Safety Reports Series

No.6

SAFETY ISSUES FOR ADVANCED PROTECTION, CONTROL AND HUMAN–MACHINE INTERFACE SYSTEMS IN OPERATING NUCLEAR POWER PLANTS

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

AFGHANISTAN
ALBANIA
ALGERIA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
BANGLADESH
BELARUS
BELGIUM
BOLIVIA
BOSNIA AND HERZEGOVINA
BRAZIL
BULGARIA
BURKINA FASO
CAMBODIA
CAMEROON
CANADA
CHILE
CHINA
COLOMBIA
COSTA RICA
COTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ESTONIA
ETHIOPIA
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
LATVIA
LEBANON
LIBERIA
LIBYAN ARAB JAMAHIRIYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITIUS
MEXICO
MONACO
MONGOLIA
MOROCCO
MYANMAR
NAMIBIA
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
PAKISTAN
PANAMA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
SAUDI ARABIA
SENEGAL
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
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
VIET NAM
YEMEN
YUGOSLAVIA
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".

Printed by the IAEA in Austria
November 1998
STI/PUB/1057

SAFETY REPORTS SERIES No. 6

SAFETY ISSUES FOR ADVANCED PROTECTION, CONTROL AND HUMAN–MACHINE INTERFACE SYSTEMS IN OPERATING NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 1998

VIC Library Cataloguing in Publication Data

Safety issues for advanced protection, control and human machine interface systems in operating nuclear power plants. — Vienna : International Atomic Energy Agency, 1998.
p. ; 24 cm. — (Safety reports series, ISSN 1020-6450 ; no. 6)
STI/PUB/1057
ISBN 92-0-104598-0
Includes bibliographical references.

1. Nuclear power plants—Safety measures. 2. Human–computer interaction. I. International Atomic Energy Agency. II. Series.

VICL 98-00208

FOREWORD

There exists an abundance of codes and standards associated with the application of digital instrumentation and control (I&C) technology in nuclear power plants. However, there is no clear consensus among suppliers and plant operators on how to present safety and reliability requirements nor among regulatory authorities on how to review and approve applications for retrofitting of digital I&C in operating plants. The cost uncertainty resulting from the delay that inevitably occurs when a regulatory body has to deal with new technology has made many nuclear plants either avoid the licensing process or delay upgrade projects. It is therefore important to identify the safety concerns and issues and to develop a clear procedure for review and approval by licensing authorities.

This Safety Report identifies and describes safety and licensing issues reflecting international experience and practices and offers good practices and effective safety approaches to I&C retrofits in operating nuclear power plants.

The report is intended for engineers, managers, researchers, developers and planners involved in upgrading protection, control and human–machine interface systems in nuclear power plants. The IAEA staff member responsible for this publication is M. Dusic of the Division of Nuclear Installation Safety.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Instrumentation and control (I&C) technology has advanced more rapidly than any other discipline that is important to a nuclear power plant (NPP). State of the art I&C systems can in most ways, especially functionally, outperform their predecessors of only a few years ago. The new systems can carry out complex control functions in a more intelligent and more precise way and provide analysed status information, while being more reliable and more economical [1–4]. Modern I&C systems take full advantage of both analog and digital capabilities to create a hybrid technology. It is this powerful technology that both nuclear and non-nuclear industries are designing into new plants and retrofitting into existing plants.

Creating a modern I&C system for new plants can be compared to designing a building to fit a specific site. By contrast, backfitting a modern I&C system to existing plants can be compared to renovating an existing structure. Both cases require creative endeavours, but the design of a new structure is clearly easier. The key issue facing operating NPPs in the quest to take advantage of modern I&C technology relates to the capability of renovating the existing structure as well as creating a new structure in harmony with it [1, 4–6].

NPPs worldwide are being driven to upgrade their existing I&C equipment, including protection, control and human–machine interface systems and components [1, 7]. The need for upgrades is being driven primarily by the growing problems with existing systems of obsolescence, lack of spares and increased maintenance costs. Existing analog systems are becoming increasingly obsolete and difficult to support as manufacturers discontinue their supply of replacement analog electronic equipment. There is great incentive to take advantage of modern technologies which offer potential performance and reliability improvements [2, 3, 6, 8].

Both industry and regulatory bodies have recognized the importance of upgrades and the introduction of advanced I&C systems [9–12]. Modern systems offer the potential to provide greater availability through the use of reliable components and features such as automatic self-testing, diagnostics and calibration. When properly implemented, upgrades with advanced I&C technology can enhance the safety and performance of operating plants [4, 9, 13, 14].

There are numerous examples of the implementation of advanced I&C technologies in NPPs throughout the world [1, 15]. Large scale integrated advanced I&C systems have been applied in new plants, including Darlington (Canada), Sizewell B (United Kingdom), Chooz B (France) and Kashiwasaki (Japan). However, the

approaches and the concerns related to the implementation of advanced technologies in new plants are very different from those for backfits to existing operating plants, as exemplified by the computerized protection system at Dungeness B (UK), the advanced information systems in German plants, the digital control computer upgrade at Bruce A (Canada), and the many control and protection upgrades in plants in the United States of America.

This report addresses specifically the safety approaches used for the implementation of advanced I&C systems in operating plants and the use of this technology in new plants. It treats software and hardware together at the 'system' level, and does not offer any separate guidance on, for example, software development and licensing. Detailed information on these subjects can be found in other publications [15–24].

1.2. OBJECTIVES

The report addresses advanced protection, control and human–machine interface systems with the objectives of:

— Identifying and addressing safety and licensing issues,
— Bringing together international experience and practice in safety evaluation and regulation,
— Promoting good practices and effective safety approaches for planning and performing retrofits in operating NPPs.

The report is intended to be of interest to engineers, managers, researchers, developers and planners involved in upgrading the protection, control and human–machine interface systems in NPPs.

1.3. SCOPE

International experience and published information [10, 13, 15, 25, 26] have enabled many of the safety issues arising from the use of advanced technology and its impact on the human–machine interface to be addressed. These issues include reliability, common mode failures, environmental qualification, qualification of commercial hardware and software, quality assurance and configuration management as well as human factors, plant procedures and training.

This report describes methodologies and approaches to address these safety issues in relation to digital I&C. In addition, it illustrates the life cycle process for advanced systems in NPPs, consisting of design basis re-engineering analysis, architecture analysis for new systems, comparison with design basis, design requirements

and specifications, detailed design, implementation, acceptance testing, installation, commissioning, operation and maintenance.

The licensing framework for addressing digital I&C and the relevant codes and standards are discussed. The report also provides a set of definitions associated with advanced protection, control and human–machine interface systems and classifies them with respect to their safety relevance.

1.4. STRUCTURE

Section 2 of the report introduces the terminology of the relevant parameters and functions and classifies systems with respect to their safety relevance.

Section 3 describes the safety issues of advanced systems while Section 4 deals with the methodologies used to address the safety issues associated with digital I&C.

Section 5 considers safety approaches for the human–machine interface, with emphasis on human performance, the human factors design process, procedures, human factors evaluation and training. Section 6 addresses the safety aspects of the upgrade process and illustrates the life cycle process for the application of advanced systems in NPPs.

2. SAFETY CATEGORIZATION AND STANDARDS

2.1. TERMINOLOGY

This section introduces the means of categorizing safety functions and systems according to their safety significance, and identifies the relevant international standards such as those of the International Electrotechnical Commission (IEC) and the Institute of Electronic and Electrical Engineers (IEEE).

The terminology used in this section is derived from IAEA [1, 26, 27], IEC [16] and IEEE [25] publications and is detailed in the Glossary.

2.2. TYPES OF FUNCTION

Many of the functions that must be performed to ensure the efficient operation of an NPP are directly or indirectly associated with plant safety. A safety function can

be defined as an action that must be accomplished to ensure safety in an NPP. The safety functions are carried out by various systems in the plant, including the I&C systems. Depending on the nature of these functions, they can be identified as being of the following types:

— Protection function,
— Control function,
— Monitoring and display function,
— Testing function.

2.2.1. Protection function

The protection function provides the first line of defence against failures in the plant. The most critical safety functions relate directly to nuclear safety in terms of protecting the personnel and the public in the event of a serious process failure.

The protection functions are primarily provided by: the reactor protection or shutdown system, which trips the reactor and maintains it in a subcritical state; the emergency coolant injection system, which provides the core cooling, removes decay heat and provides the heat sink; and the containment system, which provides isolation to retain radioactivity released in the plant. In addition, emergency protection functions are provided by, for example, the emergency feedwater cooling or boiler cooling system and the fire protection system.

Because of the high reliability requirements and significant safety impact, the systems providing protection functions should be as simple as possible and their qualification needs to be to the highest level. These systems therefore exhibit features such as redundancy and diversity and provisions to ensure good testability and maintainability.

2.2.2. Control function

The control function provides assurance that the plant is controlled and kept within its operating envelope under both normal and abnormal conditions. The control function can also provide mitigation of the effects of plant transients or postulated initiating events, thereby contributing to nuclear safety by minimizing the demand on protection functions.

The control functions are provided primarily by the various process control systems in the nuclear steam supply system. Typically, they include: reactor control or power regulation; primary heat transport or coolant control; steam generator or secondary heat sink control; feedwater control or secondary coolant control; and fuel handling control. Other important control functions are those relating to service water, electric power, air conditioning, ventilation and radioactive emissions.

2.2.3. Monitoring and display function

The monitoring and display function provides the interface between the plant and the operations and maintenance personnel. This function is important to safety as it allows the plant personnel to intercept transients and maintain the plant within the safe operating envelope. There are many dedicated systems in the plant, including the safety system monitoring computers which provide information about the plant safety margins and the state of safety equipment during normal and abnormal conditions. The monitoring and display functions also provide alarms and annunciation to the operators. These functions are also needed for emergency control during a post-accident period to provide warning of the onset of problems. The monitoring and display function also provides important information for conducting maintenance activities, particularly preventive and remedial maintenance.

2.2.4. Testing function

The testing function provides assurance of the availability and effectiveness of the safety functions provided by the I&C systems and confirms that they are not degraded. Testing is carried out to demonstrate the functionality of the various protection, control, and monitoring and display systems. For digital I&C systems, it is very important that provision be made for automated testing of safety functions. The testing function may include self-checking or automatic testing, routine testing and periodic calibration.

2.3. SAFETY CATEGORIZATION

The level of development, review and safety assessment applied to the production and implementation of a new I&C system will depend upon the safety impact of its function on the plant. Thus it is important to be able to determine that the most suitable technology and practices have been selected. The IAEA Safety Code 50-C-D [28] establishes criteria for the categorization of major systems, introducing the concepts of safety systems and safety related systems. Safety Guides 50-SG-D3 [29] and 50-SG-D8 [26] develop the requirements for these systems. The safety criteria outlined in these IAEA publications have also been used to develop the IEC standard, IEC 1226, which categorizes I&C functions and associated systems and equipment as being of significance A, B, C or D (in decreasing order) [30]. The criterion for assigning a function to a particular category is set out in the standard in terms of the safety significance of the function.

Other methods of categorization of functions and systems are being developed. These are frequently based on qualitative criteria and a quantitative

assessment of nuclear risk. A method which focuses on target reliability is described in Ref. [21].

2.3.1. Category A: Safety critical functions

Category A denotes functions and associated systems and equipment (FSE) which are critical for the achievement and maintenance of NPP safety. The successful performance of these functions prevents an initiating event from leading to a significant sequence of events, or mitigates the consequences of these events. Systems for Category A functions will also have high quality assurance and reliability requirements and therefore limited functionality.

Typically, Category A functions are provided for: safe shutdown of the reactor, removal of heat from the core and containing or limiting the consequences of an accident condition.

2.3.2. Category B: Safety related functions

Category B FSE have a supporting role to Category A functions. Category B may complement the performance of a Category A function in mitigating an initiating event so that plant or equipment damage or activity release may be avoided or minimized. The failure of systems for Category B functions could lead to or increase the severity of an initiating event, or cause degradation in the performance of a mitigating system. However, the accident sequence can be terminated and the consequences mitigated by the Category A system. Category B FSE will have a lower level of safety significance than Category A and the safety requirements of Category B need not be as high as those of Category A. The Category B FSE may have a higher level of functionality, a lower level of reliability and lower quality assurance requirements than Category A FSE.

Typically, Category B includes: control of nuclear processes such as the reactor, the heat transport system, fuel handling and the boilers; control of the emergency support services (e.g. water and power); and control and monitoring of radioactivity emission.

2.3.3. Category C: Safety support or auxiliary functions

Category C functions or systems play an auxiliary or indirect role in the achievement and maintenance of nuclear safety. Category C FSE can affect nuclear safety, but in a less significant way than Category A or Category B. They can play a part in the response to an accident, but are not directly involved in mitigating the consequences of the accident.

Typically, Category C includes control of conventional systems such as the turbine and the feedwater, various monitoring systems, plant display systems, alarm and

annunciation systems, radwaste and area radiation monitoring systems, access control systems and emergency communication systems.

2.3.4. Category D: Non-safety or other functions

Category D involves functions or systems which do not fall under any of the above categories because they have no effect on nuclear safety. However, they are important for plant operation and maintenance. Although Category D FSE usually require the lowest level of quality assurance, reliability requirements relating to factors other than nuclear safety (e.g. production, availability and personnel safety) may justify a higher level.

Typically, Category D FSE will include the I&C for many of the conventional systems, including, for example, the generators, condensers and water treatment systems.

2.4. CODES AND STANDARDS

Examples of comprehensive sets of documents relating to the safety of NPPs are provided by the IAEA Safety Standards and supporting Safety Guides. These cover the establishment of legal structures [31], plant siting [32], plant design [26, 28, 29, 33] and plant operation [34] and also the subject of quality assurance [27]. These publications set requirements and make recommendations on how to fulfil them.

IAEA Technical Reports and IAEA-TECDOCs provide practical information on technical methods. Publications on I&C systems include computer based systems [15, 35, 36], operator support [3] and maintenance [1]. Many IAEA-TECDOCs address the safety of advanced systems as related to the use of computers [2, 4, 5], operations [1], and control room design and operator support [6, 7, 13, 14].

