IAEA-TECDOC-952

Advanced control systems to improve nuclear power plant reliability and efficiency

Report prepared within the framework of the International Working Group on Nuclear Power Plant Control and Instrumentation

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

The IAEA does not normally maintain stocks of reports in this series. However, microfiche copies of these reports can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 100,— in the form of a cheque or in the form of IAEA microfiche service coupons which may be ordered separately from the INIS Clearinghouse.

The originating Section of this publication in the IAEA was:

Nuclear Power Engineering Section
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

ADVANCED CONTROL SYSTEMS TO IMPROVE
NUCLEAR POWER PLANT RELIABILITY AND EFFICIENCY
IAEA, VIENNA, 1997
IAEA-TECDOC-952
ISSN 1011-4289

Printed by the IAEA in Austria
July 1997

FOREWORD

Considerable advancement has been made in computer and information technology in the last decades leading to extensive and large-scale implementation of digital control systems in the process industry and conventional power plants The implementation of modern control systems allows these plants to operate more productively and efficiently than the ones using analog technology Similar trends have been observed in the nuclear industry

The IAEA Advisory Group Meeting on Advanced Control Systems to Improve Nuclear Power Plant Reliability and Efficiency was held in Vienna, 13-17 March, 1995 It was a consequence of the recommendations of the IAEA International Working Group on Nuclear Power Plant Control and Instrumentation (IWG-NPPCI) to produce practical guidance on the application of the advanced control systems available for nuclear power plant operation The meeting prepared an extended outline of a new technical report and suggested that the report should be published as a TECDOC and distributed to *nuclear utilities in Member States as well to main design organizations*

This TECDOC is the result of a series of a advisory and consultants meetings held by the IAEA in 1995-1996 in Vienna (March 1995), in Erlangen, Germany (December 1995), in Garching, Germany (June 1996) and in Vienna (November 1996) It was prepared with the participation and contributions of experts from Austria, Canada, Finland, France, Germany, the Republic of Korea, Norway, the Russian Federation, the United Kingdom and the United States of America

The publication not only describes advanced control systems for the improvement of nuclear power plant reliability and efficiency, but also provides a road map to guide interested readers to plan and execute an advanced instrumentation and control project The subjects include identification of needs and requirements, justification for safety and user acceptance, and the development of an engineering process The report should be of interest to nuclear power plant staff, I&C system designers and integrators as well as regulators and researchers

Special thanks are due to B K H Sun of Sunutech, Inc (USA), who chaired all the working meetings and edited the report A Kossilov, who initiated the project, and V Neboyan, who completed the work for the Nuclear Power Engineering Section, Division of Nuclear Power and the Fuel Cycle, are the IAEA officers responsible for the preparation of this publication

EDITORIAL NOTE

In preparing this publication for press, staff of the IAEA have made up the pages from the original manuscript(s). The views expressed do not necessarily reflect those of the governments of the nominating Member States or of the nominating organizations.

Throughout the text names of Member States are retained as they were when the text was compiled.

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

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

CONTENTS

1. INTRODUCTION

Many nuclear power plants in operation today were designed and built with technology from the 1960s and 1970s Major reasons which consist of (a) obsolescence, (b) lack of spare parts and original equipment manufacturer support, (c) challenges to availability due to unnecessary plant trips, (d) component failures due to aging, and (e) high maintenance and testing costs, have resulted in the need to replace analog-based instrumentation and control (I&C) equipment and systems with digital technology in current nuclear power plants

Considerable progress in digital and automation technology has been made in the last two decades leading to extensive and large-scale use of digital I&C systems in the process industry and conventional power plants The deployment of modern I&C systems has allowed these plants to operate more productively and efficiently than the old analog-based plants Safety and licensing considerations have however restricted the roles of new technology in nuclear power plants Consequently, the potential and the advantage of the digital technology have not been fully realized in nuclear applications [1 1] Nevertheless, considerable progress has been made in the application of digital I&C systems and components during backfitting of existing nuclear power plants around the world

1 1 OBJECTIVES

The objective of the report is to bring together international experience on the application of digital technology to provide guidance and to promote good engineering process for IAEA member countries when introducing digital instrumentation and control systems in their nuclear power plants Specific objectives are

- To help plan, develop, and implement control, instrumentation, protection and human-machine systems for operating nuclear power plants
- To help develop technically sound and cost effective approaches and implementation strategies in qualification, verification and validation and to address regulatory approval for digital safety systems
- To promote research and development of advanced technologies for improvement of safety, reliability, and productivity of present and future nuclear installations
- To promote user and licensing acceptance of digital instrumentation and control upgrades

The report is designed for readers in the following categories

- Engineers, managers, and operators of power companies
- Engineers and managers of design and architect engineering companies
- Government licensing and regulatory staff who review, evaluate, audit and license nuclear systems and equipment
- Scientists and engineers in research and development organizations including universities and laboratories who are interested in advancing the state-of-the-art

