead times, coordination of data collection, and simulator development are generally longer than expected. Also, service demands on the simulator beyond V&V, such as operating procedure development and subsequent training need to be factored into the schedule for availability of the simulator.

4.4.1. Factory acceptance test

The purpose of the factory acceptance test (FAT) is to assure that the HSI complies with all requirements as defined in the contract document prior to shipment to the plant. Completely assembled HSIs should be operationally and functionally tested at the supplier’s factory in the presence of the buyer’s representative. This test should demonstrate that the hardware and software perform the intended functions in accordance with the specification requirements. FAT is one of the most important phases of the project: it is the last chance to remedy any last minute problems in a context more favorable than on-site.

To ensure the quality and completeness of the tests, a test plan has to be established by the supplier and approved by the buyer prior to testing. This test plan should be prepared to identify and define the organizations, activities, resources, and planning processes deemed necessary. This plan must include a list of acceptance criteria to be prepared by the supplier according to the specification requirements of the individual components (hardware and software) including the qualification and licensing requirements if appropriate.

The project manager has to assure that the test plan demonstrates all of the required functions as defined in the contract. In order to reduce the test effort on-site, it is important to test all HSIs incorporating the full configuration data or on a representative subsystem. The test schedule must be issued in advance to allow the project team to witness these tests. The test reports should be signed by the buyer for acceptance of the HSIs prior to delivery at the plant.

4.4.2. Site acceptance test

The purpose of the site acceptance test (SAT) is to verify that all HSIs operate properly under the field environment and do not suffer damages during shipment. The SAT should be done without impact on the process (no connection to valves, pumps) and can be performed to complement the FAT (specific interfaces, etc). A list of acceptance criteria has to be prepared by the supplier, and approved by the buyer, according to the contract requirements taking into account the results of the FAT. The test shall include as a minimum the following:

- Verification of proper power supply at all test points considering a loss of power;
- Verification of all functions including displays, communication protocols and data transmission;
- Verification of proper interface, monitoring and control functions.

4.4.3. Commissioning test

The commissioning test concerns the functional tests of the system connected to the I&C system and the process. It includes final operational testing, and validation of long term performance of the HSIs. A sufficient period of time is needed for the commissioning test to validate the HSI performance from the devices in the MCR to field actuators.

4.4.4. Usage of the simulator

Verification and validation of the design using a simulator or a dynamic mock-up with the participation of the operators and/or licensing authority are important to ensure that the design is effective in supporting the performance of personnel tasks. Therefore the simulator or dynamic mock-up should be prepared before the V&V process. The simulator that is available on most plants will likely need to be updated to reflect the changes on HSIs. In the case of a multi-step project, the utility must be aware that the skills of the operator have to be demonstrating using the new HSIs while maintaining their proficiency with the current plant configuration. Management should be aware of four potential simulator upgrade paths for multi-step projects:

- Simultaneous migration to plant modernization configuration;
- Addition of simulator corresponding to modern configuration while maintaining previous simulator configuration;
- Dual mode simulator capable of switching between upgraded and existing functionality (difficult);
- New partial simulator for upgraded functionality only.

The modern design tools currently available, e.g. 3-D modeling tool with walk-through navigation, can also be utilized for V&V before finalizing the design.

4.5. HUMAN FACTORS ENGINEERING VERIFICATION AND VALIDATION

This section describes HFE V&V, which consists of the techniques that should be used to establish that the design of the HSI meets the requirements that have been placed on it and to ensure that the interface is effective in supporting the performance of personnel tasks. This includes establishing that the design supports the performance of tasks, adheres to accepted human factors practices, meets all operational requirements and that the final configuration and the design documents agree. HFE V&V activities should be well integrated into the overall design process. Prior to carrying out the V&V activities, the associated design activities should have been accomplished, a style guide or other criteria should be available, and the related function and task analysis steps should be completed.

HFE V&V requires demonstrating that:

- The interface meets all the requirements that have been placed on it. For example, that all required control capabilities and displayed quantities are, in fact, provided and that all parts of the interface are configured as intended and required by human factors guidelines and standardized practices. Such activities are referred to as verification activities;
- The interface will enable all the intended tasks to be carried out effectively. That is, the interface has to be proven to function as intended. The premise is that even though every individual requirement is met, the integrated functioning needs to be confirmed. This leads to testing of the entire system and interface to establish that it can provide all the functions and achieve the performance that is needed. Such activities are referred to as validation activities.

HFE V&V consists of a variety of activities, which will vary depending on the nature of the design change. The following factors would typically be documented in the HFE section of the project plan:

- Management. Establishing the responsibilities for managing the quality and scope of HFE V&V;
- Scope. Establishing the requirements and objectives of HFE V&V activities and the bases for the requirements;
- Participants. Identifying the personnel who will perform and participate in the HFE V&V activities (i.e. designers, HFE personnel, HFE experts, operators, etc.);
- Methods and procedures. Establishing how HFE V&V activities will be performed;
- Test conditions, data collection and analysis of results. Establishing the detailed plans and procedures to be applied, in what form results will be captured and how results will be applied;
- Acceptance criteria and performance measures. Defining the design and performance requirements that must be demonstrated according to the design specifications;
- Documentation, reporting and integrating the results. Establishing the level and status of documentation, the requirements for evaluating, communicating, and maintaining the results of HFE V&V activities and the processes for integrating the results of HFE V&V into the overall modification;
- Schedule. Establishing when HFE V&V activities will be performed and integrating HFE V&V into the overall modernization schedule;
- Tests and evaluations. Determining the less formal tests and evaluations to be performed as part of design activities that support HFE V&V.

The HFE V&V project plan should address the following human factors aspects of the design:

- Human-system interface (i.e. controls, displays, and alarms);
- Procedures (hard copy, static computer based, or automated computer based);
- Crew coordination and communication;
- Display navigation, information retrieval, and access to controls;
- Automation and the features of automation, including monitoring and control;
- Layout, configuration, and anthropometrics of workplaces and workstations and the features and equipment required for those spaces (e.g. laydown areas, access and egress, radios, phones, hard copies of procedures and drawings);
- Workplace environment (e.g. lighting, temperature, noise);
- Provisions for routine test and maintenance (e.g. cleaning displays, testing, routine consumable replacement).

In some cases, when certain features of the modification have already been verified and/or validated during previous modifications, credit can be taken for some of the previously performed verification activities (for example, a recorder replacement using same model of the device as was utilized in another, already completed modification). Thus, the scope of the V&V can be reduced. However, sufficient documented justification should be provided to support this approach.

Proper planning for HFE V&V activities includes the definition of the scope, schedule, location and required tools. V&V activities should be performed by a multidisciplinary team of qualified personnel. A sample of participants should be selected which represents the population of persons who will use or maintain the modified equipment. In selecting participants it is important to avoid bias and testing should be carried out using normal crew configurations as well as the minimum expected crew configuration.

HFE V&V consists of four major activities: (1) availability/suitability verification, (2) integrated system validation, (3) human engineering discrepancies resolution, and (4) final plant verification.

4.5.1. Availability verification

The objective of availability verification is to verify that the HSI inventory and characterization accurately describes all HSI displays, controls, and related equipment that are within the defined scope of the HSI design. The inventory should be based on the best available information sources such as equipment lists, design specifications, drawings, etc. Further, the accuracy of the inventory should be confirmed by directly observing the HSI components and comparing them to the documented description.

HSI inventory and characterization can be performed after the conceptual design is complete. It will undergo revision as the design evolves, but it needs to be completed before the HSI design itself is finalized to ensure that all

HSI components with the appropriate characteristics associated with personnel tasks are included in the final design. The inventory should provide an accurate and complete description of the HSI components. The following is a minimal set of information for the inventory:

- A unique identification code number or name;
- Associated plant system and subsystem;
- Associated personnel functions/subfunction;
- Type of HSI component:
  - Computer based control (e.g. touch screen or cursor-operated button and keyboard input);
  - Hardwired control (e.g. J-handle controller, button, and automatic controller);
  - Computer based display (e.g. digital value and analog representation);
  - Hardwired display (e.g. dial, gauge, and strip chart recorder).

In addition, the information for the components in the inventory should include characteristics such as:

- Display characteristics and functionality;
- Control characteristics and functionality;
- User-system interaction and dialog types;
- Location in data management system (e.g. location of display screen);
- Physical location.

4.5.2. Suitability verification

The objective of suitability verification is to verify that the characteristics of the HSI and the environment in which it is used conform to HFE guidelines. The selection of guidelines used in the suitability verification depends upon the characteristics of the HSI components. It also depends upon whether the project team has developed a style guide (design specific HFE guideline document). When a style guide is not available, the HFE guidelines contained in NUREG-0700 [9] may be used.

The characteristics of the HSI components should be compared with HFE guidelines. These guidelines are applicable to different aspects of the design: task independent features (e.g. font size), task specific features (e.g. scale, units) and task integration features (e.g. proximity of control display). A single guideline may apply to many identical HSI components, especially in the case of significant HSI modifications and HSIs for new plants. If there is any instance of noncompliance with the HFE guideline, it will be construed as a human engineering discrepancy (HED) that should be documented and resolved by the team.

In addition, the suitability verification also evaluates the various aspects of as-designed HSIs for usability in terms of expected tasks through a brief task scenario. The evaluators will seek to identify and document the HEDs by considering the plant operator's tasks. HEDs will be identified when HSI components and control capabilities needed for task performance are not available in the design or when unnecessary items distract the operator from their tasks.

4.5.3. Operational conditions sampling

The operational conditions for which V&V activities are conducted should:

- Include conditions that are representative of the range of events that could be encountered during operation of the plant;
- Reflect the characteristics that are expected to contribute to system performance variation;
- Consider the safety significance of HSI components.