There is an extensive body of technical standards available to support the development and deployment of I&C systems for nuclear power plants. The IEC Technical Committee 45 (Nuclear Instrumentation) produces nuclear sector specific standards which, by agreement, are consistent with those of the IAEA. The standards vary from the general [37] to the very specific [38]. The preparation of standards for advanced systems is currently under way, notably for computer based systems and control room design.

Most advanced systems use programmed digital and computer based devices. Standards for programmed digital equipment (e.g. programmable logic devices and programmable gate arrays) have not received much attention from the nuclear industry. Nuclear sector specific standards include: IEC-880 [16] on software for computers in the safety systems of nuclear power stations, and IEC-987 [39] on digital computers important to safety for NPPs.

The IEEE has also published widely on these subjects, although not necessarily specifically for the nuclear sector. Their standards include: IEEE 830 [18], a guide to software requirements specification, IEEE 1008 [19] on software testing, and IEEE 1012 [20] on software verification and validation plans. The nuclear sector standards contain material specific to the demonstration of safety, while other sector standards do not. The standards differ from those associated with conventional technologies (e.g. analog electronics), as the process is subject to a much greater level of structured description.

An important standard for digital I&C equipment in nuclear power is ANSI/IEEE/ANS 7-4.3.2 [25], which provides criteria for the use of digital computers in the safety systems of nuclear power generating stations. The standard covers a wide range of subject areas relevant to digital I&C systems, including: quality, equipment qualification, system integrity, independence, test and calibration, information display, human factors considerations, diversity, electromagnetic compatibility, qualification of commercial computers, verification and validation, and computer reliability.

An international standard which has received wide acceptance for computer software in NPP safety systems is IEC 880 [16]. This is a detailed standard specific to the nuclear sector which can be used as a basis for software development. It describes the software development and maintenance life cycle process, including: software requirements definition, development, verification, hardware and software integration, system validation, maintenance and operation. The standard provides a practical guide for the planning, managing and development of the software for digital I&C systems.

Material available on control room design includes IEC 960 [40], IEC 964 [41] and IEC 1227 [42], and there are a number of additional standards on the verification and validation of design and the application of visual display units (IEC 1771 [43] and IEC 1772 [44]). In many cases the practice is to supplement this material with project/company specific documents that refine the principles and cover omissions in the standards. This use of project/company specific material for the application of expert systems, neural networks and advanced control techniques is widespread.

Finally, while it has been recognized that the use of computers in safety systems gives rise to safety issues, little attention has been given to technologies such as programmable field gate arrays, programmable logic devices and application specific integrated circuits. Inherent to equipment using these devices are design complexity and discrete behaviour, which are regarded as two of the issues giving rise to safety concerns in the case of computers. Consequently, standards and safety practices are needed to help ensure that safety is maintained.

3. SAFETY ISSUES OF ADVANCED SYSTEMS

3.1. SAFETY AND RELIABILITY

The introduction of an advanced system is intended to enhance or maintain levels of safety while avoiding potentially unsafe or unreliable conditions [10]. Reliability is an important safety goal and reliability targets need to be met by the advanced system. These targets may be specified in terms of unavailability and spurious actuations per year. Questions are being raised about the adequacy of the methods currently being used to assess the safety and reliability of digital systems in NPPs. The safety community is seeking to ensure an appropriate balance between probabilistic safety assessment (PSA) and deterministic approaches.

The process of I&C upgrade includes estimates of reliability, assessment of safety margins, comparison with quantitative safety goals and overall assessment of safety. When qualitative or quantitative reliability goals are required, it is necessary to demonstrate that these goals (including those for the software, the hardware and the human–machine interface) have been met. The method used for determining reliability may include combinations of analysis, field experience or testing. Software error recording and trending may also be used in this connection.

Validation of the reliability and PSA models is an important issue. It becomes even more important if the PSA models are being used for day to day plant operation and maintenance and as input to the decision making process for plant modification.

The defence in depth safety principle applies to advanced systems and may be enhanced through the introduction of such systems. Care needs to be taken in the design process to ensure the availability of diverse and independent means to provide barriers against common mode failure.

3.2. COMMON MODE FAILURES

There is considerable concern that a line of defence provided by a system containing redundant channels might be defeated by a common mode failure leading to the simultaneous failure of all channels [10, 25]. The means of providing defence against common mode failures and ensuring reliability are well established for hard-wired analog I&C systems. They include:

— Redundancy, to meet the single failure criterion, coupled with voting enhanced reliability;

— Separation, isolation and independence of redundant trains and their allocated supply and auxiliary systems, to meet the requirement that the system should not be compromised by hardware common mode failures resulting from external events, e.g. fire and flood;
— Functional diversity, to meet the requirement for protection against common mode failures caused by errors in the basic safety system specification and implementation, as well as errors in software design or coding.

The introduction of computer based I&C systems has resulted in emphasis being placed on software common mode failures arising from design defects. The main issue arises from the fact that because of the discrete nature of the behaviour of the hardware and associated software, a random data constellation (input data and stored data) will not necessarily trigger a failure in the task processing on the system although it takes a trajectory close to a fault. The scale of the problem is increased by the existence of unintended or unused functions in the software (e.g. development aids or subfunctions in commercial grade software), which could be activated by an untested data constellation.

3.3. ENVIRONMENTAL QUALIFICATION

Environmental qualification has been a mandatory requirement for both new plants and modifications to existing plants [45]. The environmental qualification requirements for advanced I&C systems are similar to those for conventional equipment since it is necessary to demonstrate that the equipment can withstand the design basis accidents, including main steam line breaks and loss of coolant accidents. The equipment needs to be qualified for the steam, humidity, temperature and radiation environment pertaining during normal and accident conditions. In addition, other environmental factors such as seismic events, chemical corrosion, electromagnetic fields, power quality, grounding and smoke have also to be considered. Most electronic systems are unsuitable for prolonged use in radiation environments and the memory and processor chips cannot survive for long periods in high temperature and high humidity environments.

Modern electronics operate at lower voltages and are more likely to be at risk from electromagnetic interference (EMI), radiofrequency interference (RFI) and electrical noise present in the plant environment [9]. A demonstration is required to show that new equipment does not act as a source of electrical noise, EMI and RFI, or adversely affect existing equipment in the plant. Modern instrumentation uses a variety of new materials, optical fibre and magnetic or optical storage media, whose ageing properties and resistance to chemical corrosion will need to be determined. There is little experience of the behaviour of these new components and the standards for testing them are still being developed.

Issues relating to the life cycle management of the plant have to be considered and those for advanced digital systems include meeting the plant life assurance requirements for: shelf life, service life, the provision of spares, testing, inspection and maintenance. In the management of ageing it is necessary to ensure that the plant life is not compromised by unexpected ageing of the I&C systems.

3.4. HUMAN–MACHINE INTERFACE

A major concern when introducing new information systems into an operating NPP is the ability of humans to adapt to the new technology and to operate with mixed technologies while preserving a high safety standard. The ultimate goal is to improve safety by providing better displays which combine information from different sources, perform data processing and prioritize and highlight information essential to the operators [46].

Human–machine interactions are complex. In many applications the role of the human operator is neglected in design and the human functions are defined by default, governed by the limitations in hardware and software. It is questionable whether the role defined in this manner for the human operators can be effectively and reliably performed. For example:

— Is the information presented at a sufficiently high level of aggregation/ abstraction to support human decision making?
— Does the information integration and extraction impose additional cognitive burdens?
— Are the displays readable?
— Is the information readily accessible?

For digital I&C systems to be successfully applied to NPPs, the design needs to properly account for the role of humans in using and maintaining these systems. Operator involvement in system design and factory acceptance testing is essential to ensure that existing operational practices are adhered to and that weaknesses are detected at an early stage in the design process.

The issues to be addressed include how the new systems will affect the operator's role (shift of tasks), the method of information presentation, the ways in which the operator interacts with the system and the requirements on the operator to understand the system. Special attention needs to be paid to: possible problems of integration with existing control room systems such as conflicts between information presented on conventional panels and new displays, addressing devices, physical lay-outs, time responses, colour coding and shapes.

New systems may partially support existing operational and emergency procedures and an analysis needs to be made of whether this puts additional requirements on the system. Furthermore, the new system may require new procedures for maintenance, testing and calibration. Training of operators and maintenance staff also needs to be considered.

Operators are sometimes conservative and reluctant to accept technology changes. To avoid problems with user acceptance, a verification and validation programme has to be prepared to ensure adequate testing of the new human–machine interface. Dynamic testing and validation in training simulators may reveal possible problems before installation. The influence of the system on the whole organization needs to be evaluated.

3.5. QUALIFICATION OF COMMERCIAL HARDWARE AND SOFTWARE

The term 'commercial grade item' is used to cover hardware or software which has not necessarily been designed according to specific NPP performance requirements. It is often desirable to take advantage of these systems, which usually have a long history of development and a large number of applications. In principle the qualification requirements for commercial hardware and software used in advanced systems are no different to those for bespoke systems [9, 10, 25].

A method for completing the qualification of commercial equipment that takes advantage of its prior use has not been fully established. The current method is for the utility and the regulators to agree on an approach on a case by case basis. Information on approaches for dealing with such commercial off-the-shelf software can be found in Refs [15, 47].

3.6. QUALITY ASSURANCE

Quality assurance is applicable to both advanced and traditional technology and covers the whole process of I&C upgrade comprising hardware, software and human factors. A proper system design identifies software components, hardware components and human operators, and allocates requirements and constraints to each. Specific recommendations regarding quality assurance for safety in NPPs can be found in Ref. [27].

Problems may arise if the hardware and software development process is not co-ordinated throughout the various phases of a project. The limitations introduced by, and requirements of, human operators are often neglected in the early phase of the project and this may cause problems if additional requirements stipulated by the user have to be introduced at a later stage in the development process.

The use of software is the principal difference between digital and analog I&C systems. A number of failures in digital I&C systems caused by software quality problems have been reported. The development process may be difficult to trace if tests, reviews and audits are insufficiently documented.

For safety critical software, the safety analysis is particularly important in demonstrating that the system is safe when the software operates both as intended and in the presence of abnormal conditions and events, both external to the safety system and internal to the computer hardware or software.

The verification and validation of tools, compilers, operating systems and commercial grade software deserve special attention. Configuration control and testing procedures for such software need to be handled properly to avoid the introduction of new failures when changes to new versions are made [36].

3.7. CONFIGURATION MANAGEMENT

The issues of configuration management and change control relating to advanced systems are addressed as a part of plant configuration management used to provide assurance that the plant operates within its safe operating envelope. Configuration management is an integrated process that extends through the life cycle of the plant. It identifies and documents the physical and functional characteristics of NPP structures, systems and components, including digital hardware and software. It also includes change control and ensures that changes to the above characteristics are properly controlled through a process of development, assessment, approval, implementation, verification, recording and incorporation in the NPP documentation [1, 10].

There are two aspects of configuration management and change control which need to be carefully considered. The first concerns the plant reconfiguration prior to installation of the advanced equipment. The second, equally important, concerns changes introduced through software changes.

3.8. LICENSING CONSIDERATIONS

The licensing procedures and practices followed in the backfitting of protection, control and human–machine interface systems are dictated by national legislation and in every case the licensing body must consent to the use of the system. Many of the national requirements are common to all countries. For example, it is required that the operator of the plant, the licensee, be solely responsible for plant safety and it is the licensee that must demonstrate that the plant is safe to operate. The technical interpretation of these requirements and the associated technical issues are

largely common to all approaches to safety and licensing. For well established technologies, the identification, interpretation and resolution of these issues have been widely discussed and consensus has been reached and has been published in standards and safety guides.

The content of the licensee's safety justification has to be agreed with the appropriate licensing body and will be set on a national basis. However, it would be expected to contain:

— A description of the plant and the process,
— Identification of the hazards posed by the plant,
— Identification of the consequences of events,
— An analysis showing how the events could occur,
— A description of the measures taken to prevent the events,
— A description of the facilities and measures to be taken to mitigate the consequences of the events.

The licensing body reviews the justification provided by the licensee to determine if it adequately demonstrates plant safety and compliance with the national requirements for operating a nuclear facility. The safety issues are thus as much about system justification and demonstration of compliance as about what requirements are to be complied with.

The general national legal framework is supplemented by guidance material and standards that set out the national practice for demonstrating compliance, for example the standard review plan NUREG-0800 [48] in the USA and the Tolerability of Risk from Nuclear Power Plants [49] and the Safety Assessment Principles [50] in the UK. The content of this guidance material has generally been produced with the assumption that the technology is well understood, the design and development practices are well established and justifications have been successfully produced for a number of years. For example, analog electronics are developed using standard components and are subjected to recognized forms of analysis and testing to demonstrate their operation. The justification of safety is usually achieved by completing a failure modes and effects analysis (FMEA) to show that the failure of any component will be apparent and the equipment taken into a known state. If the result of the FMEA is not satisfactory then further justification is required to show that safety would not be compromised. This approach is usually completed by arguments based on a combination of the use of redundancy and claims for reliability supported by in-service testing. This approach has allowed new plants to be built and existing systems to be upgraded with the minimum of risk as the technology and processes are well established.

The introduction of advanced systems has given rise to some difficulty in terms of the safety arguments. The problems arise from a combination of the com-

plexity of the systems and the use of emerging development processes and a novel technology. The former gives rise to problems of understanding and analysis. The latter is linked to the immaturity in demonstration because the development techniques and the failure modes of the hardware are not fully established and there is not necessarily an effective equivalent to the FMEA of the analog electrical circuit. The difficulty of providing an adequate demonstration of safety, and the resulting risk in selecting a new technology, have been most apparent for computer based systems. This has resulted in computer technology systems being slow to be accepted for wide application in safety systems despite the many operational advantages which have been demonstrated by successful applications in control and information systems.

Computer based technology is not the only advanced technology whose rate of deployment in nuclear plants has suffered. There is considerable reluctance to deploy large scale integrated circuits, in the form of general devices, application specific integrated circuits, or configurable devices such as PLDs and PGAs.

The development of advanced hardware has also been accompanied by significant theoretical developments (e.g. in control theory and signal processing), which can now be implemented using the hardware. Thus, the use of fuzzy control, expert systems for alarm handling, smart instrument and hybrid control rooms requires, in addition to justification of the computer software and hardware, justification of the application of the new theory and techniques. This is difficult, primarily because of the complexity of the applications.