1 2 SCOPE

The report covers current plant needs and requirements, indicates how these needs can be met and identifies relevant standards, codes and practices that may be applied It addresses the recent experiences and developments of nuclear power plant I&C systems The report also identifies the features of advanced I&C systems and the relevant issues associated with user acceptance and safety justification It also describes the engineering process and future trends concerning digital I&C Several national standards and guidelines for advanced I&C systems are described with the intention to illustrate a few examples In addition, country reports are provided by the contributors to the drafting of this report to illustrate certain specific examples of advanced I&C applications in their country

The I&C systems addressed in this report include instrumentation, control systems, protection and safety systems, operation and maintenance aids, and monitoring and diagnostics systems, information management systems, and engineering support The report does not address specifically the detailed human factor principles, the control room human-machine interface, nor the national licensing rules

REFERENCE

[1 1] TAYLOR, J J , SUN, B K H , Applications of Computers to Nuclear Power Plant Operations, Nuclear News (1990) 38-40

2. TERMINOLOGY, STANDARDS AND CODES OF PRACTICE

This chapter first introduces the terminology used in the document in Section 2 1, then goes on to describe the framework of the standards in Section 2 2, which are developed in detail in section 2 3 National standards which are often central to the national licensing process have been documented separately with a few examples in Appendix A

The content of this chapter is structured to guide the reader through the area of standards and codes of practice, covering much of the background information important to plant licensing and to gaining acceptance of a digital I&C system The reader should not expect to find a comprehensive set of standards and codes of practice in this document, in part due to the rapid development of digital technology The lag of the standards and codes of practice material behind the current state of the art is reflected in the large number of supporting documents identified in the text The extensive reference to IAEA TECDOCs is deliberate, as these documents are seen as indicating international consensus on current practice and providing information on national experience supplementing that given at the end of this publication

2 1 TERMINOLOGY

There are many definitions used in discussion of the systems and their standardization, unfortunately the use of terminology is not always consistent between standard bodies nor, sometimes, within one standard organization Two areas of particular concern are those of system classification and of definitions relating to error, fault and failure For the present report, caution has been taken to account for various sources of information, including those from IEC and IAEA documents

Alarm
Audible and/or visible signal to alert the operator to events including plant failures, equipment failures, loss of calibration and approach to the permissible operating envelope, that requires action by the operator

Common Mode Failure (CMF)
A failure of a system caused by an unknown design or manufacturing fault in a hardware or software module in such a way that by a triggering by an internal or external event all modules of this type fail at the same time Redundancy by identical means may be a suitable countermeasure against CMF, only if by additional design measures, the effect of possible events is reduced to one channel of the system Random common cause failures are equivalent to a single failure

Computer
A programmable functional unit that consists of one or more associated processing units and peripheral equipment, that is controlled by internally stored programs and that can perform substantial computation including arithmetic and logic operations without human intervention during a run (IEC 987 and 880)

Computer Program
A set of ordered instructions and data that specify operations in a form suitable for execution by a digital computer (IEC 880)

Control Room
The location containing the primary human-machine interface for operator interaction with the plant

Defense in Depth
Provision of several overlapping barriers arranged such that the unwanted event occurs only if all the barriers have failed (IEC 880)

Display
A device used to indicate plant or equipment status, including visual display units, lamps, meters, etc

Diversity
The existence of two or more different and independent ways or means of achieving a specified objective Diversity is specifically provided as a defense against common mode failure It may be achieved by providing systems that are physically different from each other, or by functional diversity, where systems achieve the specified objective by offering different treatments, based on different measures

Error
A human action or process that produces an unintended result

Failure
The failure of a system results that either an intended function is not performed on demand or an unintended function is initiated

Fault
Faults in a system may be the result of design errors of hardware or software or may be caused by aging or wear or by environmental stress on the hardware of a system

Human-Machine Interface
The system through which the operating or maintenance staff interact with the plant systems

Operator Support System
A system that provides support to the operator by taking plant information and interpreting it for display to the operator in order to reduce the load of processing that the operator is required to perform

Redundancy
Provision of more than the minimum number of (identical or diverse) elements or systems with the goal to avoid the loss of the required function so that the loss of elements or systems according to the required failure tolerance does not result in the loss of the required function as a whole

Safety System
Systems important for safety provided to ensure in any condition the safe shutdown of the reactor and heat removal from the core and/or to limit the consequences of any Postulated Initiating Event or significant sequence

Safety Related System
A system that is important to safety but which is not itself a safety system

Scalability
The ability to increase the level of redundancy capacity or performance of a system by replication of the modules in that system

Signal Trajectory
A set of time histories of a group of signals, or of equipment conditions, which results in a particular output state of a system

Single Failure Criterion
An assembly of equipment satisfies the single failure criterion if it can meet its required purpose despite the occurrence of any single random failure anywhere in the assembly Consequential failures resulting from the single failure are considered to be part of the single failure

Software Life Cycle
The period of time that starts when a software product is conceived and ends when the product is no longer available for use The software life cycle typically includes a requirements phase, design phase, implementation phase, test phase, installation and checkout phase, operation and maintenance phase (IEC 880)