These sample characteristics are best identified through the use of a multidimensional sampling strategy to provide reasonable assurance that variation along important dimensions is included in the V&V evaluations. The following plant conditions should, as a minimum, be included:

- Normal operational events including plant startup, plant shutdown or refueling and significant changes in operating power;
- Failure events including instrument failures;
- Transients and accidents;
- Consideration of the role of the equipment in achieving plant safety functions;
- All risk-important scenarios and accident sequences should be included in the sample, including those identified in the probabilistic risk assessment and those identified as risk-important in the safety analysis report;
- Operation experience review — identified difficult tasks — the sample should include all personnel tasks;
- Tasks identified as problematic during the applicant's review of operating experience.

The following factors should also be considered when defining operational conditions for the V&V process.

- The operational conditions should reflect only tasks that were affected by the modification;
- For integrated system validation, the operational conditions should address the transfer of learning effects on personnel performance when a modification replaces an old HSI or procedure, and if old and new versions of the same HSI components are to be used simultaneously, evaluations should provide reasonable assurance that personnel can proficiently use both;
- Where old HSI components are to be deactivated and left in place, conditions should be identified that would test the potential for task interference. For example, the presence of deactivated HSI components may cause visual clutter that interferes with the ability of operators to locate and use other HSI components.

4.5.4. Integrated system validation (ISV)

The integrated system validation (ISV) ensures that the HSI design can be effectively and safely operated and meet all performance requirements. The goal is to test the integration of personnel and plant systems and to validate the integration of the design with personnel actions, plant response, HSIs, procedures, etc. It is intended to evaluate the acceptability of those aspects of the design that cannot be determined through other means.

A variety of tools and methods can be used to validate the design. These include interviews, questionnaires, checklists, static and dynamic mock-ups, walk-through/talk-through, and full scope simulator. For major or complex modifications, the use of a high fidelity simulator that has sufficient flexibility to realistically change the test conditions is important for successful validation. For more minor modifications the applicability and scope of the ISV may vary.

ISV should be reviewed for all modifications that may (1) change personnel tasks; (2) change task demands, dynamics, complexity, or workload; or (3) interact with or affect HSIs and procedures. ISV may not be needed when a modification results in minor changes to personnel tasks which have little or no overall effect on workload and the likelihood of error.

ISV objectives

The ISV should address aspects of performance that are changed by the modernization, including personnel functions and tasks. The objectives of the ISV are to:

- Validate the role of plant personnel;
- Validate that the shift staffing, assignment of tasks to crew members and crew coordination is acceptable;
- Validate that for each human function, the design provides adequate alerting, information, control, and feedback capability for human functions to be performed under normal, transients, design-basis accidents, and risk-significant events;
- Validate those specific personnel tasks can be accomplished within time and performance criteria with a high degree of operating crew situation awareness, and with acceptable workload levels, that provide a balance between a minimum level of vigilance and operator burden. Validate that the operator interfaces minimize potential operator error and provide for error detection and recovery capability when errors occur;

- Validate that the crew can make effective transitions between the HSIs and procedures in the accomplishment of their tasks and that interface management tasks such as display configuration and navigation are not a distraction or undue burden;
- Validate that the integrated system performance is tolerant of failures of individual HSI features.

Performance measure selection

Performance measures should be used which includes measures of the performance of the plant and personnel (i.e. personnel tasks, situation awareness, cognitive workload and anthropometric/physiological factors). Some of these measures could be used as 'pass/fail' criteria for validation and the others to better understand personnel performance and to facilitate the analysis of performance errors. Typical performance measures are:

- Plant performance measurement. Plant performance measures representing functions, systems, components and HSI use should be obtained;
- Personnel task measurement. For each specific scenario, the tasks that personnel are required to perform should be identified and assessed;
- Situation awareness;
- Cognitive workload;
- Anthropometric and physiological factors. Anthropometric and physiological factors include such concerns as visibility of indications, accessibility of control devices, and ease of control device manipulation that should be measured where appropriate.

ISV procedures

Detailed, clear and objective procedures should be available to govern the conduct of the ISV. These procedures should include:

- The identification of which crews receive which scenarios and the order that the scenarios should be presented;
- Detailed and standardized instructions for briefing the participants. The type of instructions given to participants can affect their performance on a task. This source of bias can be minimized by developing standard instructions;
- Specific criteria for the conduct of specific scenarios, such as start and stop scenarios and when events, such as faults, are introduced;
- Scripted responses for test personnel who will be acting as plant personnel during test scenarios. To the greatest extent possible, responses to communications from operator participants to test personnel should be prepared. There are limits to the ability to pre-plan communications since personnel may ask questions that were not anticipated. However, efforts should be made to detail what information personnel outside the control room can provide and script the responses to likely questions;
- Guidance on when and how to interact with participants when simulator or testing difficulties occur;
- Instructions regarding when and how to collect and store data. These instructions should identify which data are to be recorded by:
  - Simulation computers;
  - Special purpose data collection devices (such as situation awareness data collection, workload measurement, or physiological measures);
  - Video recorders (locations and views);
  - Test personnel (such as observation checklists);
  - Subjective rating scales and questionnaires;
- Procedures for documentation; i.e. identifying and maintaining test record files including crew and scenario details, data collected, and test conductor logs.

Participant training

- Participant training should be of high fidelity; i.e. highly similar to that which plant personnel will receive in an actual plant. The participants should be trained to provide reasonable assurance that their knowledge of plant design, plant operations and use of the HSIs and procedures is representative of experienced plant personnel. Participants should not be trained specifically to perform the validation scenarios;
- Participants should be trained to near asymptotic performance (i.e. stable, not significantly changing from trial to trial) and tested prior to conducting actual validation trials. Performance criteria should be similar to that which will be applied to actual plant personnel.

4.5.5. Human engineering discrepancy (HED) identification and resolution

Discrepancies are identified in cases where the availability verification, suitability verification, or ISV, find that the design does not meet the established HFE performance requirements. HED resolution is an evaluation to provide reasonable assurance that the HEDs identified during the V&V activities have been resolved.

HEDs should be captured as part of an organization’s existing problem reporting or issue tracking system. HED identification includes the relevant HSI, task criterion, an explanation of the basis for the deficiency, and where possible, a recommendation for resolution. Some HEDs can be evaluated as acceptable. In those cases, justification for the acceptability of the discrepancy should be provided and the HED should be closed with concurrence of the HFE verifiers. After the designers have established a resolution for the discrepancy, the task or HSI component should be re-evaluated to ensure that it was adequately resolved.

HED resolution is an activity that can be performed iteratively with V&V. That is, the project team may integrate these activities so that issues identified during a V&V activity are addressed and resolved prior to conducting other V&V activities. After a solution to a design problem documented in an HED is developed and installed, the corrected design should be re-evaluated by repeating the appropriate V&V. It may not be necessary to repeat the entire V&V in its full original scope. However, the scope of the re-verification or re-validation should be sufficient to ensure that the problem was adequately addressed by the design change, no new deficiencies were created, and that the new design conforms to the HSI design requirements. Resolution of discrepancies should not be performed solely by the design organization; it should include concurrence and acceptance by personnel responsible for V&V. Where agreement cannot be reached between the designer and personnel performing the V&V, discrepancy resolution should be obtained with participation from the plant modification review committee.

HEDs should not considered in isolation and, to the extent possible, their potential interactions should be considered when developing and implementing solutions. For example, if the HSI for a single plant system is associated with many HEDs, then the set of design solutions should be coordinated to enhance overall performance and avoid incompatibilities between individual solutions.

4.5.6. Final plant verification (FPV)

The last HFE V&V activity to be performed is the final plant verification (FPV). The purpose of this activity is to confirm that the as-built design conforms to the verified and validated design that resulted from the design process. By completing the FPV, the design team declares that the new and/or modified HSI conforms to the design, has been tested, and is ready for operation. The FPV includes the completion of any V&V activities that could not be performed before installation, such as control room lighting, noise, in-plant communication, and plant specific features. FPV also includes a final check to ensure that all previously created HEDs identified during the V&V process have been acceptably addressed and resolved.

Designers should have high confidence that the design will pass the FPV prior to the start of this activity. In addition, all of the equipment needs to be installed at the plant before the final verification is initiated.

4.6. TRAINING

4.6.1. Training management

Training is an essential step in all kinds of control room changes. Obviously, this also pertains to changes in I&C. Such changes most often entail workflow changes or changes to work processes. The typical situation is that work steps and manual functions are eliminated and some automated systems are added. Thus training must be performed on at least two different levels:

- Training acquiring the skills for using and maintaining a new system;
- Instructions and training for adapting to the new working practices, environment, and culture as a result of introducing the new information technology.

Most guidelines recommend that training should be planned as part of the plant upgrade project. The following aspects should be elucidated or asserted as part of the training design activity:

- The training should be made part of the training/re-training policy of the plant;
- Plant management should support the training activity and monitor its actual execution. In addition, management should be active in assessing the quality of the training and possible improvements of the current training;
- Adequate resources should be made available to implement the training.

EPRI report [16] mentions the following more detailed issues pertaining to control room upgrades:

- Changes in crew roles, responsibilities, and teamwork;
- Understanding the characteristics and functions of computer based HSIs;
- Interacting with automatic systems and decision aids;
- Recognizing and handling failures;
- Dealing with hybrid HSIs;
- Working with temporary, interim configurations.

Most of these issues are generally applicable to any control room upgrade, irrespective if a hybrid solution is involved or not. However, the two last issues relate in particular to hybrid solution.

It is important to be aware that irrespective of how well a training package is designed there will always be aspects that are not formalized, neither in the training package nor in the formal description of any new system put into the plant. Such aspects will be shaped once the system has been deployed in the plant and after a while work practices will be adapted (though possibly not in an optimal way). In other words, the final parts of the system design and training will happen after the system has been taken into use. This is important to be aware of in case of stepwise migration approaches, when the burden on the operator to find informal work practices might be considerable.

The goal of training is to establish an acceptable competence level of the crew.

Competence pertains to many different perspectives and elements, such as knowledge, skills and attitudes.

- Professional competence — knowledge about the plant and its functioning;
- Relational competence. The ability to cooperate with other people (from various professions) so that the organization as a whole may possess the competence and abilities to implement its work processes;
- Change competence. The ability to identify an area for which there is a need to establish and reinforce knowledge and competence.