The demonstration of the correctness of the delivered system and its compliance with requirements and standards is becoming increasingly dependent on the use of tools for analysis, testing and software generation, many of which are computer based. The correctness of the tools (which are usually more complex than their applications) needs to be justified in order that confidence can be placed in their output. The level of assurance required of the tools is also a subject of current debate.

In many safety applications the claim of safety enhancement can be hard to justify as the benefit of introducing an advanced system is usually operational — allowing the plant to be operated in a more flexible manner closer to its operating limits. The advanced systems often have better diagnostics and more sophisticated signal processing that allow faults to be detected earlier than is possible with conventional systems, and this is clearly a safety enhancement.

4. METHODOLOGIES TO ADDRESS SAFETY ISSUES

4.1. SAFETY AND RELIABILITY ASSESSMENT

4.1.1. Determination of safety significance

The conventional approach in designing a new plant is to develop the design and safety rationale and thereby identify the functions that are to be performed. Once identified, the safety significance of the functions is established by analysis following the approaches described in Section 2. The functions are then assigned to systems which might be conventional analog or advanced digital systems. In this process, due account must be taken of the other functions assigned to a given system and its interaction with other systems. Once functional assignment is complete, analysis is necessary to show that the safety objectives have been met.

The approach to a retrofit starts from a different position: there is already a set of functions implemented in one or more systems that are to be replaced. The process thus starts by re-engineering of the existing systems (see Section 6.1.1) to establish the functions that they perform, the safety significance of the functions and the safety constraints placed on them. The ease with which this exercise can be conducted will depend in part on the state of the system documentation. Caution must be exercised as even the best documented systems can contain undocumented functions and features.

Establishing the existing functions and their safety significance and constraints provides the baseline for the next step — the analysis of the current safety documents and requirements to ensure that any changes introduced since the original design are reflected in the new documentation and statement of safety significance.

The re-engineering process will need to take into account information from plant safety reports, licensing documentation and PSA models, design documents, operating documents, abnormal incident manuals and emergency operating procedures. Some of the issues which may be raised are:

— The plant systems involved;
— The interactions between the functions and the systems;
— The types of safety function (protection, mitigation, control, monitoring, testing);
— The reliability or availability requirements of the systems;
— The relevant initiating events;
— The frequency limits of the initiating events;
— Identification of failure modes and effects;

— Identification of possible effects for safety impacts;
— Identification of the most severe safety impact or worst case failure;
— Credit for mitigating factors, operator actions and system redundancy.

4.1.2. Requirements specification

The specification of requirements for an upgrade system is the first step in the life cycle process of the retrofitting project after the reverse engineering of the existing systems and is the main basis for system design and development. The requirements (hardware, software and human–machine interface components derived from the existing I&C functions, their associated human tasks and the existing procedures) are adapted to take account of the technology of the new system, and the safety and licensing issues as addressed in Section 3.

The requirements are the key to the life cycle quality assurance, and the specification of the requirements has to be precise. Good requirements adhere to the following principles [17]:

— Completeness — ensure that all necessary requirements are included;
— Unambiguity — ensure that requirements are interpreted the same way by all readers;
— Consistency — ensure that requirements do not conflict with each other;
— Verifiability — determine that a practical method exists to verify that each requirement is satisfied;
— Modifiability — ensure that requirements are easy to modify correctly;
— Traceability — determine that all components of the requirements can be traced to the system requirements and design;
— Readability — ensure that readers can easily read and understand all requirements.

The overall digital I&C system requirements should include [16]:

— Reliability requirements for the whole system;
— Requirements for human–machine interface during commissioning, startup, operation, testing and maintenance (for details, see Sections 5, 3.4 and 4.4);
— Constraints between hardware and software;
— Operability and maintainability requirements;
— Spare parts requirements;
— Qualification requirements;
— Environmental requirements;
— Training and documentation requirements.

4.1.3. Safety evaluations

Before a new I&C system is introduced into service in an NPP a safety evaluation has to be performed to:

— Check if the choice of technology is appropriate;
— Confirm that the system performs only the specified functions and executes them correctly;
— Ensure that the system meets targets for availability and spurious action;
— Ensure that the implementation respects constraints on independence;
— Verify that the implementation meets the applicable regulations;
— Determine the effect of the change on the plant's design and licensing basis;
— Demonstrate that the safety envelope is maintained and that the assumptions used in the safety analysis are still valid.

Before completion of the safety evaluation it is essential to ensure that a record is made of the following:

— Safety limits, limiting safety system settings and limiting control settings, with particular emphasis on the limits on important process variables which protect the integrity of the physical barriers that guard against the release of radioactivity;
— Limiting conditions for operation, such as the functional capabilities and performance levels of equipment required for safe operation of the facility;
— Surveillance (test, calibration, inspection) requirements;
— Design features such as channel accuracy and time response;
— Administrative controls, such as those related to organization and management, procedures, record keeping, and review and audit;
— Trip tolerances and safety assumptions data (e.g. instrument error, response time) in the safety analysis.

The records may include a list of any changes to original values resulting from the introduction of the new I&C.

4.1.4. Reliability, failure and hazards analysis

The approach used to determine the reliability of conventional analog systems consisting of discrete components and those with a low level of integration has been well established. It is assumed in this approach that system failures and hence the availability are dominated by random failures of the hardware. Systematic errors due

to failures in design are neglected as making an insignificant contribution to the overall failure rate.

Discussion of the reliability of an advanced computer based system should take into account the following:

— A significant contribution to failure may come from design errors in addition to random equipment failures;
— Software reliability assessment is qualitative and cannot easily be quantified statistically;
— Testing of functionality is not always practical because of the large number of tests necessary for low probabilities of failure;
— Human factors (e.g. human errors) are difficult to quantify.

The treatment of design errors and the assessment of software reliability are being dealt with through the use of software development processes that include activities designed to:

— Avoid the introduction of errors;
— Maximize the probability that once an error is introduced it will be found;
— Minimize the consequences of errors that were not found.

Unfortunately, these activities do not help produce a quantitative value for software reliability.

The purpose of failure analysis in the retrofitting of advanced I&C systems is to identify potential failures of the upgraded system or equipment, assess their significance and identify possible defences. Consideration of potential system failures is an integral part of the process of designing, specifying and implementing a digital upgrade. The failure analysis interacts with the main elements of the design process and provides the information needed to support the safety case and licensing evaluation [51].

The failure analysis of the system upgrade will include systematic treatment of:

(1) Identification of system level failures and their consequences in terms of:
— transient or accident initiators
— new types of failure not previously analysed
— challenges to safety systems
— safety system availability or probability of acting on demand
— spurious actions
— plant availability.

(2) Identification of potential causes of system failures by:
— failure modes and effects analysis (FMEA)
— fault tree analysis.

(3) Assessment of the significance of identified failures by:
— PSA, including the effect of failures in terms of activity release
— consideration of the probability of combination with other failures or events.

(4) Actions for resolution of identified failures by:
— disregarding failures that do not pose significant risk or warrant any further consideration
— modifying the upgrade design
— relying on existing systems and defence in depth to address the failure
— supplementing the defence in depth offered by existing systems, procedures and/or training such that the failure is adequately addressed.

Software hazards analysis is a method that will allow identification of:

— Hazards that could be caused by the software design requirements or specification;
— Hazardous conditions that could arise through postulated failures related to the final software design and implementation;
— Software or system design criteria that will eliminate or minimize control specific software related hazards.

The analysis provides a means of identifying combinations of allowed computer states or unforeseen failures that lead to hazardous computer outputs. This permits added safeguards to be introduced where necessary to ensure that unsafe states are not achievable. Recommendations for safeguards to mitigate the consequences of postulated failures are established in the light of the severity and likelihood of the failure, weighed against the complexity that would be introduced by implementing the safeguard. The FMEA can help to identify problems and mitigating safeguards at a component/module level.

The analysis that is carried out to identify failure modes associated with software involves three phases. The first phase focuses on the design of the system of which the software is a component, to identify the system level hazards attributable to software failure that will be assessed in the hazards analysis. The second phase focuses on the software design. In general, software design faults are avoided by reference to safety design principles and other design heuristics which are proven through experience to reflect good practice. The third phase involves an extension of the design analysis to identify failure modes that may be introduced in the development of the source code.

Software hazards analysis is performed within the context of the system design. However, such a detailed hazards analysis is labour intensive, even when tool support is used. Consequently it is not possible to complete the analysis for other than modules at a high level of abstraction. Engineering judgement is required to determine an optimal trade-off between the increase in complexity and the decrease in the specific hazard [51]. Nevertheless, it should be pointed out that formal documentation of FMEA and hazards analysis are often a licensing requirement for safety critical applications.

4.2. COMMON MODE FAILURE PROTECTION

I&C systems executing safety functions are generally designed with a redundant architecture to achieve fault tolerance and to meet the single failure criterion [9, 10]. However, redundancy provides no protection against common mode failures. The faults that lead to such failures are assumed to exist even in systems that have completed all tests for qualification and commissioning and are in long term stable operation. If triggered, these faults would lead to a 'timely correlated' malfunction (or even processor stop) in all redundant trains. 'Timely correlated' implies a time sequence too short for repair or correction but not necessarily simultaneity. This interpretation includes common cause failures and common mode failures.

The application of the defence in depth principle to digital I&C systems leads to the requirement for independently activated systems such that the independence of the safety functions is not violated by the global I&C system. Care is required in the design process to ensure that various barriers cannot be defeated by a common mode failure. Generally, a distinction is made between hardware failures (HW-CMFs) and software common mode failures (SW-CMFs).

4.2.1. Hardware common mode failures

The risk of HW-CMFs is minimized in the design of I&C systems. Defences against common mode failures due to stress from humidity and temperature, stress from seismic shock, stress from electromagnetic interference and surface voltage and lightning can be provided in the design and equipment set-up. The measures ensure that an accumulation of single failures can be excluded and an acceptable value for the mean time between failures (MTBF) achieved.

Special emphasis is placed on the design and construction of the auxiliary systems, for example those used to ensure a continuous power supply and adequate environmental conditions, and to ensure that plant internal incidents cannot lead to failure of more than one of the redundant hardware channels/trains at the same time.

This requirement involves independence of the redundant trains and can be satisfied by spatial separation and the allocation of each train to:

— separate equipment to ensure the appropriate environmental conditions (temperature, humidity, pressure),
— separate power supply.

In addition there should be electric isolation between the trains and other systems.

New I&C systems are generally installed in close proximity to existing equipment in the plant. Consequently the existing equipment is subject to a modified electromagnetic environment and careful attention needs to be paid to ensure that electromagnetic emission from the new equipment does not adversely affect the existing equipment. The use of fibre optics may be considered for transmission between new and old systems, remote auxiliary buildings and the central buildings, thus eliminating the problem of grounding and earth loops.

Many of the design measures proven by experience for analog I&C systems have the same relevance for excluding HW-CMFs from digital systems.

4.2.2. Software common mode failures

Any fault in an item of software can cause a failure and redundancy provides no defence. Consequently, any error or activity that can lead to a software fault needs to be viewed as causing a common mode failure.

Events which trigger a software fault to bring about a failure of an I&C system (SW-CMFs) are termed data constellations (a set of input and stored data which can be history dependent). It is generally accepted that it is not possible to exercise by testing all data constellations of a processor based I&C system's safety relevant functions. The following types of SW-CMF can be identified:

— Faults due to errors in the process system requirements,
— Faults due to errors in the I&C system specification,
— Faults due to errors in the coding,
— Interference between the application software and the hardware or firmware of the processor system.

(a) Faults due to errors in the process system requirements

The process system requirements are generated by the process engineer and thus any errors are usually due to a misunderstanding of the process. Independent checking of the requirements and animation/modelling provide means of detecting

errors but once errors are introduced the only real defence is functional diversity. The effectiveness of this defence will depend on the nature of the error and the extent of the protection available from the diverse system. The faults arising from this type of error are independent of the technology used to implement the system.

Functional diversity generally means that two or more protective functions based on physically diverse parameters act independently via independent I&C means on independent final elements to meet the same protection goal.

(b) Faults due to errors in the I&C specification

Errors in the I&C specification are similar to and give rise to faults with the same consequences as the SW-CMF of type (a). The difference is that this fault type originates from an error in the generation of the I&C specification from the process requirements, for example as a result of a misunderstanding between the process system engineer and the I&C engineer. Functional diversity is a countermeasure against SW-CMFs of type (b).

(c) Faults due to errors in the coding

One strategy to prevent faults is to avoid using error prone coding methods and taking measures to detect faults by verification and testing. The following constructs are to be avoided:

— Event dependent programme flow or event management by externally triggered interrupts;
— Variation of program roots, depending on different data constellations;
— A real time clock and time dependent decisions;
— The application of long term stores;
— Stack management.

The goal of these coding restrictions is to ensure that the processor system with its integrated software behaves as a deterministic logic machine. The code will then be processed strictly cyclically without any feedback from the process to be controlled.

(d) Interference between the application software and the hardware or firmware of the processor system

Once the software executes on the processor system, the only means of triggering existing but unknown faults that cause a failure (incorrect outputs or even a processor stop) is through the data constellations.

One type of interference between software and hardware is a data dependent processor load. With cyclic program processing, the load on the processors and their busses should be constant and independent of any events in the plant. One goal of tests (e.g. factory tests) is to demonstrate that the software is robust and the processor load and bus load are independent of the data constellation. Additionally, dynamic checks for correct program processing should be applied to support the defence.

Normally, only a subset of a few functions of a standard operating system are necessary to perform a safety task. It is preferable to use a reduced operating system, i.e. a subset of a proven operating system, so that it is possible to perform a type test by theoretical checks. Alternatively, but at a reduced confidence level, it is possible to use a widely used operating system (see Section 4.5). More detailed guidance on the specification, design, development, validation and licensing of software important to safety can be found in Ref. [15].

4.2.3. Software security during the system life cycle

The quality status of the software has to be maintained during the total life cycle of the safety system for all plant operation modes in order to exclude common mode failures according to the requirements of Section 4.2, especially during maintenance activities.