Validation
The test and evaluation of the integrated computer system indulging hardware and software to ensure compliance with the functional, performance and interface requirements (IEC 880 and 987)

Verification
The process of determining whether or not the product of each design phase of the digital computer system development process fulfills the requirements of the previous phase of the life-cycle process (IEC 880 and 987)

2 2 STANDARDS FRAMEWORK

Standards are usually promoted by trade requirements to allow interconnection of equipment and to promulgate good practice Nuclear sector standards not only contain these elements, but also put significant emphasis on safety matters The development of national and international standards, often led by trade organizations, also allows economic and safety advantage to be taken of the availability of compatible equipment from multiple suppliers The development of the nuclear systems market, in particularly the emerging dominance of multinational suppliers, is increasing the importance of international standards

There are a number of established sources of rules and standards for I&C systems for nuclear power plant including

- IAEA NUSS guides and their development in the Safety Guide Series supported by documents in the technical Report Series
- International Standards as developed by ISO (International Standards Organization) and IEC (International Electrotechnical Commission) who establish requirements and make recommendations on technical matters
- National standards and codes of practice, which are often the precursors of the international standard on the equivalent topic
- Company specific standards, which are often the most prescriptive and detailed of the standards, and also are most readily changed at a local level in response to changes in technology and practices

2 3 INTERNATIONAL STANDARDS AND GUIDELINES

The international standards and guidelines are discussed in two parts First, the material developed by the IAEA which takes the form of internationally agreed guides given in the Technical Reports and TECDOC (Technical Document) series Second, the international standards, particularly those developed by the IEC that are well recognized and accepted in the nuclear sector

2.3.1. IAEA publications

The IAEA instrumentation and control information falls into two groups The first group of documents produced and published by the IAEA follow a formal procedure of agreement by an international committee These documents are the NUSS guides, Safety Guides and INSAG documents The documents in this group include the following

- 50-C-D, Code on the Safety of Nuclear Power Plants Design, Rev 1 (1988)
- 50-C-O, Code on the Safety of Nuclear Power Plants Operation, Rev 1 (1988)
- 50-C-QA, Code on the Safety of Nuclear Power Plants Quality, Rev 1 (1988)
- Safety Series No 50-SG-D3, IAEA Safety Guide, Protection System and Related Features in Nuclear Power Plants (1980)
- Safety Series No 50-SG-D8, IAEA Safety Guide, Safety-Related Instrumentation and Control Systems for Nuclear Power Plants (1984)
- 75-INSAG-3, Basic Safety Principles for Nuclear Power Plants, A report by the International Nuclear Safety Advisory Group, IAEA, Vienna (1988)

The second group of IAEA documents are produced by international teams assembled by the IAEA to develop a consensus view However, they are not subject to a formal review and approval procedure The two types of documents are Technical Reports, TECDOCs Specific examples of document are

- Technical Reports Series No 282, Manual on Quality Assurance for Computer Software Related to the Safety of Nuclear Power Plants (1988)
- Technical Reports Series No 372, Development and Implementation of Computerized Operator Support Systems in Nuclear Installations (1994)
- IAEA-TECDOC-444, Improving nuclear power plant safety through operator aids, guidelines for selecting operator aids (1987)
- IAEA-TECDOC-529, User requirements for decision support systems used for nuclear power plant accident prevention and mitigation (1988)
- IAEA-TECDOC-542, Use of expert systems in nuclear safety (1990)
- IAEA-TECDOC-549, Computer based aids for operator support in nuclear power plants (1990)
- IAEA-TECDOC-581, Safety implications of computerized process control in nuclear power plants (1991)
- IAEA-TECDOC-660, Expert systems in the nuclear industry (1992)
- IAEA-TECDOC-668, The role of automation and humans in nuclear power plants (1992)
- IAEA-TECDOC-700, The potential of knowledge based systems in nuclear installations (1993)
- IAEA-TECDOC-762, Operator support systems in nuclear power plants (1994)
- IAEA-TECDOC-780, Safety assessment of computerized control and protection systems (1994)
- IAEA-TECDOC-808, Computerization of Operation and Maintenance for Nuclear Power Plants (1995)
- IAEA-TECDOC-912, Computerized supported systems in nuclear power plants (1996)

It is noted that the TECDOCs and related material contain a considerable amount of information relating to emerging technology and issues where there has been only a limited amount of work on standards which is in part due to the rapid evolution of the technology and practices

Finally, in addition to the regular publications valuable material comes from the IAEA International Working Group on Nuclear Power Plant Control and Instrumentation and from international meetings sponsored by the IAEA including the following

- Specialists Meeting on Communication and data transfer in NPP, Lyon, France 24-26 April 1990
- Technical Committee Meting/Workshop on Practical Experience With Expert System Applications in Nuclear Safety, Moscow, USSR, 1-5 October 1990
- Specialists Meeting on Advanced Information Methods and Artificial Intelligence in Nuclear Power Plant Control Rooms, Halden, Norway, 13-15 September 1994

These documents are often quite valuable as they report the experience arising from recent developments and deployment of advanced systems and often describe both the technical and regulatory issues encountered