Training must take into account all such dimensions as well as those dimensions that depend on soft issues such as the impact of tradition, social competence, organizational attitudes and an individual's motivation. A training programme must take all these issues into account in order to be successful in changing the behavior and competence of the staff. For instance, classroom training may change the theoretical knowledge of the individual, but unless the change is generally accepted by the organization the knowledge will not be taken into use and will soon be forgotten and the competence of the staff will remain unaffected.

Training for hybrid solutions must try to compensate for the additional human factor problems introduced by the hybrid solution. Several of these problems are related to the complexity of managing a wider range of technical solutions implementing one and the same function. This problem will require training in more a comprehensive curriculum to assert that staff possesses the required knowledge to handle all the applied technical solutions.

Depending on whether a step-wise migration is applied or not, there may be different needs for re-training. Frequent re-training can be confusing to the end users (operators, maintenance crew, etc.), as the various stages of the migration may not be identified clearly. The user might easily be confused with respect to the details of the current configuration, and as an example errors might happen because the user thinks he/she is running a configuration corresponding to one of the previous migration steps.

Thus it is important to take into account the training needs for each intermediate step when deciding on the details of each individual step in the migration process.

There is a wide range of hypothetical problems that might come from the mixing of different technological solutions. One of the most common examples of this is the mixing of panel-based and screen-based systems. In such a setting the users might frequently be required to leave the workstations to monitor parameters or take action at control panels. Some of the potential problems that come from such a constellation are the following:

— The user might not have easy access to pertinent information from the position he/she is located at a specific point in time;
— The user might be required to remember things when moving from one position to another (e.g. moving from the computer screen to the console);
— The user will have to switch between two different information display paradigms (the console allowing pattern-matching-like access while the screen would need some navigation before the desired information could be retrieved).

Of course, such problems should be compensated for in the work processes which are supposed to benefit from the combined systems; nonetheless, users still frequently find themselves in situations that are not normative. The normative use of the system only takes into account a restrained set of operational possibilities. Occasionally situations occur that are outside this set, and the operator has to improvise to be able to perform his/her tasks adequately. This requires flexibility from of the systems, but it also requires training in using the flexibility.

Some other training challenges come from the fact that hybrid control rooms, as well as fully computerized systems, tend to be complex.

It has been observed [17] that even though many of the new computer based HSI technologies provide advanced information presenting and processing capabilities, the operators often receive little or no training in strategies for using these capabilities effectively. Some people suggest that operator performance may benefit from combined training that addresses both the use of HSI capabilities and the skills and strategies for making the best use of the information processing capabilities.

Studies of both Converse (1995) [18] and Roth and O’Hara (1998) [19] show evidence that there is a need to train on a fairly wide ranging set of scenarios when learning, evaluating, or validating new systems. Not surprisingly, the training should include the whole range from normal to multi-fault conditions. The operators in the Roth and O’Hara study thus expressed a need to have a wider range of training scenarios. The operators participating in the study also desired more opportunities to try out systems on the simulator. This is an indication that training packages often are insufficient in presenting an adequate range of situations and the trainee remains uncertain with respect to the actual use of the systems.

This underlines the importance of placing a focus on the informal work processes of the plant, keeping in mind that they are different from work processes defined formally. It is probable that all details of the work processes can not be developed or examined a priori but must be developed as the system is taken into use. The training packages developed before the system is taken into use must only be regarded preliminary. The actual use of the system is only partly known at this stage. Once the system is put into actual use, additional usability problems may manifest and must be compensated for in both the configuration of the system and in the training packages offered to the trainee. As stated above, this requires a degree of flexibility of the technical solutions, making it possible to adapt its configuration. It also assumes the existence of a deliberate development strategy of both the system and the complementary training.

Obviously much of this work cannot be made part of a training package, completely designed beforehand, as it cannot be imagined beforehand. A training simulator is indispensable in this respect since it gives the trainee the possibility to experience how a system is to be used as an integral part of a working situation, revealing all its designed as well as its unintended effects. This becomes particularly important in a hybrid setting since unintended effects are more frequent for this type of MCR set-ups. In the case of incremental MCR upgrades, the demand on the updates of the training simulator may be demanding since it needs to follow the many upgrade steps, and must be subject to several simulator upgrades.

4.6.2. Simulator upgrade

Effective training of control room operating personnel is essential to the safe and efficient operation of a nuclear power plant. A control room simulator is the primary training tool used to deliver this training and qualify control room operating personnel.

The simulator should be adequately maintained and upgraded when necessary to ensure that it continues to be a viable training tool that accurately replicates the operational characteristics of the reference NPP. IAEA-TECDOC-1500 [63] provides guidance on upgrade and modernization of NPP training simulators. It advises that NPP management personnel, in conjunction with the training department and simulator maintenance and engineering support personnel, should continuously monitor and evaluate the performance of the simulator in order to identify the need for upgrade or modernization. An upgrade or modernization of the simulator should be conducted based upon proven project management principles and methods.

Plant training simulator upgrade or modernization is required to reflect the following plant changes:

- Control panel modifications or upgrades;
- Digital control system installations;
- Plant process control computer system upgrades or replacements;
- Implementation of supplemental simulation systems.

Four potential simulator upgrade paths can be considered for step-phased projects:

- Simultaneous migration to plant modernization configuration;
- Addition of a new simulator corresponding to the new plant configuration while retaining previous simulator configuration;
- Dual mode simulator capable of switching between upgraded and existing functionality (if possible);
- New partial simulator for upgraded functionality only.

5. CONCLUSIONS

Modernization of I&C systems, including main control room in older nuclear power plants, is becoming an important issue. Many nuclear power plants are achieving higher availability factors and higher levels of safety by adopting well planned modernization projects. I&C modernization may actually become necessary more than once during the plant lifetime.

New digital technologies offer significant opportunities to improve the access to and presentation of information to the user, e.g. operators, maintenance staff and management. However, this technology should be used prudently. Modernization of I&C system should be made for the benefit of the plant to respond to the needs of the plant and its staff. In some cases, modernization is undertaken to resolve ageing and obsolescence or to meet regulatory requirements for license renewal. The integration of new technologies during MCR modernizations should be performed cautiously and all affected aspects of plant maintenance, and operation should be carefully considered, paying particular attention to the human factors elements of these affected aspects.

It is highly recommended that a formal, well planned approach to modernization be put in place. This approach, which involves all stakeholders from the utility, design organizations and regulatory authorities, should be based on a long term vision and take into account plant performance data, experiences in similar plants and evolving I&C technologies. Because changes to the MCR will require the operations crew to adjust to the new configuration, it is important to integrate the constraints of the existing plant. New HSI functions should only be added in the MCR when there is reasonable evidence of a significant benefit to the safe and efficient operation of the plant. Before entering an I&C modernization project, it is advisable to define an overall modernization plan that addresses engineering of the upgrade, maintenance and staffing. A staff management plan should be prepared to describe the existing organization, the future organization and to identify the path to reach the new organization. Managers should be aware that the required technical skill set may not exist or be available within the utility and that new staff recruitment may be required. Such recruitment should be done early, as the chosen candidate is likely to require additional training.

The planning and execution of modernization projects which result in hybrid MCRs should carefully account for: the human factors aspects of the modifications and the proper integration of different technologies. The introduction of digital technologies may often produce extensive changes to the HSI which makes the human factors considerations of hybrid MCR modernizations extremely important.

Any modernization should be accompanied by additional training to provide staff with skills needed to use and maintain the new system and adopt the new working environment that results from introducing new technology. For the training of the operators, a simulator should be available that reflects the current control room environment and accurately replicates the operational characteristics of the reference nuclear power plant.

While the modernization of MCRs, resulting in hybrid technologies, is often conducted in response to ageing and obsolescence it is important to keep in mind that one must also plan for the eventual maintenance and/or replacement of these new digital systems.

Digital I&C technology is evolving very quickly. Some future research needs are:

- Cyber security of I&C system;
- Field programmable gate array application;
- Wireless communication technology application;
- Intelligent control applications;
- Safety software failure mode effect analysis;
- Reliability of digital safety I&C;
- Links I&C and IT systems (corporate networks);
- New operational support systems;
- Software reliability;
- Common cause failure evaluation.

GLOSSARY

advanced alarm system. A primarily digital alarm system employing alarm processing logic and advanced control (e.g. on-screen controls) and display (e.g. VDU) technology. This is in contrast to conventional alarm systems, which are largely based on analog instrument and control technologies.

analog. A form of transmission that is a continuous wave electrical signal that varies in frequency and/or amplitude in response to the variation of physical phenomena such as human speech or music. Broadcast and phone transmission have conventionally used analog technology.

anthropometry. A study and measurement of the physical dimensions of the human body.

audio. Pertaining to acoustic, mechanical or electrical frequencies corresponding to normally audible sound waves.

auditory. Pertaining to the sense of hearing.

button. A type of hardware control device or a defined control region on the display screen which, when selected, causes some action.

clearance. Tag-out, or padlock.

coding. Use of a system of symbols, shapes, colors or other variable sensory stimuli to represent specific information. Coding may be used (a) for highlighting (i.e. to attract a user's attention to part of a display), (b) as a perceptual indicator of a data group, or (c) to symbolize a state or attribute of an object (e.g. to show a temperature level or for warning purposes).

cognitive error. A human error that results from the characteristics of human performance processing such as errors in diagnosis due to information overload.

color. The aspect of objects or light sources that may be described in terms of hue, lightness (or brightness) and saturation.

component. The meaning of the word depends on its context. In context of the entire plant, it is an individual piece of equipment such as a pump, valve, or vessel, usually part of a system. In a human-system interface context, a component is one part of a large unit, such as one meter in a control board.

computer based procedure systems. Systems that present plant procedures in computer based rather than paper based formats.

computerized operator support systems. Systems that use computer technology to support operators or maintenance personnel in situation assessment and response planning. They can monitor status and provide recommendations or warnings.