These requirements include configuration management if modifications of the system are necessary to prevent unauthorized access and changes. Maintenance procedures to check the code against the actual specification requirements should be carried out periodically to ensure that the code contains no unintended functions.

4.3. ENVIRONMENTAL QUALIFICATION

The current approach to demonstrating that systems can and will continue to operate correctly is based on a combination of testing, analysis and operating experience. Testing provides a means of demonstrating resistance to environmental factors such as radiation, temperature, humidity, vibration, shock, electromagnetic and radio-frequency interference, electrostatic discharge, power quality, grounding, chemical corrosion and smoke. Environmental qualification analysis is carried out for many devices on the basis of their characteristics, material composition, operating experience and testing results. For seismic qualification both analysis and tests on a seismic table are used, depending on the application. The environmental qualification standards for different countries are similar, though the emphasis placed on different tests may vary.

The digital I&C system should be qualified for the environment in which it is to be installed. This will include seismic and may include LOCA conditions. Digital

devices are not usually suitable for a LOCA environment and it is recommended that they be installed outside high radiation, heat and humidity environments.

The environmental qualification relates to the hardware portion of digital I&C. However, system integration tests should be carried out during and after the environmental tests. The detailed tests should provide assurance of the operation of the system, including the hardware and software.

One approach to setting the environmental qualification requirements for I&C systems is as follows:

— Review the plant design basis and safety case to identify the equipment required to ensure nuclear safety;
— Produce a schedule of important environmental conditions (e.g. temperature, humidity, electromagnetic interference and seismic conditions);
— Identify the location of critical equipment;
— Establish the environmental conditions at each of the locations under normal and accident conditions to complete the environmental conditions schedule;
— Compare the equipment qualification with the schedule;
— Arrange for the relocation or replacement of any equipment not complying with the environmental conditions to which it will be subject.

An alternative approach has been to establish a bounding set of environmental conditions and require that all equipment is qualified to those bounding conditions and is installed only at locations whose environment is within the given conditions.

Methods for qualifying equipment for harsh and mild environments as described in Ref. [45] include:

— Type testing (using representative equipment under conditions simulating the environment);
— Use of operating experience (data from the use of the equipment in a similar environment);
— Analysis (theoretical description of the effect of the operating environment on the equipment);
— Combinations of the above.

There are a number of standards that identify conditions and test methods that can be used for qualification (e.g. IEC 780 for electrical and IEC 801 for electromagnetic compatbility). There are also standards for analysis methods, notably for seismic qualification.

Typical examples of components which must be qualified for operation in harsh and mild environments are connectors, junction boxes, cables, elastomerics,

communication links and various types of electronics. Some of the new I&C equipment (e.g. fibre optics sensors and communication links) being introduced in NPPs need also to be environmentally qualified.

An important element of the environmental qualification programme is a knowledge and understanding of equipment ageing and its impact on overall plant performance. The correct management of equipment ageing can have a significant impact on minimizing the maintenance budget and maximizing the plant capacity factor while maintaining plant safety. The deterioration of I&C equipment with time should be minimized to reduce I&C replacement costs. At the same time, the I&C system should help manage the deterioration of process equipment.

4.4. HUMAN–MACHINE INTERFACE

A human factors plan should be established to handle the human–machine interface [46]. The role of the human operators and the way they may be affected by the introduction of new technology need to be analysed thoroughly.

4.4.1. Human factors plan

The main purpose of a human factors plan is to identify and manage all aspects of the I&C upgrade that have an impact on humans. It identifies all categories of staff in the organization which will be influenced by the new system, including operators, maintenance staff and engineers. The plan should capture all human factors aspects of the project and cover all phases of the project, eliciting and conveying the end user viewpoints on:

— the requirements specification
— user interface design
— testing of the system
— the training programme
— the process of introducing the new system in the control room
— control room modifications.

An effective methodology is needed to assess the impact of computer based human–machine interfaces on human performance [2, 7, 8]. The process control human performance model introduced in Section 4.4.2 may serve as a framework for characterizing the activities and objectives of the control room crew and the way these may be affected by the introduction of new technology and support systems. A task analysis could be performed for large upgrade projects where the operator's role and the environment are changed significantly.

It is necessary to ensure that the new system matches the human factors standards and working conditions in the specific control room (lighting, screen positioning, colour coding, labelling, text size, etc.). Further guidance is available in standards such as IEC 1772 [44].

4.4.2. Human performance assessment

In the analysis of the human–machine interface, it is useful to introduce a framework (process control human performance model) characterizing the activities and objectives of the control room crew and the way these may be affected by the introduction of new technology and support systems.

Target activities and tasks against which to compare system features are needed in order to identify what an individual system does to support the operator or control room crew. These tasks and activities have to correspond to actions which the operating crew are required to undertake in response to the demands placed upon them by the process.

A general process control model is shown in Fig. 1. This model begins with the initial assumption that there is an ongoing operation being conducted by the control

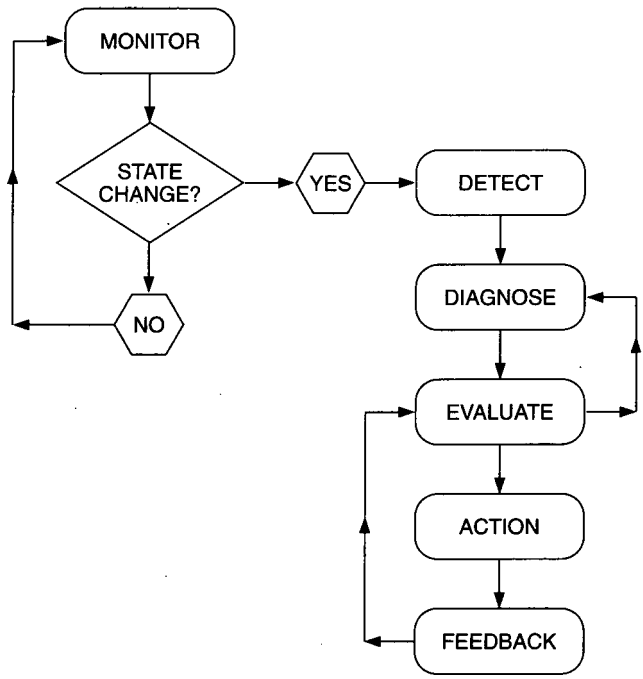

FIG. 1. General process control model.

room crew. In order to decide whether to maintain the plant at its current operating state (e.g. steady state power production) or to make some modifications or adjustments (e.g. startup, load following, implementation of a boron injection programme) the operators must first monitor the information systems in the control room to obtain an overview of the plant status. They need, in other words, first to be aware of the conditions and restrictions in place at their plant prior to acting.

The control room crew is responsible for responding to changes in plant status, either by ensuring that operation is as planned, or recognizing that a malfunction is occurring. In either case, the operating crew must first detect the change in the plant. If the change is within the range of responses expected for the specific mode of operation, then the detection serves primarily as confirmation that things are functioning as expected. If, however, the change in plant performance is outside the expected region of plant response, then detection should serve to identify some sort of 'fault' in the response of the plant.

Following initial fault detection, one of several things may happen. If the disturbance is minor, then the operator may attempt to diagnose the cause of the malfunction and correct it. However, if the disturbance results in the actuation of the plant's engineered safety features, then one of two typical activity sequences occurs. If event based emergency operating procedures (EOPs) are used, then some diagnosis of the initiating event is required in order for the operator to select the appropriate mitigation procedure. In event based mitigation strategies, this initial diagnosis is crucial to the success of subsequent operating crew responses. It is more likely, however, that plant personnel use 'symptom based' or 'functional recovery' EOPs.

Regardless of whether an event based or function based mitigation strategy is used, the crew establishes specific goals for the mitigation strategy itself. That is, they evaluate the status of the plant and systems, and in response to the initiating event, they gauge the appropriateness of specific recovery efforts as outlined in the EOPs.

Following the evaluation or planning phase of event mitigation the actual recovery actions are performed. In this phase, the operators carry out actions, executing tasks contained in the EOPs. An ongoing activity during mitigation is obtaining information from the system about the effects which the recovery efforts are having on both individual plant components and on the system as a whole. This information gathering comes in the form of feedback from the process to the operators, which is obtained via the instrumentation or other systems in the control room. The crew uses the information from these systems to evaluate the effectiveness of their recovery efforts, to confirm the appropriateness of the mitigation strategy employed, or to identify the need to reconsider the strategy.

The purpose of the human performance model is to identify the tasks within the more general process control model that forms part of each of the process control activities (detection, diagnosis, etc.). These tasks, in turn, are intended to be used to show how a control room crew could use the information provided by a new support

system. A signal validation system might assist in determining whether an instrument was faulty or whether other fault hypotheses should be pursued. Decomposing each of the new systems considered in this way yields a systematic description of the control room tasks supported by each system. It can also be used to determine how a given task can be supported by different types of information (alarms, condition monitoring, etc.) as well as to facilitate the selection of information presentation techniques (colour coding, textual versus graphic display of process data, etc.).

A note of caution about the human performance models needs to be made. First, the I&C systems, the EOP 'philosophy' (e.g. event based versus symptom based) and other key elements of the operations environment (crew staffing, training, tasks allocated, etc.) differ between plants and between vendors. The model is only intended to identify the typical activities which may be conducted by the operating crews.

Secondly, the model, as presented, is not intended to be predictive, in the sense of implying invariant sequences of activities; for example, diagnosis often occurs before actions can be carried out. Neither does it predict the specific strategies which might be used to accomplish a given activity (e.g. hypothesis driven versus topographic based diagnostic strategies). Rather, its purpose is to identify the domain of process control tasks which are the basis for monitoring and control activities, to provide some logical ordering of these tasks into relevant groups, and in doing so, to provide a basis for analysing how the new information systems support control room crew performance in a process control setting.

4.4.3. Human decision support

The backfitting of NPP control rooms with more advanced computer based solutions opens possibilities for improving the support given to the operators in their cognitive tasks discussed above. Computer based operator support systems (COSSs) can assist the operators in different operational situations, ranging from normal operation to disturbance and accident conditions [3, 14, 52]. The individual cognitive tasks and their association with advanced I&C techniques are discussed below.

Detection

Early detection of faults and disturbances in NPPs reduces the risk of disturbances developing into severe plant conditions (shutdown or accidents) as the operators have more time for diagnosis and counteractions. Furthermore, early detection of a disturbance usually means better localization of the problem area in the plant, thereby facilitating the diagnostic task. The traditional way of informing operators about possible problems is through alarm systems based on the checking of process variables, which should stay within prescribed limits. In many cases a disturbance in a plant subsystem may propagate into neighbouring subsystems before the

operator is alerted by the alarm systems. The operators are therefore confronted with a large number of alarms within a short period of time and this makes the diagnostic task difficult. Alarm filtering techniques may reduce this problem to some extent.

An alternative method for fault detection is based on mathematical reference models describing the dynamic behaviour of the process. If measured process variables are compared with corresponding calculated variables from the reference models in real time, the time needed to detect disturbances can be reduced compared with traditional alarm systems [53].

Surveillance of critical safety functions

In the case of major disturbances which may develop into severe accident situations, traditional event oriented alarm systems may not provide sufficient assistance to the operators. This is partly due to the fact that these kinds of systems may fail to draw operator attention to the important problems in the plant. An event oriented, limit checking system leads to a large number of alarm messages even in situations where there is only a moderate plant disturbance. The presentation of unimportant information mixed with important information may be misleading for the operator. Furthermore, an event oriented alarm system tends to draw the operator's attention to problems with many individual components while in accident situations attention should rather be directed towards the performance of critical plant functions.

These problems have resulted in a function oriented approach to NPP monitoring for disturbances which may have the potential to develop into accidents. From a systematic study of scenarios that may lead to accidents, a set of critical safety functions is defined. These functions have to be maintained to prevent serious consequences arising from the disturbance, such as harm to the staff and plant damage. Several systems have been developed on the basis of this principle [40, 54].

Diagnosis

One of the most challenging tasks for human operators is fault diagnosis. Diagnostic systems have been developed on the basis of various principles. The best known principle is employed in rule based expert systems, where information on patterns of the alarms and other process variables are matched with precalculated patterns from known disturbances so as to arrive at hypotheses for the cause of the alarms. Another technique is based on searching through goal and success trees to establish the plant status. A further concept uses a multilevel flow modelling method. The mass flow and energy flow are used to set up constraints for the correct functioning of the plant, and an imbalance indicates a failure event. Yet another technique utilizes fuzzy logic reasoning.

An ideal system should integrate different methods and techniques, thereby incorporating important qualities of the various principles mentioned above. In this way, more robust systems will be obtained as a result of the diversity in diagnostic methods and knowledge [53].

Prediction and planning

Predictive simulation is becoming feasible and can assist operators in on-line prediction of important plant parameters and in planning mitigation strategies. Several applications exist for simulation of core behaviour during a planned power transient. This is of great help for reactor operation in dynamic core state situations where xenon variations often have a complex influence on the power distribution. The operator can thus avoid control strategies that are unacceptable in terms of operational constraints by considering the predicted margins to these constraints for different strategies. Examples of more comprehensive plant-wide predictive simulators are also emerging. They provide means for simulating complex interactions between different plant systems even in accident situations.

Procedures

A number of observed and potential problems in the nuclear industry are related to the quality of operating procedures and much work has been done in recent years on improving the quality of procedures, especially EOPs. Improvements have been made to most aspects, including structure and contents, implementation and maintenance.

Many of the problems identified can be directly addressed by developing computerized procedure handling tools. Thus, there is a growing interest in the use of modern computer technology for improving procedure preparation, implementation and maintenance.

4.5. QUALIFICATION OF COMMERCIAL HARDWARE AND SOFTWARE

The qualification requirements for use/reuse of commercial grade hardware and software products will depend upon the safety category of the target application. The ease with which qualification can be achieved will depend on the availability and accessibility of documentation and information about the system, including:

— system functional specification
— system interface specification

— qualification history
— evidence of successful application and operation
— quality assurance applied during development
— development method
— source code (for analysis)
— factory and other test results
— modification history.