2.3.2. International standards

There are many international standards relating to advanced I&C The most relevant to nuclear systems are those produced by IEC 45, particularly those of IEC Sub-committee 45A (Reactor Instrumentation), which is dedicated to the production of standards in the field of Instrumentation and Control of Nuclear Reactors These standards are taken as parent documents of the IAEA NUSS documents and Safety Guides

The key IEC standards relating to digital I&C systems include the following

- IEC 880, Software for computers in the safety systems of nuclear power stations, First edition (1986) This standard defines a life cycle for the safety-classified computer based systems and develops requirements applicable to software through the life cycle Detailed recommendations are provided in a set of appendices
- IEC 987, Programmed digital computers important to safety in nuclear power plant, First edition, (1989) This standard gives requirements on project structure and the hardware from requirements through design, development to the end of the life of the hardware
- IEC 1226, Nuclear power plants instrumentation and control systems important to safety, - Classification, First edition (1993) This standard addresses the categorization of I&C functions, systems and equipment (FSE), based on the consequence of a possible initiating event (deterministic approach), then gives general requirements for each category of I&C systems (application of IEC 880, reliability, quality assurance, etc)

The IEC 45A Sub-Committee is currently progressing a number of projects some of which are linked to IEC 880 and IEC 1226 Some of the examples are

- Supplement 1 to IEC 880 this supplement addresses some of the topics missing in the IEC 880 edition 1, such as diversity, use of formal methods, use of pre-existing software products, and use of software engineering tools
- IEC 1513, General requirements for computer based systems important to safety this forms a system level document above the IEC 880 (software aspects) and the IEC 987 (hardware aspects) standards It will provide a nuclear specific standard with a scope equivalent to IEC 1508
- Supplement to IEC 1226, It deals with a risk based approach possible for categorization of I&C functions, systems and equipment

The standards relating to the design of the control room include IEC 964, Design for control rooms of nuclear power plants, First edition, 1989 This standard defines the activities related to analysis, design, implementation and verification and validation of control rooms in nuclear power plants Two further standards that develop the detail of aspects of IEC 964 are published in 1995, these are

- IEC 1772, Nuclear power plants Main control room - Application of visual display units (VDU), First Edition (1995)
- IEC 1771, Nuclear power plants Main control room - Verification and validation of design, First Edition (1995)

In addition to these nuclear specific standards IEC Technical Committee 65 has development in progress a system standard, IEC 1508, Functions of Safety I&C Systems It will be a safety pilot standard for all industrial sectors and cover the whole life cycle of I&C systems containing electrical, electronic and programmable devices that are important to safety The standard is in seven parts

- Part 1 defines a safety life cycle in parallel with the system life cycle and categorizes a system according to its importance for the safety of the process Four categories of systems important to safety are defined
- Part 2 defines hardware requirements for an electrical/electronic/programmable electronic system
- Part 3 defines software requirements

- Part 4 provides definitions
- Parts 5&6 provide guidance on the application of the parts 1, 2 & 3
- Part 7 presents a bibliography of engineering techniques referenced in parts 2 & 3 The publication of the seven parts is planned for 1997 and 1998

There is also IEC 1069, Assessment of properties of a I&C system This standard will have eight parts and define properties, a general assessment method and address the assessment of each property including functionality, performance, dependability, operability, security and properties independent from the task (e g quality assurance)

Other IEC and ISO Committees also exist which define standards on specific topics independent of any application sector including

- IEC TC 56 on dependability of technical systems, whose scope includes the management of risk, requirements for dependability and the software aspects of dependability
- ISO JTC1/SC7 on information technology
- ISO/IEC 12207 on software life cycle, which describes software engineering processes
- ISO TC 176 dealing with quality matters with the following standards
  - ISO 9001, 9002, 9003, Quality assurance in design, development, production, installation, inspection, test
  - ISO 9000-3, Software Quality Assurance
  - ISO 9004-1, Dependability of software

These are widely accepted as basic quality standards to be applied to any system development process The committee is also preparing ISO 9004-2 to 7 Quality Assurance in services, material, quality improvement, project management, quality plan and configuration management

3. NUCLEAR POWER PLANT NEEDS AND REQUIREMENTS

3 1 INTRODUCTION

There has been a major change in nuclear power plant needs during the past 40 years During the 1950s and 1960s the industry was developing nuclear power technology and most of the effort was directed at developing new nuclear processes and the corresponding instrumentation and control (I&C) systems to monitor and control the new nuclear equipment and systems Economic consideration influenced development efforts in the latter years In the 1970s the need to improve plant construction and operating costs became apparent and I&C system developments were primarily directed at improving the plant cost and reliability as well as meeting seismic and environmental qualifications to survive nuclear accidents Radiation monitoring instrumentation was also improved during this period as the requirements for employee and public safety with respect to radiation exposure became more stringent

During the 1980's and 1990's the nuclear industry had to respond to low public acceptance of nuclear power plants following the Three Mile Island and Chernobyl accidents which appeared identical to the public despite their different consequences Regulatory demands for more stringent safety requirements and better assurance of equipment performance at the plant's end-of-life also created significant work with respect to risk assessment, environmental qualification and retrofitting As the plants age, equipment related problems such as component failure and obsolescence have become very critical