darkboard. An alarm display in which the medium is dark (not illuminated) if all monitored plant parameters are in the normal range. Thus, an illuminated alarm-display device indicates a deviation from normal plant conditions. This is in contrast to many conventional alarm systems, which employ display devices to indicate both normal and abnormal changes in the plant's condition.

diagram. A special form of a picture in which details are only shown if they are necessary to perform a task. For example, an electrical wiring diagram for a facility would show wiring but not necessarily furniture or plumbing.

dialogue. A structured series of interchanges between a user and a computer. A dialogue can be initiated by a computer (e.g. question and answer) or by a user (e.g. command language).

digital. A method of storing, processing and transmitting information through the use of distinct electronic or optical pulses that represent the binary digit 0 and 1. Digital transmission/switching technologies employ a sequence of discrete, distinct pulses to represent information, as opposed to the continuously variable analog signal.

display. A specific integrated, organized set of information. A display can be an integration of several display formats (such as a system mimic which includes bar charts, trend graphs, and data fields).

display device. The hardware used to present the display to users. Examples include video display units and speakers for system messages.

display element. A basic component used to make up display formats, such as abbreviations, labels, icons, symbols, coding and highlighting.

display format. The general class of information presentation. Examples of general classes are continuous text (such as a procedure display), mimics and piping and instrumentation diagram (P&ID) displays, trend graphs, and flowcharts.

display network. A group of display pages within an information system and their organizational structure.

display page. A defined set of information that is intended to be displayed as a single unit. Typical nuclear power plant display pages may combine several different formats on a single VDU screen, such as putting bar charts and digital displays in a graphic P&ID format. Display pages typically have a label and designation within the computer system so they can be assessed by operators as a single ‘display’.

display selection. Refers to the specification of data outputs, either by a user or automatically.

display structure. Functional or information-presenting aspects of a display that are consistent in appearance and use across applications, e.g. providing reference to the user's location in an information system and display of control options available.

dynamic mockup (prototype). A dynamic representation of a HSI that is not linked to a process model or simulator. A model of an interface, which includes the functions and capabilities expected in the final system, though not in a finished form.

flowchart. A diagram that illustrates sequential relations among elements or events. Flowcharts are often shown as boxes connected by arrows.

function. (1) a software supported capability provided to a user to aid in performing a task; (2) a process or activity that is required to achieve a desired goal; see, e.g. safety function.

graphical display. A display that provides a pictorial representation of an object or a set of data. Graphical displays include line, solid object, and perspective drawings; bar, pie, and line charts and graphs; scatter plots; displayed meters; flowcharts and schematic diagrams.

graphics. Data specially formatted to show spatial, temporal, or other relations among data sets.

human engineering discrepancy (HED). A departure from some benchmark of system design suitability for the roles and capabilities of the plant operator. This may include a deviation from a standard or convention of human factors engineering practice, an operator preference or need, or an instrument/equipment characteristic that is implicitly required for an operator's task but is not provided to the operator.

human factors engineering (HFE). The application of knowledge about human capabilities and limitations to plant, system and equipment design. HFE ensures that the plant, system, or equipment design, human task and work environment are compatible with the sensory, perceptual, cognitive and physical attributes of the personnel who operate, maintain and support it.

human-system interface (HSI). The human-system interface (HSI) is that part of the system through which personnel interact to perform their functions and tasks. In this publicatioin, 'system' refers to a nuclear power plant. Major HSIs include alarms, information displays, controls, and procedures. Use of HSIs can be influenced directly by factors such as: (1) the organization of HSIs into workstations (e.g. consoles and panels); (2) the arrangement of workstations and supporting equipment into facilities such as a main control room, remote shutdown station, local control station, technical support center, and emergency operations facility and (3) the environmental conditions in which the HSIs are used, including temperature, humidity, ventilation, illumination and noise. HSI use can also be affected indirectly by other aspects of plant design and operation such as crew training, shift schedules, work practices and management and organizational factors.

Iluminance. The luminous flux incident on a surface, measured in lumens per square meter (lux) or in Footcandles (fc).

icon. Pictorial, pictographic or other nonverbal representation of objects or actions.

illumination. The amount of light falling on a surface.

layout. The physical arrangement of the parts and components that make up a module or a unit of equipment.

luminance. The luminous intensity per unit projected area of a given surface as viewed from a given direction. Measured in candelas per square meter or footlamberts.

menu. A type of dialogue in which a user selects one item out of a list of displayed alternatives. Selection may be made by actions such as pointing and clicking and by depressing an adjacent function key.

menu bar. A specialized function area that displays categories of alternatives of user responses.

mimic. A display format combining graphics and alphanumerics used to integrate system components into functionally oriented diagrams that reflect the components' relationships.

parameter. (1) a power conversion process variable or quantity that can assume any of a given set of physically feasible values. Plant parameters are typically measures of the performance of systems and processes of the plant, e.g. the parameter 'T-hot' is a measure of the temperature of reactor coolant that has passed through the reactor core. (2) a variable that is measured.

ringback. An alarm display feature that provides a distinct cue such as a slow flash or audible tone to indicate that an alarm condition has cleared, i.e. the monitored parameter(s) has returned to its normal range.

simulator. A facility that physically represents the HSI configuration and that dynamically represents the operating characteristics and responses of the plant in real time, including a process model.

soft control. A control device that has connections with the control or display system mediated by software rather than direct physical connections. As a result, the functions of a soft control may be variable and context dependent rather than statically defined. Also, the location of a soft control may be virtual (e.g. within the display system structure) rather than spatially dedicated. Soft controls include devices activated from display devices (e.g. buttons and sliders on touch screens), multi-function control devices (e.g. knobs, buttons, keyboard keys, and switches that perform different functions depending upon the current condition of the plant, the control system, or the human-system interface), and devices activated via voice input.

tile. A type of spatially dedicated, continuously visible alarm-display that changes state (i.e. brightness, color, and/or flash rate) to indicate the presence or absence of an alarm condition, and includes text to identify the nature of the alarm state.

variable. A quantity that can assume any of the given set of values.

video display unit. An electronic device for the display of visual information in the form of text and/or graphics. Typically abbreviated as VDU.

warning signal. A signal that alerts the operator to a condition requiring immediate action (see caution signal).

Annex I

CASE STUDY

I–1. QUALIFICATION OF COMMERCIAL OFF-THE-SHELF PRODUCTS

This presents an application-specific product qualification (ASPQ) methodology that has been developed at the Atomic Energy of Canada Limited (AECL) and successfully applied to qualify Programmable Electronic System (PES) equipment intended for use in domestic CANDU® 6 and advanced CANDU® reactor (ACR-1000®) power plants and special purpose reactors at the Chalk River Laboratories in Canada.

I–2. APPROACH OF ASPQ

As a minimum, an ASPQ of a PES product should address the following fundamental areas:

- Suitability of the PES product for the intended application, particularly with respect to functional safety suitability requirements over the expected in-service life;
- Product documentation;
- Evidence of correctness of the design;
- User documentation for safety.

The assessment of a PES product should derive and apply appropriate qualification requirements and a degree of formality and depth of assessment appropriate to its importance to safety. The range of qualification methodologies applied should be appropriate to the PES importance to safety. Before ASPQ can begin, the system class must be determined using appropriate methods to categorize safety functions and classify the system (e.g. using IEC 61226 0 and IEC 61513 0. Figure I–1 provides a simplified view of the ASPQ process.

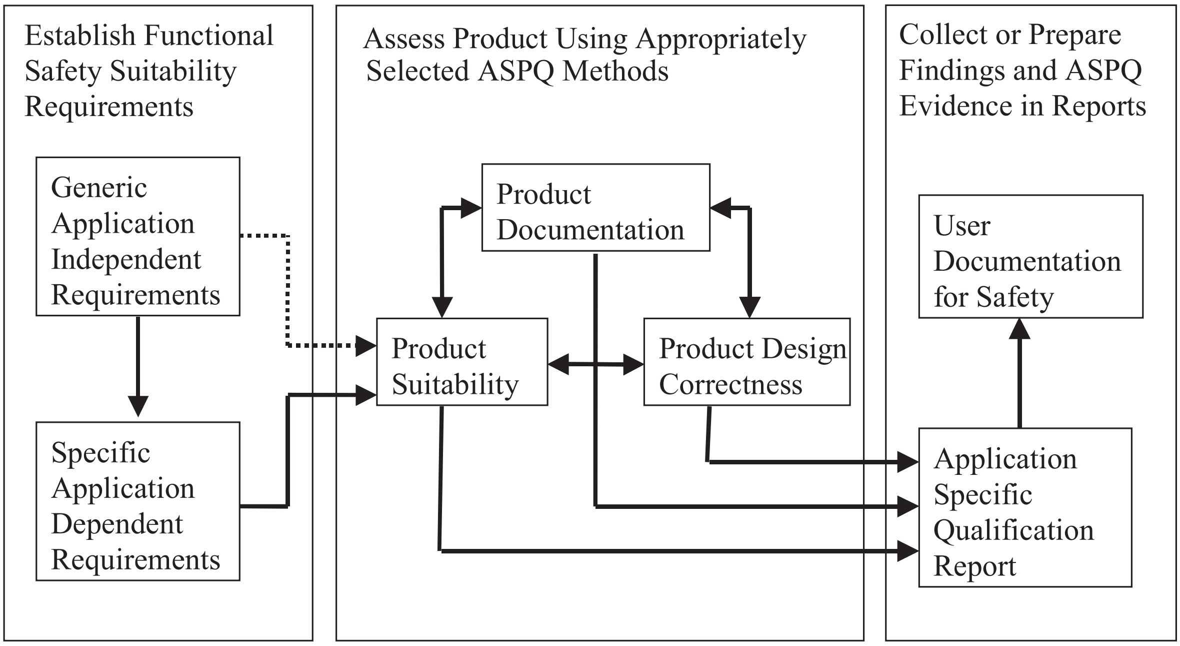

Establish Functional Safety Suitability Requirements
Generic Application Independent Requirements
Specific Application Dependent Requirements
Assess Product Using Appropriately Selected ASPQ Methods
Product Documentation
Product Suitability
Product Design Correctness
Collect or Prepare Findings and ASPQ Evidence in Reports
User Documentation for Safety
Application Specific Qualification Report

FIG. I–1. Simplified view of the ASPQ process.