The assessment/qualification process will also have to examine specific features and requirements such as:

— ability to deliver the required functionality, and amount of excess/unused functionality
— response time
— reliability/availability
— suitability of failure modes
— fault tolerance
— environmental qualification
— maintainability and testability
— human factors.

A limited amount of additional information on software reuse is given in Chapter 13 of Ref. [15] but software and standards are starting to emerge that address this topic (e.g. the first supplement to IEC 880 [16]).

It should be possible to qualify commercial grade advanced digital products for category C (IEC 1226 [30]) applications. In cases where there is some application specific prequalification for non-nuclear safety applications (e.g. for boiler protection or crane controls), qualification for category B applications should be possible. Qualification for category A functions will be exceptional, as in most cases the necessary documentation will not be available.

4.6. QUALITY ASSURANCE

4.6.1. Quality assurance process

A well defined quality assurance process is one of the key prerequisites for successfully performing an I&C upgrade. The quality assurance covers hardware, software and human factors associated with an I&C upgrade and may be initiated by establishing:

— A project quality assurance plan identifying posts, post holders and their responsibilities;
— A hardware quality assurance plan covering the main phases of design, construction, interfaces and deliverables, fabrication and testing of the hardware including computer platforms, networks and cabling;
— A software quality assurance plan describing the various software life cycle activities;
— A human factors plan ensuring that end user needs are covered.

The plans need to be in compliance with the principles and recommendations of the IAEA Code and Safety Guides Q1–Q14, Safety Series No. 50-C/SG-Q [27].

It is important to divide the project into well defined phases, each with deliverables that can be reviewed at the end of the phase prior to proceeding to the next. Audits should be performed during the project to monitor project status and progress and ensure compliance with quality standards and plans. Any change to the project plans must be documented and revised documentation issued; deviations from the plans will be recorded as non-compliance and corrective action taken.

Many of the QA practices necessary for success are well established and applicable equally to analog and digital systems. However, because of the perception that design complexity is the major source of error in digital systems, special attention should be paid to verification and validation activities. These are described below for new software. Additional material can be found in IAEA reports [15, 55] and standards such as IEC 880 [16].

4.6.2. Verification

Verification plan

Each phase of the software development process is completed by a verification activity that is conducted according to the verification plan. The plan documents all the criteria, techniques and tools to be utilized in each phase of the verification process. It describes the activities to be performed to evaluate the deliverables from each phase. The level of detail is such that an independent group can execute the verification plan and reach an objective judgement on whether or not the implementation performed during the phase has been completed correctly.

Deliverables are placed under configuration control before a verification activity is performed, and the findings (including the need for corrective action) are recorded. Best practice dictates that verifiers should be independent of the development staff and should not advise them on any corrective action.

Design verification and critical reviews

The verification exercise completed at the end of the design phase seeks to confirm that:

— The design is a complete and correct representation of the functional requirements contained in the specification and that no functions have been added or omitted;
— The design structure of the hardware and software complies with the design rules and standards;
— The assignment of functions to the various elements meets any requirements for segregation, separation and diversity;
— The design lends itself to testing and in-service proof testing and maintenance;
— The documentation is readable and records any defensive features used in the design to support safety arguments.

The results of the design verification are documented in a report that identifies:

— Items which do not conform to the software functional requirements;
— Items which do not conform to the design standards;
— Modules, data, structures and algorithms poorly adapted to the problem.

Coding phase verification

Code verification is carried out to check that the code represents the design and performs the required function. The process involves: inspection of performance, a check compliance with the coding standard and in some cases module testing. The verification activity may also include a check of the module testing to ensure it has achieved its purpose of showing that each module performs its intended function and does not perform unintended functions.

Software test specification

The verification of the software test specification ensures that it records:

— The environment in which the tests are to be executed;
— The test procedures to be followed;
— Acceptance criteria, i.e. a detailed definition of the criteria to be fulfilled for acceptance of modules and major software components at the subsystem and system level;
— Error detection and corrective action procedures.

The verification team are at liberty to request additional tests if they consider the coverage is not adequate.

Software test report

The software test report is verified to ensure it includes the following items for both the module and major design levels:

— Hardware configuration used for the test;
— The version of the code tested;
— Storage medium used and access requirements for the final code tested;
— Input test listing;
— Output test listing;
— Additional data regarding timing, sequence of events, etc.;
— Anomaly reports and requests for corrective action.

System integration

The verification of hardware/software integration is a combination of hardware and software verification ensuring that procedures are available and are followed to:

— Assemble hardware modules by interconnecting wiring according to the system design drawings;
— Assemble software modules by a linkage processor;
— Load the software into the hardware;
— Verify by testing that the hardware/software interface requirements have been satisfied and that the software is capable of operating in the given hardware environment.

4.6.3. Validation

The validation of a system is usually completed by a combination of testing and analysis to verify that the system performance, functional and temporal, meets the requirements. The testing element is usually completed by exercising the system with the range of static and dynamic inputs expected during normal and disturbance conditions to confirm that the system functions as expected, displays the specified alarms and indications and responds to operator action.

The test coverage cannot be exhaustive but each function should be subject to at least one test. The testing will also examine the timing and behaviour of the system at its interface with the plant. The analysis element of the validation can involve reverse engineering of the loaded code to an intermediate form derived from the specification.

The procedures, test plans and acceptance criteria are defined before the modification takes place, some parts being produced very early in the system life cycle, i.e. at the program planning phase. The specification will also include the test procedures and any requirements for test equipment and its calibration.

The validation report will contain a full record of the tests and the results and will serve as a reference in the event of regression testing or after system modification. All anomalies will be recorded and analysed so that any anomaly is resolved or a request for corrective action issued.

Validation activities and partial testing should not be confused with confidence building measures carried out to support the system safety justification. The latter are conducted with the expectation of success, i.e. they are not intended for error detection used to build up a statistically significant body of evidence to support the validation and system justification.

Nuclear power plant simulators are now available for the purposes of training, analysing the behaviour of the plant in both normal and accident situations and the assessment of improvements in process, automation and human–machine interface systems. These simulators can also be used to support validation testing as they can provide plant data and, in cases where the system output can be connected to the simulator, the opportunity for dynamic system testing as described below.

The main phases of the engineering process and the main software modules of a simulator are depicted in Fig. 2. Generally, it has to be assumed that the I&C upgrade contains a limited number of I&C functions which form a subset of the I&C

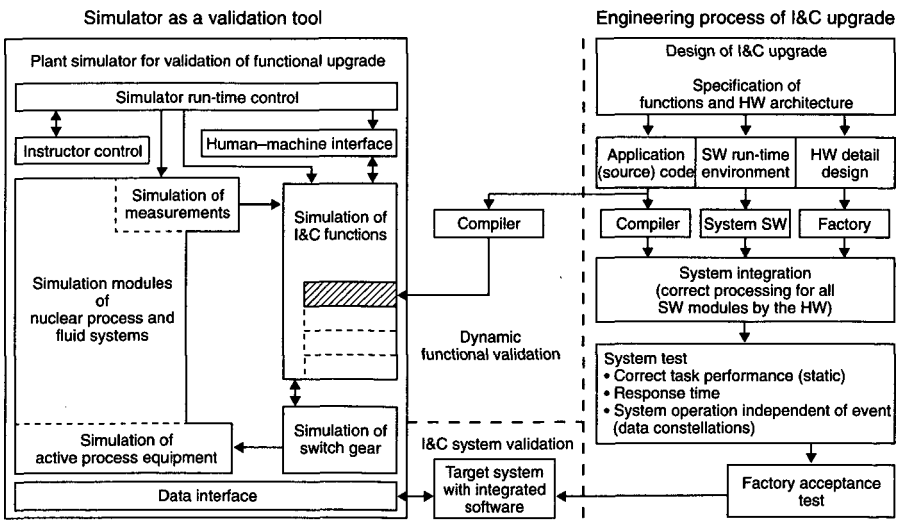

FIG. 2. Simulator based validation process for digital I&C functions.

functions simulated. In principle, there are two possibilities for simulator based validation: functional validation and I&C system validation with integrated software.

For dynamic functional validation the verified and pretested application source code of the functions to be upgraded can be compiled and integrated into the simulator in place of the originally simulated I&C functions. Through simulation of design basis events and accidents, validation of the functional behaviour can be performed by comparison with the safety system requirements. Special care has to be taken in the selection of the compilers if the target system for the upgrade and the simulator system do not permit use of the same compiler.

Functional validation in the system test phase is considered a prerequisite for demonstrating:

- correct task performance by static input and output checks
- correct response times
- event independence of system operation by consistent and even inconsistent data constellations.

There is an advantage in performing the validation of the intended functions at an early phase of the engineering process.

An alternative validation procedure for the complete target system is to link it to the simulator via a data interface. As opposed to the first mentioned validation procedure, the coupling problem between a simulator and a real time target system can only be solved for special situations and not generally.

4.7. CONFIGURATION MANAGEMENT

Configuration management is an essential part of plant management with respect to change control in design, material procurement, construction, installation, commissioning, operation and maintenance [1]. It covers physical changes, the associated documentation and the procedures for operation, maintenance and testing. The basic philosophy is that the plant has to be in a known and safe configuration. Any deviation from this state, whether temporary or permanent, has to be properly planned, documented, reviewed, approved and implemented in accordance with established plant procedures.

Configuration management provides:

- The technical information necessary to make changes to the plant hardware, software and documents.
- The background information needed to change plant procedures (operating, maintenance, testing, training, quality assurance and quality control).

— Reduction in uncertainties and delays in operating, maintenance, testing and procurement activities through the availability of accurate documentation (drawings, specifications, manuals and analyses).
— Support to the procurement process by ensuring that accurate information is available to support conformance of material with design requirements by means of certificates of origin, vendor manuals, inspection, environmental qualification, seismic qualification, etc.
— Assurance of the availability of updated licensing documents such as safety analyses, design documents and technical specifications.

Many of the quality assurance issues are also addressed by configuration management and are of interest to both NPP operators and regulators. In an operating plant these issues directly affect plant operation and nuclear safety and are often identified as areas of concern during the plant quality assurance audits. The plant must have procedures to handle these QA issues, namely:

— document control
— control of materials, equipment and services
— identification and control of materials, parts and components
— handling, storage and shipping
— non-conformances
— corrective actions
— quality records.

Most of the above items will be relevant to the hardware configuration management of a digital system. But software configuration management and change control for software performing safety functions need special attention and a more rigorous approach in an operating plant. For safety applications, it is necessary to perform both software change analysis and safety analysis as part of the initial review of the change. The rigour of the change control and the qualification requirements of the staff making the change depend on the criticality of the software application as governed by its categorization. As a minimum, the following must be considered:

— configuration identification (identifying, naming, purchasing, establishing baselines)
— configuration change control (requesting, evaluating, approving and implementing changes)
— configuration status accounting
— configuration audits and reviews
— interface control

— subcontractor and vendor control
— document control.

Configuration control can be compromised by poorly executed modifications, inappropriate operating configurations or incorrect maintenance work (inappropriate parts replacement, incorrect calibration or incorrect work protection isolation). The use of digital technology and computer based information systems can make the situation worse, because improvements are easier to make and therefore more likely to be attempted. With each attempt there is a risk of a loss of configuration control unless appropriate steps are taken to manage the process. As a result, security requirements for configuration changes are established. Automatic system reconfiguration in the event of failures of system parts is useful for providing system working ability.

Configuration management tools that are effective at maintaining control but still permit a change to be made effectively are an area of growing interest to nuclear plants.

4.8. APPROACH TO THE RESOLUTION OF CURRENT LICENSING CONCERNS

The resolution of licensing issues identified in Section 3.8, such as the licensing procedures and practices, is only possible on a national basis as dictated by national legislation. The problems are, however, essentially technical and economic and are associated with providing the assurance that the regulatory requirements have been met. Methods, tools and techniques are being developed to facilitate system assessment and demonstration.

Modern hardware components, such as application specific integrated circuits (ASICs) or programmable logic devices (PLDs), are very complex. The definition of the failure modes of these components is not tractable in practice as the number of instances of each mode could be far greater than the open circuit, short circuit and off-value failure modes of discrete components. In order to have the same confidence in systems incorporating these 'modern' components, a means needs to be found to remove the dependence of the safety justification on the component failure mode. This may be possible by adopting new design practices, for example performing the design and its associated failure analysis at the module level.

The reliability analysis of discrete circuits is based on the assumption that the equipment and components are in working order at the start of life with the historical endurance failure rates. Reliability data are available for most integrated circuits. In addition, manufacturers are often able to provide endurance failure data for whole assemblies (e.g. computer boards). However, this is not the case for many custom

made integrated circuits such as ASICs, where the population is small and operational history is limited. The validity of the data provided for those programmable devices that undergo physical change on programming (e.g. PLDs) has to be carefully considered. These issues could be addressed by analysis and frequent proof testing until sufficient service data are available. The amount of data deemed sufficient will remain a matter for agreement between the licensee and the regulator. This question should be discussed with the regulator during the feasibility stage for the system, prior to a commitment to the technology.

The assumption that the components are in working order is related to the demonstration that the delivered system is compliant with its requirements at the start of operation. The complexity of integrated circuits is such that in practice they may not be exhaustively tested. This is not unique to integrated circuits, as individual valve and transistor characteristics had often to be checked prior to their use in discrete component circuits. The safety justification needs to address this issue, possibly using redundancy arguments or diversity designs to exclude the possibility of a common mode fault.

The justification of tools used for analysis, testing and code generation would appear to be particularly important in the case of advanced systems because of their great dependence on such tools. The approach to demonstration of safety has essentially been based on diversity: the use of two tools to check the same process for the same result, re-engineering of a process to ensure that the starting point is recovered or using diverse means of demonstration (e.g. testing and analysis).

Significant progress has been made with software engineering technology for computer based systems and these systems have now been successfully licensed in a number of countries. The route adopted has typically incorporated a combination of static analysis and dynamic testing to support a mature and highly controlled development process for the system and its software.

5. SAFETY APPROACHES FOR THE HUMAN–MACHINE INTERFACE

This section identifies the key issues of human performance associated with upgrading of I&C systems and describes important aspects of the human factors design process. The verification and validation programmes to ensure adequate testing of the human–machine interface are also discussed. Dynamic testing and validation in training simulators may reveal possible problems before installation in the plant. The influence of the system on the whole organization needs to be evaluated and training of the staff planned.