The various issues and concerns surrounding the NPP have created the need for more creative I&C solutions The needs have also opened the door for new I&C related products that reach out well beyond the traditional plant control loop These products have been made possible by recent advances in I&C and digital technology They include digital I&C, computerized calibration tools, testing and maintenance tools, real time process surveillance and diagnostic systems, engineering analysis and simulation tools, and more advanced fault tolerant control systems that can allow the plant to operate until it can be conveniently shutdown for repairs

3 2 CURRENT ISSUES AND CONCERNS

3.2.1. Plant performance, reliability and safety

While safety performance of nuclear power plants remains a key issue, improvement in plant capacity factor is equally important for economic and continued viability of many plants The development of a competitive and deregulated electricity generation market, for example in the UK and the USA, has driven the need for lower operating and maintenance cost and greater production capacity factor

Many plants have seen their capacity factor dropping over the years and are struggling to reach values above 80% The capacity factor improvement will require reduction of spurious trips, forced outages, forced derating, unscheduled maintenance outages and avoidance of outage extension

The reduction in plant performance is due in part to equipment failure and system performance degradation due to aging and other factors that becomes more common There is also increasing demand on the plant to meet more stringent safety and regulatory requirements as well as accommodate more flexibility in plant operation, e g , load following and achieve higher output for example by unit uprating It is necessary that plant system and procedural modifications are made to meet these demands

The plant modifications and equipment aging have affected system performance For I&C, there has been noticeable increase in instrument drift which need correction through calibration The process system performance has degraded or shifted leading to lower safety tolerances and operating margins

For example, the Candu heat transport temperature has increased over the years due to boiler and heat exchanger fouling (poor chemistry performance) The consequence has been lower safety and operating margins, the associated penalty of lower operating power level and the cost of modification programs such as the steam generator cleaning or replacement The capacity factor has decreased in many plants and has been a major concern for both the utilities and the regulators

The plant performance and safety issues receive serious attention by the utility management and the regulators and are also the subject of formal reviews such as peer evaluation and regulatory review Some of the performance indicators used for this review process are number of spurious trips (unplanned scrams), safety system failure (impairment or unavailability), capacity factor, significant event reports, environmental emissions and radiation dose Novel ideas including the use of advanced I&C technology are needed to improve the performance indicators

3.2.2. Safety and licensing issues

The safety and licensing issues have become very high profile because of negative public perception of NPP safety Consequently the plant safety and licensing requirements have increased over the years and are always under close scrutiny by the regulatory agencies and the governments The requirements are changing and the licensing process has become more stringent The licensing process for any change in the plant including modification, renovation or upgrade is much more onerous The regulatory authorities have expanded their watch-dog roles, which can be classified as prescriptive, monitoring, coordinative, and advisory This has put more demands on the NPP and the need for more nuclear safety staff

The safety requirements are in general based on the principle of defense in depth and countermeasures against common mode system failures But in reality all the resulting requirements including diversity, independence, separation, redundancy and single failure criteria can not always be fully met in existing design The change in safety requirements makes I&C modification difficult, particularly in applying current safety standards to plants built to yesterday's standards Probabilistic safety assessment of existing plant and other safety evaluations have resulted in the need for NPP retrofit or safety upgrade The regulators are expecting more from the plant operators in all these areas and demanding closer compliance to current requirements The regulators are also demanding a change in the trend of the safety performance indicators including spurious trips or scrams, safety system failure, significant event reports, radiation dose

While technical performance expectations have always been very demanding, far more attention is now being paid to quality assurance issues Procedural compliance during the course of work, as verification and validation and the associated documentation are now seen to be more important Today the replacement of redundant safety systems follows a much more rigorous process to ensure that common mode failures cannot reduce plant safety This requires special proves for computer based systems with the same hardware and software in the redundant channels

3.2.3. Maintenance, testing and operational issues

Maintenance activities and the associated cost have increased considerably as plants age The problem stems from a lack of or an inadequate manufacturer's documentation and technical specification, shortage of spare parts, poor material management, inadequate configuration control and lack of modern diagnostic and maintenance tools Some of the current systems are difficult to maintain and are not user friendly Effort is needed to develop better maintenance strategies for these systems using techniques such as the reliability centered maintenance and to improve documentation to avoid future problems

For example, as the I&C equipment ages, many of the components, e g capacitors, transistors and the circuit boards begin to deteriorate This increases the failure rate of the equipment and is accompanied by signal drift with time The lower I&C reliability of critical circuits will result in more

frequent plant outages As individual circuits become increasingly scarce, when failures occur, component level rather than circuit level maintenance is required This significantly increases the time it takes to return the control system to service For critical parts in non-redundant systems this can lead to longer outages and therefore lower plant availability The higher failure rates also result in an increase in maintenance effort and cost