An ASPQ report summarizes the documented evidence and the assessment arguments, and applies to the hardware, software and (to the extent they may affect functional safety) any configuration or maintenance tools associated with the PES product.

I–2.1. Suitability evaluation

To establish ‘suitability of the product’, ASPQ suitability requirements (i.e. a set of critical characteristics for acceptance that are a sub-set of the overall requirements for the PES) must be determined. The PES product or component is then assessed against these requirements based on the documented features, capabilities, functions, behaviours and/or limitations of the product. The suitability evaluation involves three important activities:

- The suitability requirements need to be determined and documented by the assessor, and this includes application-independent and application-dependent suitability requirements;
- The product documentation needs to be obtained and the adequacy of the documentation determined to be sufficient to support such an evaluation;
- Appropriate evaluation methods need to be applied to evaluate product suitability.

The application-independent suitability requirements are generic and are determined from the accepted norms and best practice as defined by the requirements of appropriate safety-related system development reference standards (e.g. IEC nuclear I&C family of standards IEC 62138 0, and IEC 61508 0) For example, appropriate requirements for determinism of a Class 1 PES can be derived from IEC 61508 0 requirements for SIL 3 and would include requirements such as static resource allocation, simple state behavior and a predictable maximum response time. In Class 2 and Class 3 applications, it may be justifiable (based on consideration of the application-dependent suitability requirements) to relax or ignore an application-independent suitability requirement derived from the reference IEC standards.

The application-dependant suitability requirements are specific and are identified from an assessment of the safety-related ‘reliance’ placed on the PES product or component in the target application. This is very context-specific and typically must consider factors both external and internal to the PES. For example, the potential impact on safety of a configuration tool to make software changes safely (i.e. a safety-related function) may depend entirely upon what state the equipment is required to be in (typically an external factor), what protections are built into the PES product or component ensure safety (typically an internal factor), and the intended modes of use of the tool (could be either an external or internal factor).

PES product or component specifications are reviewed to understand the product architecture, features, capabilities, behaviours and attributes. The plant design basis documentation for the system of which the product or component is a part, such as the design requirements, system architecture, technical specifications, safety analysis, HAZOP study, design manual, and user manuals (if they exist), should also be consulted. In some cases, there may not be clear or adequate requirements specified in the design basis documents to sufficiently derive ASPQ application-dependent suitability requirements. In this situation, the assessor will need to work with I&C system designers or maintainers to fully understand the context of use and state clearly any assumptions made.

The suitability requirements are derived from and should consider any safety-related reliance on the PES. Safety-related reliance may be direct or indirect, external or internal, and applies to the design, commissioning and in-service life cycle. Suitability requirements should define the expected product features, capabilities, behaviors or attributes needed to ensure functional safety and may include specific requirements with respect to any or all of the following types of requirements, as necessary:

- Specific safety properties/behavior of the product, e.g. requirements for fail-safe behavior, fail-detected behavior, failure recovery behavior, immunity to single failures, or common cause failures, all as applicable to the operational requirements of the application context;
- Functionality (including human factors considerations);
- Reliability properties/attributes, e.g. requirements for useful life, requirements for redundancy, or tolerance limits on input power quality;

- Maintainability features/functions (including reparability, on-line serviceability, safe maintenance modes);
- Testability features/functions, e.g. specific requirements to support in-service testability;
- Performance properties/attributes e.g. determinism or response time;
- Security features/functions.

These suitability requirements include consideration of:

- Seismic requirements;
- Environmental tolerance requirements, e.g. temperature, vibration and shock, radiation, humidity, stress and loading, dust, pressure, fire resistance, etc;
- Electromagnetic compatibility (EMC) requirements, e.g. immunity to radiated electromagnetic field, magnetic field, conducted disturbances, electrostatic discharge (ESD), electrical fast transient/burst (EFT/B), and surge; as well as limits on radiated and conducted emissions, as dependent on the location.

The suitability evaluation should be based on a comparison and assessment of compliance of the ASPQ suitability requirements and the product documentation.

I–2.2. User documentation for safety

The user documentation for safety is reviewed and the qualification must ensure that any issues that may directly or indirectly impact safety over the life cycle of the product are addressed, such as:

- Any recommended procedures for operation and maintenance;
- Requirements for periodic inspection or proof testing;
- Procedures or restrictions on the modification of software or the upgrade of firmware (if applicable);
- Documentation of any customization or modification required to dedicate the equipment and needed for future equivalent replacements;
- Identification and documentation of environmental limits and lifetime limits (i.e. the hardware useful life).

As required, either the manufacturer or the project should prepare supplementary user documentation for safety. This documentation may be incorporated in a user or operating manual, in a training manual or in a maintenance manual as appropriate.

I–2.3. Evidence of correctness

To establish evidence of correctness of the product design, the qualification should consider and document an adequate reviewable argument using the following four general approaches:

Approach 1: Evidence of compliance to appropriate and recognized safety-related I&C systems development standard(s).

Approach 2: Evidence of reliability, gathered from documented reliable in-service operational field experience, i.e. a ‘proven in use’ argument.

Approach 3: Evidence based on complementary testing (i.e. testing to demonstrate the product operates in a manner consistent with its documentation and in a manner that meets the application requirements).

Approach 4: Evidence based on analysis of the detailed design.

For System Class 1 PES, adequate evidence of correctness from either approach 1 or any two of approaches 2, 3, or 4 above should be documented. If the evidence available is generally reasonable but slightly deficient in specific areas, supplemental evidence from any of the other approaches may be used to compensate and provide the requisite confidence in the correctness of the product design. For System Class 2 and 3 PES, adequate evidence of correctness from any one of the approaches 1–4 above should be documented. If the evidence is generally reasonable but deficient in specific areas, supplemental evidence from any of the remaining approaches, or combination of approaches may be used to compensate and provide the requisite confidence in the correctness of the product design. In this context, adequate evidence means that by applying the ASPQ methods, it can be shown the product in the defined context of use meets or exceeds the norms and expectations for functional safety established by industry best practices as interpreted from appropriate industry standards and guidelines, and as suitably graded according to the system class. For example, proven in use arguments should meet the specific requirements defined in IEC 61508 for minimum operating hours, fault-free operation, and similar applications as appropriate for the system class.

I–2.4. Special case considerations

Several special cases for ASPQ may affect the ASPQ requirements or the requirements on the process and approach taken. Careful consideration of these special cases (when appropriate) may affect the overall ASPQ effort. The special cases identified are the ASPQ of:

- A PES product having a previous qualification (ASPQ or GPQ);
- A PES product that meets specific criteria as "simple non-modifiable devices" (SNDs);
- A PES product that embeds stand-alone software (i.e. 'software-only') products;
- A PES product is used such that minimal reliance is placed on hardware or operating system;
- A PES product used with compensating measures at the system design level;
- PES containing software implemented using limited variability languages;
- Configuration and maintenance tools used with a PES;
- A PES product where modifications are required;
- A PES product having internal sub-components.

When these special cases apply, additional considerations may influence the approach, including methods chosen.

I–2.5. Evidence gathering and assessment methods and their selection

A summary of the assessment 'evidence gathering and assessment methods' included in the approach and used to perform ASPQ is provided in Table I.1. The applicability of each method in providing evidence of the adequacy of product documentation, suitability, or correctness of the design is indicated. Table I.2 provides a further breakdown of the type of suitability requirement addressed by each assessment method (as to safety, functionality, reliability, maintainability, testability, performance, and security).

The set of possible methods to be applied to perform a given ASPQ depends on the system class of PES product required and the suitability requirements determined. Appropriate evidence gathering and assessment methods are then selected based on availability of evidence to support the method and the expected benefit in providing suitability evidence or evidence of correctness. When licensing is an issue (i.e. for Class 1, most Class 2, and some more significant Class 3 systems [e.g. plant display systems where human factors are a concern]), the assessor must ensure: that the ASPQ evidence obtained is in a reviewable and verifiable form; and that the qualification argument is complete and defensible. When deriving and interpreting ASPQ requirements, the manner in which the ASPQ methods are applied, the degree of formality in the process, the depth of analysis, and the level of detail in the documentation will all depend on the system class (some judgment is required).

Experience has shown that ASPQ assessments of products that are intended by design for use in safety-related applications tend to be much easier. Qualification of non safety-market products may be feasible, however, they incur added costs to secure vendor support for the qualification and additional methods are often required to obtain adequate evidence (e.g. product modifications, complementary testing, etc.).

I–2.6. OTHER CONSIDERATIONS FOR ASPQ

The use of COTS PES products in nuclear safety-related applications is increasing and has demonstrated tangible benefits. However, the vulnerabilities of digital technology must be appropriately considered and addressed. The ASPQ process plays an important role in guiding the proper integration of PES technology during I&C system design by identifying technology limitations that need to be addressed to ensure functional safety.