5.1. HUMAN PERFORMANCE ASSOCIATED WITH I&C SYSTEMS

Ensuring adequate human performance is applicable equally to analog and digital I&C systems. However, digital I&C systems introduce a number of unique features as described in Section 3.4. Control rooms and control panels using digital I&C systems tend to be much more compact than their analog equivalents, which is one of the major reasons for choosing digital equipment. Consequently, many of the controls and displays are multifunctional and therefore special care is required to ensure successful human interaction, particularly during off-normal or unusual events.

Displays often present information in a concentrated manner and they are often 'stacked' in 'pages' or display hierarchies. The logic of what is presented, and the quantity of information and the form in which it is presented to the operator, become of special concern.

Many operators are familiar with a large, spatially fixed arrangement of controls, alarms and indicators in a control room. They utilize a strong 'pattern recognition' approach to the diagnosis of the plant condition. In digital I&C systems, the combination of compactness and a multi-purpose function inhibits this type of approach, which means the design has to recognize operator preferences. It is also essential to provide retraining to help operators develop the required skills and avoid errors.

When automation is introduced, it is difficult to ensure that the operator will remain 'in the loop' and be capable of taking over and acting as a backup to the automatic system when needed [1, 6]. Special care has to be taken to ensure that systems are designed so that the operators maintain awareness of the various operating modes of the control systems, the transition points, the limits on operator action, the circumstances in which the operators need to take over control, and the procedures for executing control without 'fighting' the control system or creating unnecessary transients. The operators should be provided with adequate support functions analysing the state of the automatic systems and interlocks to maintain their awareness of the situation.

Advanced computer based systems facilitate complex, high level analysis such as plant state identification and fault diagnosis. Such systems support tasks that operators in conventional control rooms had to perform by collecting information from instrumentation and applying experience and knowledge. In the design of advanced computer based processing systems it is important to make the reasoning behind the systems transparent to the operator, to explore diverse techniques and methods when possible, and to make the operators aware of the limitations of the system.

As a result of the use of software, digital I&C systems often provide flexibility in the configuration of the controls, alarms and displays and permit the use of prioritization or other logic in displaying alarms or sequencing certain actions. However, the systems need to be designed so that they do not confuse the operator and that the operator is not led into making errors.

Maintenance issues, particularly requirements for software maintenance, can be different for digital I&C systems. Such software related processes as installation, maintenance, testing and configuration control require significantly different maintenance skills and training. Systems must be designed to anticipate maintenance and provide displays and controls for aiding these activities. The personnel involved need special technical skills, for example in programming, display design and software testing. Changes are validated and controlled to ensure that they do not introduce errors that degrade safety.

Experience in design, development, testing and operation show that the implementation methods for digital I&C systems can affect the functioning of both operations and maintenance personnel. The current approach emphasizes a systematic, interactive team effort involving hardware and software specialists, control system designers, human factors specialists, operators and regulators. This approach tends to be an open ended and iterative process that if not carried out systematically may be unnecessarily inefficient, expensive and time consuming.

5.2. HUMAN FACTORS DESIGN PROCESS

The importance of a well designed human–machine interface for reliable human performance and nuclear safety is widely acknowledged [7, 46]. Errors caused by operators in the control room are a significant contributing factor to NPP incidents and accidents. For example, the errors in the Three Mile Island accident were due to several factors, including a poorly designed control room and inadequate provisions for monitoring the basic safety parameters of the functioning of the plant.

The ultimate responsibility for safe operation lies with the utility which owns the facility. During plant operations this responsibility is shared with the operations staff. The control room crew interact with systems throughout the plant, many of which they cannot observe directly [42]. In doing so, they rely on the I&C systems to provide them with the necessary information to make decisions and to relay instructions back to the remote systems. Operator performance is greatly affected by the quality of the interface with the process. The functioning of the human–machine system is strongly influenced by the capabilities and limitations of the operator and the quality of the human–machine interface.

In most cases, the role of the operator is a very active one. The operator determines which systems to activate and when to issue instructions to the systems. The technology employed in the control room and the design of the control room are instrumental in shaping operator performance and in determining to a large extent how efficient the operators can be in carrying out their role. Changes in technology demand careful evaluation since they may impact safety related actions.

In order to facilitate the introduction of new digital technology, the intermediate step of a hybrid solution (i.e. visual display units added to a conventional control room) can be an alternative in many cases for the following reasons: adaptation and acceptance by the operators may be easier; experience is gained without impacting production; and the licensing process can be gradually developed from operational systems to safety systems. Moreover, a hybrid design solution may provide an optimal combination of traditional and advanced information systems [44].

If an upgrade influences the operators' work, a task analysis needs to be performed (see Section 4.4.2) to analyse the operator interaction with the new system and establish the operator dependence on key information from the new system. Typically, tasks are transferred from operation to maintenance as a result of I&C automation and the self-testing and self-checking procedures of the new equipment.

The operator workload is carefully analysed and optimized. The totality of tasks assigned to an operator under the worst possible circumstances must not prevent an adequate level of performance. Conversely, it is important that an operator not be given too few tasks such that he or she is under-stimulated and demotivated. If carefully designed, new systems may provide operators with efficient and interesting tools for carrying out data processing and information analysis tasks. In this way, the information basis for operator decisions can be enhanced.

Experience is gathered during plant operation on the effectiveness of the control room and the information systems. Reports are made available on situations with disturbances, trips or incidents caused by human errors, and these are analysed to identify weaknesses in the existing designs for use as inputs for the new system design. Conversely, for systems with high availability and a good operations record, the key design features are carried over to the new system design.

It is desirable that the operations staff be involved early in the upgrade project. In this way operational experience and requirements, particularly undocumented functions, are carried over to the design team. The operations staff will work with the new system once it is installed. They have to feel that this is their system and that their specific needs and requirements have been taken into account and are reflected in the new system design.

In an upgrade, operator involvement in design may be needed to apply the existing presentation scheme in the control room to the new system in order to provide a smooth transition. However, the upgrade should utilize the benefits of modern technology for operator support and the integration of information. The old analog technology is based on the concept of one sensor for each indicator in the control room, while digital technology makes it possible to process information from several sources, correlate this information and present it to the operator in an overview display offering a detailed analysis. Typical areas of application are alarm analysis, post-trip guidance and critical function monitoring.

Human factors need to be addressed in all phases of an upgrade project starting with the requirements specification [41]. Human factors experts should be assigned to the project team. There are several types of question to be considered in the case of an I&C upgrade. For instance:

— How does the operator interact with the system?
— How might the operator misinterpret information provided by the new system?
— What are the possibilities for performing an erroneous operation by means of the new system?

If the user interface is not properly designed, the operator may drive the system into a non-intended state, and the system will remain inoperable until it is reset. Consequently, the system has to be designed to be robust against human errors.

Information display

Guidelines should be followed on the design of display formats (mimic displays and trend graphs, display format elements such as labels, icons, symbols, colour, text and coding, data quality and update rate) and display devices.

Operator–system interaction

It is important to specify: dialogue format, navigation, display controls, information entry, system messages, prompts and system response time, methods for ensuring the integrity of data accessed through the user interface, prevention of inadvertent change or deletion of data, minimization of data loss due to computer failure, and protection of data from unauthorized access.

Process control and input devices

Physical devices, including alphanumeric keyboards, function keys, trackballs, joysticks, mice, touch screens, light pens used for information entry, operator dialogue, display control and information manipulation must be considered, as must display and control integration.

Alarms

Alarm systems are important classes of systems where human factors issues are concerned. It is necessary to review the methods for alarm generation, prioritization, structuring and filtering, ways to acknowledge alarms and alarm presentation. Proper integration of conventional alarm systems and advanced computerized alarm systems

is an important issue. A particular concern is the operator's ability to read and understand the information obtained from the alarm system in severe transients without being overloaded.

Analysis and decision aids

New systems often contain functions that enhance the traditional data processing and presentation schemes. These may be expert systems for fault diagnosis, on-line simulators for predictive analysis of plant behaviour, post-trip analysis systems, etc. When such advanced operator support systems are introduced, validation programmes are necessary (see Section 5.4). These programmes should involve the operators in order to ensure that they fully understand the performance and behaviour of the analysis and decision aids.

Inter-personnel communication

Activities related to oral and computer mediated communication between plant personnel should be considered.

Workplace design

The organization of displays and controls within individual workstations, the control room configuration and the environment are topics to be considered.

5.3. PLANT PROCEDURES

There are many important plant procedures which need to be updated or developed after the introduction of an advanced I&C system. The degree of detail contained in the procedures depends on the product and on its safety categorization, complexity, reliability and safety requirements. For example, a category A system is expected to have a very extensive testing procedure, and a new digital product will require detailed training procedures for the operators and the maintenance personnel. Operating, testing, maintenance, calibration, emergency operating and training procedures will need to be updated.

For I&C systems, the normal operating procedures, testing procedures and emergency operating procedures specify the operating limits, the safety margins, operating margin to trip and operator actions for various alarms and annunciations. The safe operating envelope of the equipment has to be maintained. It is desirable that the procedures be tried before being brought into use. The use of simulator can be

beneficial for verifying the functionality, human factors impacts and effectiveness with respect to operability and testability.

Maintenance and calibration procedures are developed to include the additional capability and functionality of the digital system. The software quality assurance and configuration control of the system are also considered. The change control of the digital system, especially the software change control procedures, is based on the software categorization of the safety function. It is obvious that a higher category system, which performs a critical safety function, will have more rigorous procedures. The skill level and qualification requirements of the staff making the changes also need to be specified, although it is unlikely that the operations staff would be allowed to modify software for a Category A system in an operating plant.

With the introduction of digital technology (trip and control computers, monitoring and testing computers, distributed control systems, digital controllers, digital meters, programmable controllers, data acquisition computers) — either custom designed or procured as commercial grade items — appropriate station policy and procedures need to be developed to handle a wide variety of products. Many of the old procedures need to be replaced or revised, new procedures written, staff trained and qualified, and documentation updated. Care must be taken to develop maintenance procedures which bring consistency among various products from different manufacturers as well as with existing station procedures. The system safety function category, product type, manufacturer's recommendations and specific station needs will influence the development of the new procedures. For example, if an old analog system is replaced by a new digital controller, many of the old features may be retained for the hardware, but the software will need a new set of procedures based on the product qualification, quality assurance requirements and the station needs.

Procedures for training and skill development have become more formal and rigorous not only for licensed operators but also for maintenance staff, designers and nuclear safety analysts. With the introduction of digital products, existing training manuals need to be revised and new ones developed. Simulator retraining will also be required. Some computer based training tools are available with digital products and many new ones are being developed. Simulator based training is also becoming important.

Computer based procedures are now being used quite extensively in NPPs. Some of these procedures are associated with digital systems and the others are stand-alone procedures for calibration, diagnostics, maintenance, testing and the recording of data. Many of these stand-alone procedures are available in hand-held or portable computers. Some of these procedures are supplied by the vendors with commercial packages.

5.4. HUMAN FACTORS EVALUATION

In the validation of human–machine systems, it can be useful to relate the various individual systems to the operator tasks supported by the system. A human performance model (as described in Section 4.4.2) which breaks down the activities performed by control room operators into a connected sequence of subtasks will be useful in the evaluation process. The purpose of the evaluation and validation of a new human–machine interface is to ensure that it:

— supports the right tasks;
— provides the correct information for the task;
— fits the existing information coding schemes;
— does not result in excessive task demands;
— does not excessively increase the amount of information;
— supports the continuity of operator activities;
— is designed for specific user needs.

Important steps to ensure operator acceptance include:

— establishing the correct expectation about the system prior to use;
— obtaining design input to ensure that the system supports operator tasks;
— ensuring that operators trust the system and understand its capabilities and its limitations;
— ensuring that operators are trained to use the system;
— ensuring that the system can be used in the manner intended and does not produce unintended actions or behaviour.

System definition and modelling

Before the system is evaluated, the elements and features of the system that are supposed to influence the operator's performance have to be described. A systematic analysis of the system's purpose and functions is made along with the identification of expected effects on human performance, the relevant critical performance indicators and possible constraints in the proposed evaluation programmes. The human performance model described in Section 4.4 can serve as a reference for defining the role of the new system.

Once the system is defined, it is important to specify the proposed model of the human–machine interaction. The models and underlying assumptions are specifications of how the human and the machine are expected to interact. These specifications can then be compared with the actual system design. Formulating a model of how the operator will interact with the system makes it possible to compare test and evaluation

results available from other similar systems. As an example, a simple model of the human–machine interaction describes the limitations of human information processing as constraints on the system design.

Methods for testing and evaluation

A variety of techniques are used for the testing and evaluation of human–machine interfaces [43]. Two main categories are: non-performance-based test and evaluation methods (analytical methods), and performance based studies (empirical methods).

Non-performance-based evaluations are based on expert judgement of the system rather than performance measures collected from simulator based tests, for example the judgement of experienced users on whether the system performs as intended. Studies will also be conducted in which the system is compared with accepted human factors engineering design recommendations. The guideline evaluations are based on comparisons between the human–machine interface and the available recommendations. The model based evaluations rely on a model of the expected user or the interaction between the user and the system.

Performance based evaluations (empirical methods) commonly rely on the recording of some manifestation of human performance in interaction with the system. These studies vary in their degree of experimental control and fidelity. Data from these studies are collected and quantified in a systematic way for subsequent analysis. The informal unit test is similar to a task analysis but is less exhaustive. The technique is based on exposing the system to potential and representative users. Test subjects are interviewed during runs with the system and their performance is observed. The evaluation uses limited simulation for dynamic tests and concentrates on the new system without considering other systems. The evaluation also uses realistic full scope simulation aimed at gaining knowledge about how the system affects human performance. A major characteristic of full scale evaluation is that it aims to isolate the performance effects that are directly attributable to the introduction of the new system.

5.5. TRAINING

For safe plant operation, operator behaviour is as important as equipment reliability. Training programmes are provided for both plant operators and I&C specialists and are designed to be consistent with the complexity of the functions and systems implemented. The implementation of digital systems will also require training for NPP staff (operators, maintenance staff and technical engineers). The training requirements need to be established in consultation with the vendors. The

appropriate documents (design manuals and manufacturers' manuals) should be used. The training programmes should cover normal and abnormal reactor operation, and should also include operator interfaces with the computer systems and the recognition of hardware and software abnormalities.