The testing and operation activities are affected in a similar manner The testing activities, especially, for the safety systems have increased significantly over the years due to the increasing safety requirement of demonstrating system availability This has increased the work load on operators and the maintenance staff In many cases, the testing circuits for the safety systems were not designed to the same standards as the safety systems This has an adverse effect on safety system performance Demonstration of safety system performance depends much on the routine testing, regular calibration and maintenance call-ups

The regulators have recently raised the issue of utilizing probabilistic safety assessment (PSA) models to support plant operation, maintenance and testing This will put additional burden on the plant management with respect to demonstrating that the plant remains within the safe operating envelope as defined by the risk models The models will need to be validated and updated continuously

3.2.4. Equipment obsolescence and spare parts problem

Equipment obsolescence and unavailability of spare parts have become major problems The rapid change in I&C technology has the result that many of the devices installed in existing nuclear plants are no longer being manufactured The product life cycles for I&C equipment has been steadily decreasing over the past 40 years In the 1950s, pneumatic and relay logic equipment with a manufacturing life cycle of 20 or 30 years was prevalent Today, digital or computer based products have manufacturing life cycles of typically 5 years The service life cycle can be extended by parts support from the manufacturer and by stocking of spare parts including discrete components making up the part, when the manufacturer ceases to provide parts support

Unfortunately, carrying large stock of obsolete parts has major disadvantages which do not make it suited as an effective solution to obsolescence, because (i) investment in additional spare parts stock is expensive, (ii) consumption cannot be accurately predicted and the stock can be exhausted, (iii) changes to performance or regulatory requirements may force earlier change-out, (iv) spare parts such as semi conductors are aging (increasing the failure rates) even if not in use, and this has been observed by several vendors

The skill and facilities required for component level maintenance, i e , identifying and replacing a failed transistor, are quite different than those required for parts level maintenance, i e , identifying and replacing a failed circuit board Most plants adopt parts level maintenance strategy when the manufacturer provides parts support When that support disappears, the plant staff do not have the skills to immediately move to a component level maintenance strategy The lack of documentation, particularly for older equipment, that is required to successfully carry out component level maintenance can also be a serious problem This can significantly increase the difficulty in maintaining the equipment

Finally, for some older technologies, such as mechanical & pneumatic controls, when the required components are no longer available from the manufacturer, it is possible to self-manufacture the component However, for some modern technologies, such as solid state digital electronics, it is very difficult and usually impractical to manufacture parts Even replacing the part (or assembly) with a functionally equivalent commercially available part can be a problem Often the modern parts can be functionally equivalent but are not electrically or environmentally compatible with that part's required role in the old system The difficulty and cost of satisfying the old part's performance requirements with a new part can be formidable

3.2.5. Human performance and human-machine interface

Many plants have reported that a high percentage (e g , 60%) of all major failures in the plants are caused by human errors Therefore, there has been much focus on elimination of human errors, enhancement of human performance and general improvement of human machine interface Both the utility management and the regulators are demanding improvement in this area

Reviews of operating experience and interviews with plant staff have brought much insight into the subject of human performance in NPPs Significant events are routinely investigated through the methods of root cause analysis and human performance evaluation Deficiencies in the operation, testing and maintenance support systems including tools, procedures, training and documentation, are found to be major contributors to poor human performance and human errors

The display and annunciation systems have received much attention over the years from both the NPP staff and the regulators In a number of cases the plant displays, the alarms, and the annunciation have been found to be either inadequate or ineffective to handle many of the unusual situations Alarm avalanche is a well known problem

There have also been noticeable problems in the area of communication between various groups in the plants and even with the outside groups during plant normal and emergency situations

3.2.6. Aging, life extension and environmental qualification

Nuclear plant life assurance program looks at the different aspects of plant life, including designed life, estimated residual life and life extension beyond the design basis It is a long term management issue and is high on the agenda for discussion between the licensee and the regulators Within this context the adequacy of predictive maintenance, degree of inspection and testing, and the effectiveness of system surveillance program are raising serious questions

The safety analysis and the risk assessments have raised serious concerns about the capability of existing equipment for design basis accidents, viz , main steam line break and loss of coolant In many existing plants, the equipment is not environmentally qualified and replacement or upgrading of equipment to meet the current environmental requirements (EQ) has become a major effort It has led to expensive retrofit programs

Other important environmental issues include seismic qualification, chemistry control, electromagnetic immunity, and radiation damage of materials Seismic qualification of existing facilities and installation of seismic instrumentation are ongoing The chemistry control in some plants has been poor and this has caused serious problems with the boilers and heat exchangers Chemistry sampling, monitoring and control has been enhanced However, many old chemistry measuring devices still need to be replaced with better and more effective equipment

Many electronic devices in the plants are vulnerable to electromagnetic and radio frequency interference (EMI/RFI) as well as signal noise Measures to improve immunity are being introduced There is a concern that digital devices may also be vulnerable, particularly low voltage devices Radiation damage of elastomeric material, e g , cables is a concern Low signal cables are especially vulnerable to radiation induced aging