TABLE I–1. ASPQ EVIDENCE PROVIDED BY EVIDENCE GATHERING AND ASSESSMENT METHODS

Qualification methods		Evidence obtained		
		Adequacy of documentation	Stability	Evidence of correctness
Method 1.	Qualification feasibility assessment	√	√	
Method 2.	Assessment of product specifications (hardware, software, and tools)	√	√	√
Method 3.	Proven in use assessment			
	a) Operating history data	√	√	√
	b) Failure data assessment	√	√	√
	c) Product design revision history assessment	√		√
	d) Reference site assessments		√	√
Method 4.	Maintenance assessment			
	a) In-service maintenance process assessment	√	√	
	b) In-service testability assessment	√	√	√
Method 5.	Hardware design assessment			
	a) Environmental tolerance assessment	√	√	√
	b) Electromagnetic immunity and emissions assessment	√	√	√
	c) Seismic tolerance assessment	√	√	√
	d) Hardware reliability, failure modes and diagnostic assessment	√	√	√
	e) Assessment of hardware useful life	√	√	√
Method 6.	Hardware development process assessment			
	a) Assessment of hardware testing techniques	√		√
	b) Hardware design process assessment	√		√
	c) Product manufacturing process methods and QA assessment	√		√
Method 7.	Software design assessment			
	a) Software safety impact assessment	√	√	√
	b) Assessment of software diagnostics and self-check capability	√	√	√
	c) Assessment of software goodness of design	√		√
	d) Software HAZOP	√	√	√
Method 8.	Software development process assessment			
	a) Assessment of software design-implementation processes	√		√
	b) Assessment of software testing techniques	√		√
	c) Assessment of software configuration management process	√		√
	d) Software support and support-life assessment		√	√

TABLE I–1. ASPQ EVIDENCE PROVIDED BY EVIDENCE GATHERING AND ASSESSMENT METHODS (cont.)

Qualification methods		Evidence obtained		
		Adequacy of documentation	Stability	Evidence of correctness
Method 9.	Evidence from 3rd party certifications and assessments			
	a) Assessment of 3rd party corporate quality system certifications	√	√	√
	b) Assessment of 3rd party product safety certifications	√	√	√
	c) Assessment of 3rd party hardware test standards compliance	√	√	√
	d) Assessment of 3rd party software development process certifications	√		√
Method 10.	Limited product modifications		√	
Method 11.	Complementary testing		√	√

TABLE I.2. SUITABILITY EVIDENCE PROVIDED BY EVIDENCE GATHERING AND ASSESSMENT METHODS

Qualification methods		Suitability evaluation evidence						
		Safety	Functionality	Performance	Reliability	Maintainability	Testability	Security
Method 1.	Qualification feasibility assessment	√	√	√	√	√	√	√
Method 2.	Assessment of product specifications (hardware, software, tools)	√	√	√	√	√	√	√
Method 3.	Proven-in-use assessment							
	a) Operating history data	√	√	√	√			
	b) Failure data assessment	√	√	√	√			
	c) Product design revision history assessment			√	√	√		
	d) Reference site assessments	√	√	√	√	√		√
Method 4.	Maintenance assessment							
	a) In-service maintenance process assessment	√	√			√	√	√
	b) In-service testability assessment	√	√	√	√	√	√	√
Method 5.	Hardware design assessment							
	a) Environmental tolerance assessment			√	√			
	b) Electromagnetic immunity and emissions assessment			√	√			
	c) Seismic tolerance assessment			√	√			
	d) Hardware reliability, failure modes and diagnostic assessment	√	√	√	√			
	e) Assessment of hardware useful life			√	√	√		

TABLE I.2. SUITABILITY EVIDENCE PROVIDED BY EVIDENCE GATHERING AND ASSESSMENT METHODS (cont.)

Qualification methods	Suitability evaluation evidence						
	Safety	Functionality	Performance	Reliability	Maintainability	Testability	Security
Method 6. Hardware development process assessment							
a) Assessment of hardware testing techniques	√	√	√	√		√	√
b) Hardware design process assessment	√	√		√	√		√
c) Product manufacturing process methods and QA assessment				√			
Method 7. Software design assessment							
a) Software safety impact assessment	√	√					√
b) Assessment of software diagnostics and self-check capability	√	√	√	√		√	
c) Assessment of software goodness of design	√			√	√		√
d) Software HAZOP	√	√		√	√		
Method 8. Software development process assessment							
a) Assessment of software design-implementation processes	√		√	√	√		√
b) Assessment of software testing techniques	√	√	√	√	√	√	√
c) Assessment of software configuration management process				√	√		
d) Software support and support-life assessment					√	√	
Method 9. Evidence from 3rd party certifications and assessments							
a) Assessment of 3rd party corporate quality system certifications				√	√		
b) Assessment of 3rd party product safety certifications	√	√		√	√		√
c) Assessment of 3rd party hardware test standards compliance			√	√		√	
d) Assessment of 3rd party software development process certifications	√			√	√		
• Limited product modifications	√	√	√	√	√	√	√
• Complementary testing	√	√	√	√	√	√	√

Qualification can be technically challenging and may, at times, present difficulties. These situations should be recognized and planned for accordingly. Sometimes the involvement of experienced assessors and/or specialists is required, particularly in defining or clarifying ASPQ requirements or in selecting an appropriate choice of evidence gathering and assessment methods. For more complex systems (i.e. having potentially many PES components) and particularly for Class 1 systems, it can be a technically involved assessment process. To ensure that an ASPQ is completed in the shortest achievable time period, a project approach is taken whereby activities are well planned and scheduled. The plan should include consideration of additional issues, such as concerns by manufacturers over access to and protection of proprietary design technology, willingness to grant access to and permit documentation of commercially sensitive product failure or sales data, the frequent need for non-disclosure agreements, access to the manufacturers key product development staff, and ownership rights to the final ASPQ report may also be barriers. Finally, the approach emphasizes the need to address qualification issues as early as possible in the design and procurement process, and put clear expectations on the product manufacturer/suppler to support the process. This greatly reduces risk, improves the up-front consideration of qualification issues in a project, and helps to minimize the likelihood of problems.

REFERENCES TO ANNEX I

[I–1] IEC 61226, Nuclear Power Plants — Instrumentation and Control Systems Important for Safety — Classification of Instrumentation and Control Functions, 2005.

[I–2] IEC 61513, Nuclear Power Plants — Instrumentation and Control for Systems Important to Safety — General Requirements for systems, 2001.

[I–3] IEC 62138, Nuclear Power Plants — Instrumentation and Control Important for Safety — Software Aspects for Computer based Systems Performing Category B or C Functions, 2004.

[I–4] IEC 61508, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, 2005.

ORGANIZATIONS

EPRI	Electric Power Research Institute
EUCG	Electric Utility Cost Group
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineer
INPO	Institute of Nuclear Power Operations
NEI	Nuclear Energy Institute

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Information Technology Impact on Nuclear Power Plant Documentation IAEA-TECDOC-1284, IAEA, Vienna (2002).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Management of Life Cycle and Ageing at Nuclear Power Plants: Improved I&C Maintenance, IAEA-TECDOC-1402, IAEA, Vienna (2004).

[3] EPRI 1003696 Final Report “Interim Human Factors Guidance for Hybrid Control Rooms and Digital I&C Systems”, August 2003, USA.

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Knowledge Management for Nuclear Industry Operating Organization, IAEA-TECDOC-1510, IAEA, Vienna (2006).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, The Nuclear Power Industry's Ageing Workforce: Transfer of Knowledge to the Next Generation, IAEA-TECDOC-1399, IAEA, Vienna (2004).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Configuration Management in Nuclear Power Plants, IAEA-TECDOC-1335, IAEA, Vienna (2003).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Protecting Against Common-Cause Failures in Digital I&C Systems, IAEA Nuclear Energy Series No. NP-T-1.5, IAEA, Vienna (2009).

[8] EPRI 2005a — 1010042, “Human Factors Guidance for Control Room and Digital Human-System Interface Design and Modification: Guidelines for Planning, Specification, Design, Licensing, Implementation, Training, Operation, and Maintenance”, December 2005, USA.

[9] NUREG-0700, “Human- System Interface Design Review Guidelines”, Rev. 2, March 2002, USA.

[10] NUREG-0899, U.S. Nuclear Regulation Commission, Guidelines for the preparation of emergency operating procedures, Washington DC, 1982.

[11] NUREG-0711 Revision 2 Human Factors Engineering Program Review Model, U.S. Nuclear Regulatory Commission, Washington DC, 2004.

[12] IEC 60964, “Design for Control Rooms of Nuclear Power Plants,” 1989.

[13] EPRI, 2005b, “Guidance for the Design and Use of Automation in Nuclear Power Plants”, EPRI — 1011851, November 2005.

[14] IEEE Std 7-4.3.2 Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, 1993.

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Information Integration in Control Rooms and Technical Offices in Nuclear Power Plants, IAEA-TECDOC-1252, IAEA, Vienna (2001).

[16] EPRI 1008122 Human Factors Guidance for control room and digital human-system interface design and modification: Guidelines for planning, specification, design, licensing, implementation, training, operation, and maintenance, 2004.

[17] NUREG/CR-6637,US Nuclear Regulatory Commission, Human Systems Interface and Plant Modernization Process: Technical Basis and Human Factors Review Guidance, Stubler, W.F., O’Hara, J.M., Higgins, J.C. & Kramer, J, January 2000, Washington, DC, USA.

[18] NUREG/CR-6398, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Evaluation of the Computerized Procedures Manual II (COPMA II), Converse, S.A, 1995, Washington, DC.

[19] BNL Letter Report J6012-3-4-7/98, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Integrating Digital and Conventional Human System Interfaces: Lessons Learned from a Control Room Modernization Program, Roth, Emilie & O’Hara, John (1998).,Washington, DC.

[20] D. STAMATIS, Failure Mode Effect Analysis: FMEA from Theory to Execution, 2003, ASQ Quality Press Milwaukee, Wisconsin.

[21] IEC STD 60812, Analysis techniques for system reliability- Procedure for failure mode and effects analysis (FMEA), 2006.

[22] MIL-STD-1629A, Procedures for Performing a Failure Mode, Effects and Criticality Analysis, 1980.

[23] IEEE STD 603-1998, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

[24] FMEDA — Accurate Product Failure Metrics, FMEDA Development Paper, Revision 1.1 February 19, 2007, John C. Grebe, William M. Goble, exida, Sellersville, PA 18960 USA.

[25] IEC STD 61508, Part 2, 2000, Requirements for electrical/electronic/programmable electronic safety-related systems.

[26] Fault tree and failure mode and effects analysis of a digital safety function, IAEA/IWG/ATWR and NPPCI technical committee meeting on advanced control and instrumentation systems in nuclear power plants. Espoo (Finland). 20–23 Jun 1994.