The operators will require a user manual that defines each interface device, with an explanation of its function.

Operator training should be conducted on a training system which is equivalent to the actual hardware/software system. From a training point of view, it is beneficial to connect the new human–machine interface to the plant training simulator before it is installed at the plant. This makes it possible for the operators to get used to the new system before commissioning starts (see also Section 4.4).

6. SAFETY ASPECTS OF THE UPGRADE PROCESS FOR ADVANCED PROTECTION, CONTROL AND HUMAN–MACHINE INTERFACE SYSTEMS

This section describes the process and safety implications of introducing advanced systems as part of a plant upgrade by reference to the life cycle process: system requirements specification; detailed design; acceptance testing; installation; commissioning; and operation and maintenance. It is a prerequisite that the necessary preconditions with respect to system categorization and safety approvals have been met.

6.1. SYSTEM REQUIREMENTS SPECIFICATION

The first phase in the upgrade process is the capture of the functionality of the existing system, for both the process control and operator interface to be implemented in the new system. The introduction of a new system provides the possibility of inclusion of additional functions. The upgraded system has to be integrated and to interface with the existing systems that are retained and the boundary conditions of the existing plant. Consequently, the design process is more complicated than that for the design of a system in a new plant.

6.1.1. Design basis re-engineering analysis

The system requirements specification of the safety functions to be upgraded has to comply with current standards and requirements for documentation.

I&C systems performing safety relevant functions in NPPs that have been operating for several years normally use solid state or relay logic technology. The basic

requirements and system properties of existing I&C systems are usually not included in the original design documentation, as is required by current standards. Consequently, a re-engineering of the design basis requirements is necessary to provide the basis for backfitting with new I&C systems. The capture of system properties is a difficult task. For example, hard-wired I&C systems generally have prompt processing behaviour with a response of the order of milliseconds. Therefore, the response time is usually specified only for functions which require a delay time for process reasons, whereas the tolerable maximum response time is not specified.

Once the original requirements have been captured, an analysis and review are performed to determine which of the original functions are to be retained and what new functions, if any, need to be added.

The system requirements specification gives the design basis for the subsequent engineering phases. The main safety items it contains are:

— The functional requirements which are re-engineered from the as-built features of the existing I&C systems;
— Functional upgrades which improve safety and operations and reduce maintenance costs;
— The requirements on fault tolerance and reliability according to the categorization of the functions to be backfitted;
— The boundary conditions given by the retained existing I&C functions and their interfaces with the upgraded functions, the available space for control cabinets and power supplies and the capacity of the ventilation systems.

The re-engineered system requirements specification also forms the basis of the licensing process for the upgraded I&C system. Special care should be given to documenting the individual functions required and confirming what has been achieved by the upgrade.

6.1.2. Architecture analysis for new systems

The architecture of the new system has to conform with the existing plant boundary conditions and meet the relevant design requirements resulting from the failure criteria. The boundary conditions are:

— Availability of separate rooms for redundant trains;
— Availability of reserve capacity for the air conditioning and power supply systems and independence of the relevant subsystems servicing the separate rooms;
— Level of redundancy and diversity of existing transducers and sensors located in the process systems to measure the required safety parameters;

— Level of redundancy and diversity of final elements used to activate the safety systems and the related design of contactors and power bars in the switchgear.

The analysis of the architecture of the new system with respect to the boundary conditions set by the existing plant and equipment may limit the achievable failure tolerance and form the basis for the reliability analysis.

6.1.3. Comparison with the existing design basis

The re-engineered design basis specification of the I&C functions to be upgraded has to be complete, consistent and unambiguous. It forms a basis for the comparison of the requirements specification and the as-built documentation of the existing I&C systems. The main criteria for this comparison are:

— the reasons for preserving functions and for intended functional upgrades;
— the reasons for omitting functions from the intended upgrade;
— performance measures, e.g. response time;
— failure tolerance;
— reliability;
— testability for recurrent tests and the degree of self-checking performance;
— facilities available for conducting periodic proof testing;
— environmental conditions, including the level of electromagnetic interference to be tolerated;
— compatibility of signal interfaces with other systems.

6.1.4. Analysis of compatibility with existing systems

The design of the upgrade system based on the requirements specification from re-engineering differs from that for a new system in a new plant. In the latter case, the design is completed in a 'top down' manner and the functions assigned to the system will consequently be designed to be complete and consistent. The freedom in design for an upgrade will be constrained by the need to meet all the boundary conditions imposed by the existing plant, including available cabinet space, cable trays, links to the process information and alarm systems.

Consequently, significant effort ought to be spent in capturing the uses of the existing system and procedures, especially to identify whether originally unintended functions have been used and whether originally intended functions have been bypassed because they did not prove effective during plant operation. In addition, the way alarms are currently displayed and cleared, and conventions on alarm and trip protocols have to be considered for the design of the new systems.

6.2. DETAILED DESIGN PHASES

The detailed design phases of an advanced system are based on the requirements specification for the intended upgrade, namely:

— Functional specifications
— I&C system specification according to the fault tolerance requirements
— Boundary conditions for integration into the plant.

An engineering plan is prepared, including the important engineering or design activities with predefined input and output documentation (e.g. according to IEC 880 [16] or an equivalent procedure). Usually the detailed design for an upgrade consists of the following phases:

— design specification
— software design
— hardware design and procurement
— software coding
— system integration and model testing
— system testing and validation.

Design assessment and various analyses form an important part of the upgrade design work. Similarly, design verification is planned and executed at the end of every phase of the design.

6.3. ACCEPTANCE TESTING

The advanced system in general requires two types of acceptance testing before it is integrated into the plant. The first is the factory acceptance test of the total system with integrated hardware and software at the vendor's test facilities. This involves exhaustive tests, witnessed by both the designers and the plant operations staff. It includes essential functional tests, hardware tests, hardware and software integration tests, and any other special tests.

The second is the site acceptance testing, which is usually carried out after the system has been received, checked and installed but before any actuators have been connected. It provides plant conditions and proper interface with other station systems. This testing also allows correction of deficiencies detected after installation before the system is turned over for commissioning.

The site acceptance tests are carried out according to the plant design acceptance procedure. This procedure may include a checklist for verification and

acceptance of design documentation, quality assurance records, design verification and validation records, operating and testing manuals, training manuals, safety evaluation records and equipment lists.

6.4. INSTALLATION

As much as possible of the installation construction work that does not affect the existing system will be done during plant operation. The connection to existing measurement transducers and the introduction of break-in boxes for the actuator/controls may be done during an outage, allowing the data collection and other functions to be tested during normal operation of the existing system with the control signals from the new system disconnected. This on-site open loop test with outputs still disconnected is used to demonstrate the compatibility of the new digital system with the remaining existing I&C systems. This proof testing may be performed as a part of the backfitting. The control signals may be connected to the actuators instead of the existing system outputs using jumpers in the break-in boxes or via permanent connections in an outage.

6.5. COMMISSIONING

Commissioning is the final test or check-out after the system has been installed and accepted in the field condition; it is based on a commissioning specification and the associated work procedures. The commissioning specification is based on design requirements and is reviewed by the designers to ensure that all design issues have been covered.

The scope and extent of the commissioning specification can also be influenced by the category of the system or software. For example, the commissioning tests will be more rigorous for a category A system.

The commissioning work should be planned and scheduled. On completion of the commissioning, the results are verified and documented. The commissioning deficiencies are also documented and corrective actions identified. Specific design and operating documents may need to be updated following the commissioning.

Finally, the commissioning results are reviewed and accepted by the designers, operating staff, vendors and regulators.

6.6. OPERATION AND MAINTENANCE

Once the system is installed and commissioned in the plant, the functions and tasks of operating and maintaining the system become closely related. For a digital

I&C retrofitting project, the utility concerns include system operation, operational support services and the operating personnel. Operations staff have the task of keeping the digital system in safe and reliable operation during power generation and performing continuing and periodic surveillance and testing. Plant maintenance staff keep the digital system and components in an optimal state for safe and reliable operation and respond to operator needs by modifying the system to correct faults, improve performance or adapt it to a specified environment.

For safe and efficient operation of plant systems and equipment, operator behaviour is as important as equipment reliability. To permit human–machine interaction, operator control of the upgraded system may be required. Such control does not provide the operator with the capability of altering the stored program logic. If the upgraded system is safety related and operator parameter change facilities are available, appropriate procedures and/or locking devices have to be included to prevent the operator from inadvertently changing parameters which could affect the set points of the safety system.

An important element of the operator's function with respect to a digital safety system is performing periodic testing of all basic safety functions and major non-safety functions to verify the basic functional capabilities and to detect degradation. Special testing may be needed to detect failures that cannot be revealed by the self-checking provisions of the safety systems or by alarm or anomaly indications [16].

Data are collected and documented to record maintenance and repair activities during normal operation. Maintenance staff also deal with anomaly reporting, changes in functional requirements, technological evolution and changes in operating conditions. A procedure should be established to address the symptoms when an anomaly occurs and to document the system environment, system status, root causes, corrections, and particularly the software modification process [16].

To ensure software maintainability, the digital I&C maintenance personnel will plan for continuity of software engineering support, verification and validation, and performance monitoring to continuously assess the software and to maintain confidence in the operational system. In addition, software change control has to be maintained, spare parts have to be made available and software tools and supporting documentation need to be provided to the operations and maintenance staff.

GLOSSARY

The definitions given below may not necessarily conform to definitions adopted elsewhere for international use.

alarm. Audible and/or visible signal to alert the operator to events (including plant failures, equipment failures, loss of calibration and approach to permissible operating envelope) that require action by the operator.

common mode failure. A failure of a system to perform its functions owing to an unknown design or manufacturing fault in hardware or software, causing the required functions to fail in redundant trains at the same time. It is also a failure of a system to perform its function as a result of a common cause, where the defence in depth (multiple barrier, redundancy or diverse level of protection) has been breached.

configuration management. An integrated management process that identifies and documents the physical characteristics of a facility's structures, systems, components and computer software. It also ensures that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated in the facility documentation. Items under configuration control (e.g. documents, hardware, software) should be subject to a proper change control procedure.

defence in depth. Provision of several overlapping consecutive limiting barriers such that a given threshold can be surpassed only if all barriers have failed [16].

diversity. The existence of two or more different ways or means of achieving a specified objective. Diversity is specifically provided as a defence against common mode failure. It may be achieved by providing systems that are physically different from each other, or by functional diversity, where similar systems achieve the specific objective in different ways [40]. Diversity can also be achieved by the existence of redundant components or systems to carry out an identified function, where such components or systems operate under different conditions, have different sizes, different manufacturers and different working principles or involve different physical methods [28].

error. A human action or process that produces an unintended result.

failure. The delivery of an unintended action as a result of a fault being exercised.

fault. The effect of an error or deficiency such that the equipment performance would not be as intended if the fault were exercised.

fault tolerance. The built-in capability of a system to provide continued correct execution in the presence of a limited number of hardware or software faults.

function. A specific purpose or objective to be achieved, specified or described without reference to the physical means of achieving it.

functionality. A qualitative indication of the range or scope of the functions that a system or item of equipment can carry out. A system that carries out many complex functions has a 'high functionality'; a system that can only carry out a few simple functions has a 'low functionality'.

human factors engineering. The area of knowledge dealing with the capabilities and limitations of human performance in relation to the design of machines, jobs or modifications of the human's physical environment.

human–machine interface. The system through which operating and maintenance staff interact with the plant systems. The interface includes displays, controls, procedures and operator support systems.

instrumentation and control (I&C) system. A hardware and/or software implementation of automatic and manual controls, consisting of instrumentation, control and information systems.

performance. The effectiveness with which a function is carried out (e.g. time response, accuracy, sensitivity to parameter changes).

postulated initiating events. Events that lead to anticipated operational occurrences and accident conditions, their credible causal failure effects and their credible combinations.

redundancy. Provision of alternative (identical or diverse) elements or systems so that any one can perform the required function regardless of the state of operation or failure of any other [16, 26].

reliability. The probability that a system will meet its minimum performance requirements when called upon to do so.

safe operating envelope. Operating limits of the plant as defined by the nuclear safety analysis assumptions, constraints, data and conditions.

single failure criterion. A criterion (or requirement) applied to a system such that it is capable of performing its task in the presence of any single failure (including consequential failure). An assembly of equipment satisfies the single failure criterion if it can meet its purpose as defined in its requirements despite any single random failure assumed to occur anywhere in the assembly. Consequential failures resulting from the assumed single failure are part of the single failure.

software. Programs, procedures, rules and any associated documentation pertaining to the operation of a computer system.

validation. The test and evaluation of the integrated computer system (hardware and software) to ensure compliance with functional, performance and interface requirements [16, 39].

verification. The process of determining whether or not the product of each phase of the digital computer system development process fulfils the requirements of the previous phase [16, 39].

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Computerization of Operation and Maintenance for Nuclear Power Plants, IAEA-TECDOC-808, Vienna (1995).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Control Rooms and Man–Machine Interface in Nuclear Power Plants, IAEA-TECDOC-565, Vienna (1990).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Implementation of Computerized Operator Support Systems in Nuclear Installations, Technical Reports Series No. 372, IAEA, Vienna (1994).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Reliability of Computerized Safety Systems at Nuclear Power Plants, IAEA-TECDOC-790, Vienna (1995).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment of Computerized Control and Protection Systems, IAEA-TECDOC-780, Vienna (1994).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, The Role of Automation and Humans in Nuclear Power Plants, IAEA-TECDOC-668, Vienna (1992).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Control Room Systems Design for Nuclear Power Plants, IAEA-TECDOC-812, Vienna (1995).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Modern Instrumentation and Control for Nuclear Power Plants: A Guidebook, Technical Reports Series No. 387, IAEA, Vienna (in press).

[9] ELECTRIC POWER RESEARCH INSTITUTE, Guideline on Licensing Digital Upgrades, Rep. EPRI-TR-102348, Palo Alto, CA (1993).