There are two aspects of aging management that impact on I&C The first is minimizing the I&C replacement cost due to the deterioration of I&C equipment with time The second is the opportunities for I&C equipment and systems to help manage the deterioration of process equipment There are considerable amounts of money associated with premature expiration of life of process equipment and major I&C equipment (e g cables, control systems, computer systems, reactor flux detectors, etc)

3.2.7. Use of advanced instrumentation and control technology

An increasing number of plants are using advanced I&C technology for both upgrades and new systems Digital technology has created a number of opportunities including improved functionality, reliability, availability and flexibility to meet new requirements There is also the possibility of improved plant information with lower capital and operating costs and reduced time to implement changes

Digital technology has also introduced a number of commercial and technical risks that must be managed to ensure that the benefits will be realized The risks with digital technology include licensing difficulties and the possibility of introducing unintended functions, unexpected failure modes, and losing expected functions Digital technology typically requires more formal equipment qualification, better configuration control and more computer knowledgeable technical support staff to maintain or modify the software and the hardware

For safety system applications, software quality assurance and demonstration of computer based system reliability have become a major licensing issue The licensing acceptance of these products are very restrictive even though many of the products have been successfully used in other industries The introduction of these systems has been slow and only recently has gained some support from the regulators The cost of introducing these new digital systems in the NPP has also been much higher than in the other industries

3.2.8. Economic issues

Nuclear plant operators are under much pressure to reduce cost so that NPP can compete in the market place with other energy providers This has created a focus on achieving cost reduction in all areas of power plant operation, i e , reducing operating, maintenance and administrative costs, minimizing capital cost, and decommissioning cost The life cycle cost of NPP operation are central to continued plant viability The operators of NPP are looking at all options for achieving cost reduction and capacity factor hence income improvement Additional measures include minimization of failure cost, and reduction of financial risk including those associated with licensing problems and unexpected accidents or serious process failures

A cost-effective I&C upgrade can be important incentive for the NPP Getting it right can create enormous economic benefit not only in the I&C area but more importantly in the process equipment area It is common for advanced technology to improve control performance, increase reliability, reduce operating and maintenance costs and provide benefits in other areas such as system surveillance The improved performance usually is accompanied by improved reliability of the corresponding process systems due to reduced wear and tear of equipment, in turn resulting in improved overall plant capacity factors

However, an I&C upgrade not done right can create new unexpected failure modes that can result in significant plant outages and equipment damage It is not uncommon for poorly executed advanced control projects to result in significant plant restart delays and in a few notable cases, serious equipment damage has occurred

3.2.9. Outage management

Outage management has become a major issue over the last several years with improvements being made in areas such as labor loading, tooling, planning and execution Further outage management improvements are being studied to achieve higher capacity factors in the existing NPP The issues that need to be resolved with the primary goal of achieving higher capacity factor are (i) Mechanisms for expanding work force to handle peak resource requirements (e g , additional maintenance, engineering and other support staff), (ii) Outage scope need to be better defined and controlled such that freeze dates for work packages are maintained and formal review of what is and what is not outage work is

established, (iii) Special outage support service groups such as radiation escort and entry coordination, dedicated crews, prior resolution of jurisdictional disputes between trades and avoidance of duplication of support service be addressed, (iv) Special shift schedule arrangements to allow work on critical items to proceed, (v) Methods for obtaining timely startup approvals and documentation reviews, (vi) Establishment of teams for outages where specialist planning and execution are required in work such as refueling outages, vacuum building outages and turbine outages Another important aspect of outage management that requires discussion is outage timing, because there is a financial benefit to move outage days into periods of low unit cost of electricity available from the distribution grid

3.2.10. Acceptance of changes

There are many groups involved in NPP operation including the plant management, the operators, the and maintenance staff, engineering and service groups, the regulators and the general public which also have an interest in the plant It is important that all accept the changes that are being made in existing plants or being proposed for future plants The degree of acceptance varies among the groups and in most cases needs significant effort by the NPP owners to just get a simple change accepted by all

Major system changes generally include both functional changes and technology changes This creates significant changes in the manner in which all users interact with the system One of the most dramatic changes is the transition from individual instrument interfaces to CRT based interactive displays The change creates many opportunities to make mistakes if staff with limited experience and training are involved in the change

Typically the best people to make and use the changes are those that have detailed knowledge of the plant and the new technology Unfortunately, because of the way the nuclear and the I&C industries are structured and operated, the plant staff generally are not very familiar with the latest technology Effective implementation of new technology in nuclear plants must therefore be done by integrated teams of both supplier and utility staff Managing the size of these teams and the responsibilities among the team members can have dramatic effects on the success of the projects, especially on acceptance

Even with the most experienced staff in an optimum team structure, the resulting system creates a very different environment for the eventual users Operation, maintenance and technical support staff all need to be retrained to effectively work with the new systems Failure to deal with these effectively including options for older employees who are unable to make the transition, can result into serious labor-management conflicts

3.2.11. Quality management issues

NPP design, construction and operation must meet high level of quality assurance as specified in plant licensing Quality management issues receive serious attention by the regulators and the owners Peer evaluation results of the plant performance have shown that many of the plant issues and concerns are common to many plants Some of these issues are configuration management, verification and validation, knowledge of the staff, training and skill development, work management system, and information management