[27] RISTORD, L., ESMENJAUD, C., FMEA Performed on the SPINLINE3 Operational System Software as part of the TIHANGE 1 NIS Refurbishment Safety Case, Organisation for Economic Co-Operation and Development — Nuclear Energy Agency, Committee on the safety of nuclear installations, 75 — Paris (France) Proceedings of the CNRA/CSNI workshop on licensing and operating experience of computer based I and C systems, p. p. 231–244, 10 Jun 2002.

[28] Methods and tools used at the IPSN for the safety assessment of critical software, IAEA Specialists meeting on design and assessment of instrumentation and control systems in NPP coping with rapid technological change, Oct 1998, Vienna 188 p.p. 33–41.

[29] Software safety analysis techniques for developing safety critical software in the digital protection system of the LMR, Korea Atomic Energy Research Institute, Taejon (Korea, Republic of) KAERI/AR-591/2001 Report.

[30] [IEC 61508-4], Functional safety of electrical/electronic/programmable electronic safety-related systems — Part 4: Definitions and abbreviations.

[31] NUREG/CR-6268, Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding, Rev. 1, September 2007.

[32] J. BUKOWSKI and W. GOBLE, Verifying common-cause reduction rules for fault tolerant systems via simulation using a stress-strength failure model, ISA Transaction 40 (2001) 183–190.

[33] IAEA Technical Meeting on Common-Cause Failures in Digital Instrumentation and Control Systems of Nuclear Power Plants, Bethesda, Maryland, USA, 19-21 June 2007, hosted by the US NRC, DOE, EPRI, and NEI.

[34] NUREG/CR-5044, ***Estimation*** Techniques for ***Common Cause Failure*** Events, 1988 March.

[35] http://www.nea.fr/html/jointproj/icde.html, www.eskonsult.se./icde/

[36] NUREG/CR-5460, A Cause-Defense Approach to the Understanding and Analysis of Common-cause Failures, March 1990, SAND89-2368.

[37] Reliability evaluation of standby safety systems due to independent and common cause failure, Proceeding of the 2006 IEE International Conference on Automation Science and Engineering, Shanghai, China, October 7–10, 2006.

[38] Verifying common-cause reduction rules for fault tolerant systems via simulation using a stress-strength failure model, ISA Transition 40 (2001) 183–190.

[39] NUREG/CR-6268, Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding, Rev. 1, 2007.

[40] NUREG/CR-6819, Common-Cause Failure Event Insights**,** Date Published: May 2003, NRC.

[41] CCF analysis for reactor protection system reliability studies, INEEL/CON-99-00445, August 1999, Oak Ridge, Tennessee.

[42] AECB (Atomic Energy Control Board), C-138 Draft Regulatory Guide, Software in Protection and Control Systems, October 1999, Canada.

[43] USNRC, Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues, 1997, National Academy Press.

[44] EPRI TR-102348, Guide on Licensing Digital Upgrades, Revision 1, March 2002.

[45] J. BUKOWSKI and W. GOBLE, Verifying common-cause reduction rules for fault tolerant systems via simulation using a stress-strength failure model, ISA Transaction 40 (2001) 183–190.

[46] NUREG/CR-6303, Method for performing Diversity and Defence-in-depth Analysis of Reactor Protection Systems, December 1994.

[47] IEC STD 61882, Hazard and Operability (HAZOP) studies- Application guide, 2001

[48] NUREG-0800, Standard Review Plan, Branch Technical Position (BTP) 7-19, Guidance for Evaluation of Defence-in-Depth and Diversity in Digital Computer based Instrumentation and Control Systems, March 2007.

[49] USNRC Digital Instrumentation and Controls, DI&C-ISG-02, Interim Staff Guidance, September 2007.

[50] IEEE STD 379-2000: IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems.

[51] Verifying common-cause reduction rules for fault tolerant systems via simulation using a stress-strength failure model, ISA transactions 40, 2001, 183–190.

[52] IEC 61508-6, Annex D, A methodology for qualifying the effect of hardwire-related common cause failures in multi-channel programmable electronic systems.

[53] NREG/GR-0020, Embedded Digital System Reliability and Safety Analyses, NRC, Feb 2001.

[54] NRC, 10 CFR Part 50 Appendix B, Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants.

[55] EPRI TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, 1996.

[56] EPRI TR-107330, Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, 1996.

[57] EPRI TR-102348, Guideline on licensing digital upgrade, 2002.

[58] D. MANDIĆ, Usage of Commercial Grade Programmable Digital Systems in Safety Related Applications, 6th International Conference on Nuclear Option in Countries with Small and Medium Electricity Grids, Dubrovnik, Croatia, 21–25 May 2006, Paper Ref. No. S4-4, Nuklearna elektrarna Krško — NEK, Vrbina 12, 8270 Krško, Slovenia

[59] J. de GROSBOIS, et al., Qualification of Commercial Off-the-shelf Digital; Equipment For Use in Safety and safety-Related Nuclear Applications, InucE 2007.

[60] CSA N290.14, Qualification of Pre-Developed Software for use in Safety-Related Instrumentation and Control Applications in Nuclear Power Plants, 2007.

[61] IEC 61513, Nuclear Power Plants — Instrumentation and Control for Systems Important to Safety — General Requirements for systems, 2001.

[62] IEC 62138, Nuclear Power Plants — Instrumentation and Control Important for Safety — Software Aspects for Computer based Systems Performing Category B or C Functions, 2004.

[63] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidelines for Upgrade and Modernization of Nuclear Power Plant Training Simulators, IAEA-TECDOC-1500, Vienna (2006).

CONTRIBUTORS TO DRAFTING AND REVIEW

Choe, I.N.	Korea Power Engineering Company, Republic of Korea
De Grobois, J.	Atomic Energy of Canada Limited, Canada
Dionis, F.	Electricité de France, France
Freel, S.	GSE Systems, United States of America
Glöckler, O.	International Atomic Energy Agency
Jung, C.H.	Atomic Energy of Canada Limited, Canada
Kalechstein, W.	Atomic Energy of Canada Limited, Canada
Naser, J.	Electric Power Research Institute, USA
Nilsen, S.	OECD
Oh, I.S.	Korea Atomic Energy Research Institute, Republic of Korea
Ra, J.C.	Korea Power Engineering Company, Republic of Korea
Rasmussen, B.	Kurz Technical Services, United States of America
Scharf, T.	AREVA NP, Germany

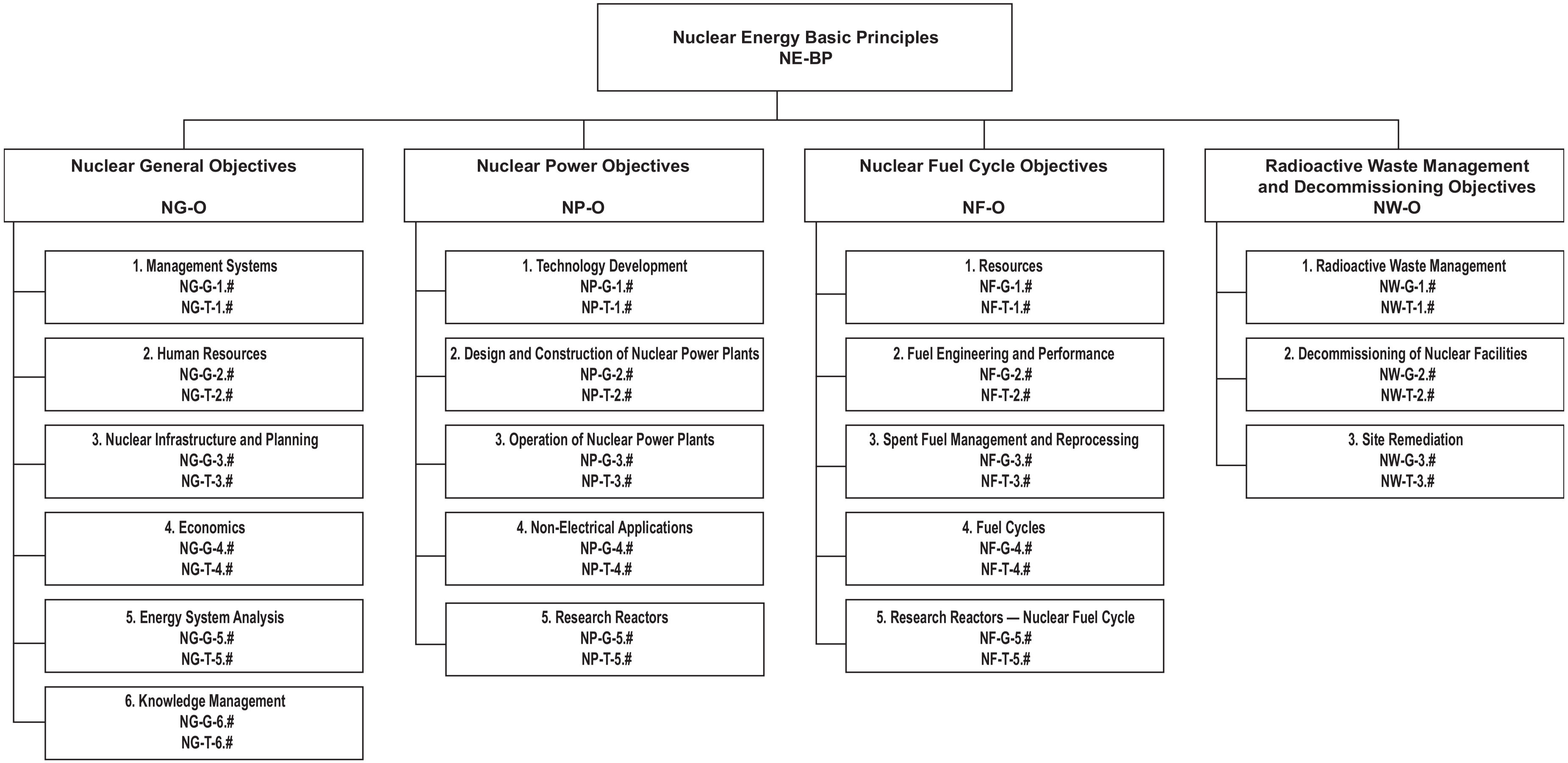
Consultants Meetings

Vienna, Austria: 13–16 March 2006
Vienna, Austria: 16–18 April 2007
Vienna, Austria: 25–28 November 2008