[10] NATIONAL ACADEMY OF SCIENCES, Digital Instrumentation and Control Systems in Nuclear Power Plants: Safety and Reliability Issues, Final Report, National Academy Press, Washington, DC (1997).

[11] NUCLEAR REGULATORY COMMISSION, Digital Computer Systems for Advanced Light Water Reactors, SECY-91-292, US Govt Printing Office, Washington, DC (1991).
[12] NUCLEAR REGULATORY COMMISSION, Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs, Section II Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems, as clarified by the Staff Requirements Memorandum on SECY-93-087, US Govt Printing Office, Washington, DC (1993).
[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Implications of Computerized Process Control in Nuclear Power Plants, IAEA-TECDOC-581, Vienna (1991).
[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Based Aids for Operator Support in Nuclear Power Plants, IAEA-TECDOC-549, Vienna (1990).
[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Software Important to Safety in Nuclear Power Plants, Technical Reports Series No. 367, IAEA, Vienna (1994).
[16] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Software for Computers in the Safety Systems of Nuclear Power Stations, Rep. IEC 880, Geneva (1986).
[17] NUCLEAR REGULATORY COMMISSION, High Integrity Software for Nuclear Power Plants, Rep. NUREG/CR-6263, Vols 1, 2, US Govt Printing Office, Washington, DC (1995).
[18] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Guide to Software Requirements Specification, Rep. IEEE-830, New York (1984).
[19] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Standard for Software Unit Testing, Rep. IEEE-1008, New York (1987).
[20] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Standard for Software Verification and Validation Plans, Rep. IEEE-1012, New York (1986).
[21] CANDU OWNERS GROUP, Guideline for Categorization of Software in Nuclear Power Plant Safety, Control, Monitoring and Testing Systems, Rep. COG-95-264, Toronto (1995).
[22] CANDU OWNERS GROUP, Guide for the Qualification of Software Products, Rep. COG-95-179, Toronto (1995).
[23] CANDU OWNERS GROUP, Investigation of Environmental Qualification and Qualification of Embedded Software for Smart Instruments, Rep. COG-94-206, Toronto (1994).
[24] ATOMIC ENERGY CONTROL BOARD, Software in Protection and Control Systems, Regulatory Guide, Rep. C138, AECB, Ottawa (1996).
[25] AMERICAN NATIONAL STANDARDS INSTITUTE/INSTITUTE OF ELECTRICAL AND ELECTRONIC ENGINEERS/AMERICAN NUCLEAR SOCIETY, Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations, ANSI/IEEE/ANS 7-4.3.2 (1993).
[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety-Related Instrumentation and Control Systems for Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D8, IAEA, Vienna (1984).
[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and other Nuclear Installations, Code and Safety Guides Q1–Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).

[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Design, Safety Series No. 50-C-D (Rev. 1), IAEA, Vienna (1988).

[29] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection System and Related Features in Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D3, IAEA, Vienna (1980).

[30] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Instrumentation and Control Systems Important for Safety — Classification, Rep. IEC 1226, Geneva (1993).

[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Governmental Organization, Safety Series No. 50-C-G (Rev. 1), IAEA, Vienna (1988).

[32] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Siting, Safety Series No. 50-C-S (Rev. 1), IAEA, Vienna (1988).

[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Functions and Component Classification for BWR, PWR and PTR: A Safety Guide, Safety Series No. 50-SG-D1, IAEA, Vienna (1979).

[34] INTERNATIONAL ATOMIC ENERGY AGENCY, Code on the Safety of Nuclear Power Plants: Operation, Safety Series No. 50-C-O (Rev. 1), IAEA, Vienna (1988).

[35] INTERNATIONAL ATOMIC ENERGY AGENCY, Manual on Quality Assurance for Computer Software Related to the Safety of Nuclear Power Plants, Technical Reports Series No. 282, IAEA, Vienna (1988).

[36] INTERNATIONAL ATOMIC ENERGY AGENCY, Verification and Validation of Software Related to Nuclear Power Plant Control and Instrumentation, Technical Reports Series No. 384, IAEA, Vienna (in press).

[37] INTERNATIONAL ELECTROTECHNICAL COMMISSION, General Principles of Nuclear Reactor Instrumentation, Rep. IEC 231 (plus supplements), Geneva (1975).

[38] INTERNATIONAL ELECTROTECHNICAL COMMISSION, High-Voltage Coaxial Connectors used in Nuclear Instrumentation, Rep. IEC 498, Geneva (1975).

[39] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Programmed Digital Computers Important to Safety for Nuclear Power Stations, Rep. IEC 987, Geneva (1989).

[40] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Functional Design Criteria for a Safety Parameter Display System for Nuclear Power Stations, Rep. IEC 960, Geneva (1988).

[41] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Design for Control Rooms of Nuclear Power Plants, Rep. IEC 964, Geneva (1989).

[42] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Control Rooms — Operator Controls, Rep. IEC 1227, Geneva (1993).

[43] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Main Control Room — Verification and Validation of Design, Rep. IEC 1771, Geneva (1995).

[44] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants — Main Control Room —. Application of Visual Display Units (VDU), Rep. IEC 1772, Geneva (1995).

[45] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Methods for Qualifying Equipment for Harsh and Mild Environment, Rep. IEEE-323, New York (1983).

[46] NUCLEAR REGULATORY COMMISSION, Advanced Human–System Interface Design Review Guideline, Rep. NUREG/CR-5908, Vols 1, 2, US Govt Printing Office, Washington, DC (1994).

[47] ELECTRIC POWER RESEARCH INSTITUTE, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications, Final Report, EPRI-TR-106439, Palo Alto, CA (1996).

[48] NUCLEAR REGULATORY COMMISSION, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, Ch. 7, Instrumentation and Control, Rep. NUREG-0800, Rev. 4, Washington, DC (1996).

[49] HEALTH AND SAFETY EXECUTIVE, Tolerability of Risk from Nuclear Power Plants, HSE Bodes, Sudbury (1991).

[50] HEALTH AND SAFETY EXECUTIVE, Safety Assessment Principles for Nuclear Plants, HSE Bodes, Sudbury (1992).

[51] GALLAGHER, J.M., "Licensing issues of computer-based systems important to safety", presented at Special Issues Mtg of Committee on Nuclear Regulatory Activities and Committee on the Safety of Nuclear Installations, Paris, 1996.

[52] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Expert Systems in Nuclear Safety, IAEA-TECDOC-542, Vienna (1990).

[53] INTERNATIONAL ATOMIC ENERGY AGENCY, Advanced Information Methods and Artificial Intelligence in Nuclear Power Plant Control Rooms (Proc. IAEA Specialists Mtg Halden, 1994), IAEA-12-SP-384.37, Vienna (1994).

[54] NUCLEAR ENERGY AGENCY OF THE ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, Specialist Meeting on Operator Aids for Severe Accident Management and Training, Rep. NEA/CSNI/R(93)9, Paris (1993).

[55] INTERNATIONAL ATOMIC ENERGY AGENCY, Manual on Quality Assurance for Installation and Commissioning of Instrumentation, Control and Electrical Equipment in Nuclear Power Plants, Technical Reports Series No. 301, IAEA, Vienna (1989).

CONTRIBUTORS TO DRAFTING AND REVIEW

Baldwin, J.	AEA Technology, United Kingdom
Bastl, W.	Institute for Safety Technology, Germany
Basu, S.	Ontario Hydro, Canada
Berg, O.	OECD Halden Reactor Project, Norway
Bock, H.-W.	Siemens, Germany
Dusic, M.	International Atomic Energy Agency
Jung, C.-H.	Korea Atomic Energy Research Institute, Republic of Korea
Juslin, K.	VTT Automation, Finland
Kossilov, A.	International Atomic Energy Agency
Leret, E.	Electricité de France, France
Pobedonostsev, A.B.	Bureau of Machine Building, Russian Federation
Schildt, G.H.	Technische Universität Wien, Austria
Sun, B.K.H.	Sunutech, United States of America
Wach, D.	Institute for Safety Technology, Germany
Wall, D.N.	Nuclear Installations Inspectorate, United Kingdom

Consultants Meetings

Vienna, Austria: 28 August–1 September 1995,
11–15 March 1996, 5–9 May 1997

No. 8, October 1998

WHERE TO ORDER IAEA PUBLICATIONS

☆ ☆ **In the United States of America** the exclusive sales agent for IAEA publications, to whom all orders and inquiries should be addressed, is:

Bernan Associates, 4611-F Assembly Drive, Lanham, MD 20706-4391, USA
Telephone: 1-800-274-4447 (toll-free) • Fax: (301) 459-0056 / 1-800-865-3450 (toll-free)
E-mail: query@bernan.com • Web site: http://www.bernan.com

☆ ☆ **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 Hunter Publications, 58A Gipps Street, Collingwood, Victoria 3066
Telephone: +61 3 9417 5361 • Fax: +61 3 9419 7154 • *E-mail: jpdavies@ozemail.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
E-mail: jean.de.lannoy@infoboard.be • Web site: http://www.jean-de-lannoy.be

BRUNEI Parry's Book Center Sdn. Bhd., 60 Jalan Negara, Taman Melawati, 53100 Kuala Lumpur, Malaysia
Telephone: +60 3 4079176, 4079179, 4087235, 4087528 • Fax: +60 3 407 9180
E-mail: haja@pop3.jaring.my • Web site: http://www.mol.net.my/~parrybook/parrys.htm

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

DENMARK Munksgaard Subscription Service, Nørre Søgade 35, P.O. Box 2148, DK-1016 København K
Telephone: +45 33 12 85 70 • Fax: +45 33 12 93 87
E-mail: subscription.service@mail.munksgaard.dk • Web site: http://www.munksgaard.dk

EGYPT The Middle East Observer, 41 Sherif Street, Cairo
Telephone: +20 2 3939 732, 3926 919 • Fax: +20 2 3939 732, 3606 804 • *E-mail: fouda@soficom.com.eg*

FRANCE Nucléon, Immeuble Platon, Parc les Algorithmes,F-91194 Gif-sur-Yvette, Cedex
Telephone: +33 1 69 353636 • Fax +33 1 69 350099 • *E-mail: nucleon@wanadoo.fr*

GERMANY UNO-Verlag, Vertriebs- und Verlags GmbH, Poppelsdorfer Allee 55, D-53115 Bonn
Telephone: +49 228 94 90 20 • Fax: +49 228 21 74 92
Web site: http://www.uno-verlag.de • E-mail: unoverlag@aol.com

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

INDIA Viva Books Private Limited, 4325/3, Ansari Road, Darya Ganj, New Delhi-110002
Telephone: +91 11 327 9280, 328 3121, 328 5874 • Fax: +91 11 326 7224
E-mail: vinod.viva@gndel.globalnet.ems.vsnl.net.in

ISRAEL YOZMOT Ltd., 3 Yohanan Hasandlar St., P.O. Box 56055, IL-61560 Tel Aviv
Telephone: +972 3 5284851 • Fax: +972 3 5285397

ITALY Libreria Scientifica Dott. Lucio di Biasio "AEIOU", Via Coronelli 6, I-20146 Milan
Telephone: +39 2 48 95 45 52 or 48 95 45 62 • Fax: +39 2 48 95 45 48

JAPAN Maruzen Company, Ltd., P.O. Box 5050, 100-31 Tokyo International
Telephone: +81 3 3272 7211 • Fax: +81 3 3278 1937 • *E-mail: yabe@maruzen.co.jp • Web site: http://www.maruzen.co.jp*

MALAYSIA Parry's Book Center Sdn. Bhd., 60 Jalan Negara, Taman Melawati, 53100 Kuala Lumpur,
Telephone: +60 3 4079176, 4079179, 4087235, 4087528 • Fax: +60 3 407 9180
E-mail: haja@pop3.jaring.my • Web site: http://www.mol.net.my/~parrybook/parrys.htm

NETHERLANDS Martinus Nijhoff International, P.O. Box 269, NL-2501 AX The Hague
Telephone: +31 793 684 400 • Fax: +31 793 615 698 • *E-mail: info@nijhoff.nl • Web site: http://www.nijhoff.nl*

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

POLAND Foreign Trade Enterprise, Ars Polona, Book Import Dept., 7, Krakowskie Przedmieście Street, PL-00-950 Warsaw
Telephone: +48 22 826 1201 ext. 147, 151, 159 • Fax: +48 22 826 6240
E-mail: ars_pol@bevy.hsn.com.pl • Web site: http://www.arspolona.com.pl

SINGAPORE Parry's Book Center Pte. Ltd., 528 A MacPHERSON Road, Singapore 1336
Telephone: +65 744 8673 • Fax: +65 744 8676
E-mail: haja@pop3.jaring.my • Web site: http://www.mol.net.my/~parrybook/parrys.htm

SLOVAKIA Alfa Press, s.r.o, Račianska 20, SQ-832 10 Bratislava • Telephone/Fax: +421 7 566 0489

SPAIN Díaz de Santos, Lagasca 95, E-28006 Madrid
Telephone: +34 91 431 24 82 • Fax: +34 91 575 55 63 • *E-mail: madrid@diazdesantos.es*

Díaz de Santos, Balmes 417–419, E-08022 Barcelona
Telephone: +34 93 212 86 47 • Fax: +34 93 211 49 91 • *E-mail: balmes@diazsantos.com*
General E-mail: librerias@diazdesantos.es • Web site: http://www.diazdesantos.es

UNITED KINGDOM The Stationary Office Ltd, International Sales Agency, 51 Nine Elms Lane, London SW8 5DR
Telephone: +44 171 873 9090 • Fax: +44 171 873 8463
E-mail: Orders to: book.orders@theso.co.uk • Enquiries to: ipa.enquiries@theso.co.uk
Web site: http://www.the-stationery-office.co.uk

☆ ☆ Orders (except for customers in the USA) and requests for information may also be addressed directly to:

98-01699

Sales and Promotion Unit, International Atomic Energy Agency
Wagramer Strasse 5, P.O. Box 100, A-1400 Vienna, Austria
Telephone: +43 1 2600 22529 (or 22530) • Facsimile: +43 1 2600 29302
E-mail: sales.publications@iaea.org • Web site: http://www.iaea.org/worldatom/publications

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 92–0–103298–6
ISSN 1020–6450