Technical Meeting

Toronto, Canada: 28 October–3 November 2007

Structure of the IAEA Nuclear Energy Series



Nuclear Energy Basic Principles
NE-BP

Nuclear General Objectives
NG-O

1. Management Systems
NG-G-1.#
NG-T-1.#

2. Human Resources
NG-G-2.#
NG-T-2.#

3. Nuclear Infrastructure and Planning
NG-G-3.#
NG-T-3.#

4. Economics
NG-G-4.#
NG-T-4.#

5. Energy System Analysis
NG-G-5.#
NG-T-5.#

6. Knowledge Management
NG-G-6.#
NG-T-6.#

Nuclear Power Objectives
NP-O

1. Technology Development
NP-G-1.#
NP-T-1.#

2. Design and Construction of Nuclear Power Plants
NP-G-2.#
NP-T-2.#

3. Operation of Nuclear Power Plants
NP-G-3.#
NP-T-3.#

4. Non-Electrical Applications
NP-G-4.#
NP-T-4.#

5. Research Reactors
NP-G-5.#
NP-T-5.#

Nuclear Fuel Cycle Objectives
NF-O

1. Resources
NF-G-1.#
NF-T-1.#

2. Fuel Engineering and Performance
NF-G-2.#
NF-T-2.#

3. Spent Fuel Management and Reprocessing
NF-G-3.#
NF-T-3.#

4. Fuel Cycles
NF-G-4.#
NF-T-4.#

5. Research Reactors — Nuclear Fuel Cycle
NF-G-5.#
NF-T-5.#

Radioactive Waste Management and Decommissioning Objectives
NW-O

1. Radioactive Waste Management
NW-G-1.#
NW-T-1.#

2. Decommissioning of Nuclear Facilities
NW-G-2.#
NW-T-2.#

3. Site Remediation
NW-G-3.#
NW-T-3.#

Key

BP:	Basic Principles
O:	Objectives
G:	Guides
T:	Technical Reports
Nos. 1-6:	Topic designations
#:	Guide or Report number (1, 2, 3, 4, etc.)

Examples

NG-G-3.1:	Nuclear General (**NG**), **G**uide, Nuclear Infrastructure and Planning (topic **3**), **#1**
NP-T-5.4:	Nuclear Power (**NP**), Report (**T**), Research Reactors (topic **5**), **#4**
NF-T-3.6:	Nuclear Fuel (**NF**), Report (**T**), Spent Fuel Management and Reprocessing, **#6**
NW-G-1.1:	Radioactive Waste Management and Decommissioning (**NW**), **G**uide, Radioactive Waste (topic **1**), **#1**

IAEA
International Atomic Energy Agency

Where to order IAEA publications

In the following countries IAEA publications may be purchased from the sources listed below, or from major local booksellers. Payment may be made in local currency or with UNESCO coupons.

AUSTRALIA
DA Information Services, 648 Whitehorse Road, MITCHAM 3132
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

BELGIUM
Jean de Lannoy, avenue du Roi 202, B-1190 Brussels
Telephone: +32 2 538 43 08 • Fax: +32 2 538 08 41
Email: jean.de.lannoy@infoboard.be • Web site: http://www.jean-de-lannoy.be

CANADA
Bernan Associates, 4501 Forbes Blvd, Suite 200, Lanham, MD 20706-4346, USA
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: customercare@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 1-5369 Canotek Rd., Ottawa, Ontario, K1J 9J3
Telephone: +613 745 2665 • Fax: +613 745 7660
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

CHINA
IAEA Publications in Chinese: China Nuclear Energy Industry Corporation, Translation Section, P.O. Box 2103, Beijing

CZECH REPUBLIC
Suweco CZ, S.R.O., Klecakova 347, 180 21 Praha 9
Telephone: +420 26603 5364 • Fax: +420 28482 1646
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FINLAND
Akateeminen Kirjakauppa, PO BOX 128 (Keskuskatu 1), FIN-00101 Helsinki
Telephone: +358 9 121 41 • Fax: +358 9 121 4450
Email: akatilaus@akateeminen.com • Web site: http://www.akateeminen.com

FRANCE
Form-Edit, 5, rue Janssen, P.O. Box 25, F-75921 Paris Cedex 19
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: formedit@formedit.fr • Web site: http://www. formedit.fr

Lavoisier SAS, 145 rue de Provigny, 94236 Cachan Cedex
Telephone: + 33 1 47 40 67 02 • Fax +33 1 47 40 67 02
Email: romuald.verrier@lavoisier.fr • Web site: http://www.lavoisier.fr

GERMANY
UNO-Verlag, Vertriebs- und Verlags GmbH, Am Hofgarten 10, D-53113 Bonn
Telephone: + 49 228 94 90 20 • Fax: +49 228 94 90 20 or +49 228 94 90 222
Email: bestellung@uno-verlag.de • Web site: http://www.uno-verlag.de

HUNGARY
Librotrade Ltd., Book Import, P.O. Box 126, H-1656 Budapest
Telephone: +36 1 257 7777 • Fax: +36 1 257 7472 • Email: books@librotrade.hu

INDIA
Allied Publishers Group, 1st Floor, Dubash House, 15, J. N. Heredia Marg, Ballard Estate, Mumbai 400 001,
Telephone: +91 22 22617926/27 • Fax: +91 22 22617928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell, 2/72, Nirankari Colony, Delhi 110009
Telephone: +91 11 23268786, +91 11 23257264 • Fax: +91 11 23281315
Email: bookwell@vsnl.net

ITALY
Libreria Scientifica Dott. Lucio di Biasio “AEIOU”, Via Coronelli 6, I-20146 Milan
Telephone: +39 02 48 95 45 52 or 48 95 45 62 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Website: www.libreriaaeiou.eu

JAPAN

Maruzen Company, Ltd., 13-6 Nihonbashi, 3 chome, Chuo-ku, Tokyo 103-0027
Telephone: +81 3 3275 8582 • Fax: +81 3 3275 9072
Email: journal@maruzen.co.jp • Web site: http://www.maruzen.co.jp

REPUBLIC OF KOREA

KINS Inc., Information Business Dept. Samho Bldg. 2nd Floor, 275-1 Yang Jae-dong SeoCho-G, Seoul 137-130
Telephone: +02 589 1740 • Fax: +02 589 1746 • Web site: http://www.kins.re.kr

NETHERLANDS

De Lindeboom Internationale Publicaties B.V., M.A. de Ruyterstraat 20A, NL-7482 BZ Haaksbergen
Telephone: +31 (0) 53 5740004 • Fax: +31 (0) 53 5729296
Email: books@delindeboom.com • Web site: http://www.delindeboom.com

Martinus Nijhoff International, Koraalrood 50, P.O. Box 1853, 2700 CZ Zoetermeer
Telephone: +31 793 684 400 • Fax: +31 793 615 698
Email: info@nijhoff.nl • Web site: http://www.nijhoff.nl

Swets and Zeitlinger b.v., P.O. Box 830, 2160 SZ Lisse
Telephone: +31 252 435 111 • Fax: +31 252 415 888
Email: infoho@swets.nl • Web site: http://www.swets.nl

NEW ZEALAND

DA Information Services, 648 Whitehorse Road, MITCHAM 3132, Australia
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: service@dadirect.com.au • Web site: http://www.dadirect.com.au

SLOVENIA

Cankarjeva Zalozba d.d., Kopitarjeva 2, SI-1512 Ljubljana
Telephone: +386 1 432 31 44 • Fax: +386 1 230 14 35
Email: import.books@cankarjeva-z.si • Web site: http://www.cankarjeva-z.si/uvoz

SPAIN

Díaz de Santos, S.A., c/ Juan Bravo, 3A, E-28006 Madrid
Telephone: +34 91 781 94 80 • Fax: +34 91 575 55 63
Email: compras@diazdesantos.es, carmela@diazdesantos.es, barcelona@diazdesantos.es, julio@diazdesantos.es
Web site: http://www.diazdesantos.es

UNITED KINGDOM

The Stationery Office Ltd, International Sales Agency, PO Box 29, Norwich, NR3 1 GN
Telephone (orders): +44 870 600 5552 • (enquiries): +44 207 873 8372 • Fax: +44 207 873 8203
Email (orders): book.orders@tso.co.uk • (enquiries): book.enquiries@tso.co.uk • Web site: http://www.tso.co.uk

On-line orders
DELTA Int. Book Wholesalers Ltd., 39 Alexandra Road, Addlestone, Surrey, KT15 2PQ
Email: info@profbooks.com • Web site: http://www.profbooks.com

Books on the Environment
Earthprint Ltd., P.O. Box 119, Stevenage SG1 4TP
Telephone: +44 1438748111 • Fax: +44 1438748844
Email: orders@earthprint.com • Web site: http://www.earthprint.com

UNITED NATIONS

Dept. I004, Room DC2-0853, First Avenue at 46th Street, New York, N.Y. 10017, USA
(UN) Telephone: +800 253-9646 or +212 963-8302 • Fax: +212 963-3489
Email: publications@un.org • Web site: http://www.un.org

UNITED STATES OF AMERICA

Bernan Associates, 4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4346
Telephone: 1-800-865-3457 • Fax: 1-800-865-3450
Email: customercare@bernan.com · Web site: http://www.bernan.com

Renouf Publishing Company Ltd., 812 Proctor Ave., Ogdensburg, NY, 13669
Telephone: +888 551 7470 (toll-free) • Fax: +888 568 8546 (toll-free)
Email: order.dept@renoufbooks.com • Web site: http://www.renoufbooks.com

Orders and requests for information may also be addressed directly to:

Marketing and Sales Unit, International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 (or 22530) • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

10-31701

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–107710–3
ISSN 1995–7807