Effective configuration management in all phases of plant work, especially the control of change, is a major issue in the context of plant operation The introduction of advanced technology generally has repercussions well beyond the individual group responsible for introducing the change as a control system change can affect several other station and service support groups A typical example is a change of the control room display from an indicator to a CRT This change will affect virtually every production related group in the plant and service support groups such as the operator training simulator center If not properly thought out, the consequences of a major change in technology can easily grow beyond expectations The unexpected additional costs can sometimes overwhelm the expected benefits,

unfortunately once a change has been implemented it becomes almost impossible to retract This places significant additional burden on the new technology advocates

Adequate verification and validation of changes is a concern, because of the ongoing problem with changes made in the plant and its potential impact Furthermore, verification and validation of engineering analysis tools and computer programs for engineering calculations and nuclear safety analysis have raised concerns The quality assurance of safety analysis codes has also become a licensing issue

Staff qualification, retraining and skill development is an ongoing issue in the quality management of NPP It is even more crucial if a new digital technology is introduced, because the benefit of the new technology can only be fully utilized if the operating and maintenance staff get the necessary skill

Finally, the plant work management and information management systems must meet current standard in terms of storing and retrieving all technical and operational information needed for the safe and economical operation of the plant Proper selection and successful implementation of commercial database systems for this job is an issue

3.2.12. Emergency preparedness and accident management

Emergency preparedness, accident management and ability to maintain effective communication within and outside the plants during emergencies are important issues Existing nuclear plants must have adequate systems, procedures, and training in place for emergency preparedness and ensure effective accident management The regulators have also raised concerns regarding post accident venting and post accident radiation monitoring This has resulted in the upgrading of existing post accident venting and monitoring devices, provisions for safety parameter display, operation from emergency control room, and availability of mobile radioactive analysis facility

3 3 PLANT NEEDS AND REQUIREMENTS

The various issues and concerns of NPPs have been described in the previous sections Based on these, the overall plant requirements are stated in the following sections These requirements should be clear and understood by the owners, designers and vendors Any advanced I&C system being installed or proposed should meet both the short term and the long term needs of the plant

3.3.1. Plant modification

Most of the existing plants that started operation between 1970's and 1980's are going through various levels of modification Modification can be defined as parts substitution, equipment change, upgrade or enhancement of existing system, retrofit of new system and lay-up or mothball of plants or systems Management of these modification from the generation of proper specifications or requirements through to installation and project close out are important

Parts substitution and equipment replacement are performed in response to equipment failure or obsolescence In order to complete this, reconstitution of the technical specification is usually required Upgrade and enhancement of existing systems are also performed in response to aging related failures and the wish to achieve system performance and efficiency improvement and safety enhancement

The retrofits of new systems are needed due to safeguard or security improvement and also due to safety improvement done through safety parameter monitoring, post accident monitoring, emission monitoring, environmental qualification, seismic qualification and waste management Most retrofits are in response to regulatory requirements for radiological and environmental emission

The lay-up or mothball of a unit involves its safe shutdown and placing its systems and equipment in a non-operational state, while ensuring that the requirements of nuclear safety, employee safety and the regulatory compliance are met

3.3.2. Safety and licensing needs

NPP needs considerable support to resolve increasing safety and licensing issues covering subjects such as (i) establishment of safe operating envelope, (ii) specification of nuclear safety requirements, (iii) means for compliance with licensing requirements, (iv) measurement of safety performance indicators, (v) use of risk assessment for design, operation and maintenance, (vi) management of environmental emission, (vii) use of codes and standards Many existing plants are faced with new requirements due to situations which were not covered in earlier safety analysis

The activities associated with regulatory compliance and monitoring of safety performance and reporting back to the regulators and the utility management have become complex, time consuming and costly Therefore, equipment and tools are needed that can help to reduce the labor cost of compliance activities and measurement of safety performance indicators The current monitoring and analysis systems are often manual paper-based recording systems, and automation and integration of the data into an information system can yield considerable labor savings and better demonstration of compliance

Effective use of plant safety assessment models (PSA) is needed It is being promoted by both the utilities and the regulators to obtain assurance that the plant operation, testing and maintenance activities are within the safe operating envelope and that the plant configuration control is maintained The PSA models should be maintained as a living document for day to day use in the plant and should also provide a better mechanism for safety assurance and regulatory compliance

Better management of radiological and chemical emission from the plants during normal and abnormal operating conditions are needed to meet more stringent environmental requirements Many older I&C systems must be upgraded to meet the current standards

Finally, the plant needs an effective means for assuring that it not only meets the codes and standards of its original design, but can meet the challenges of new codes and standards

3.3.3. Plant life cycle management

NPP needs effective life cycle management program to cover areas such as (i) Plant life assurance, life extension, equipment replacement and retrofit, (ii) Maintenance programs for preventative maintenance, corrective maintenance and call-ups, (iii) Inspection and testing programs for periodic inspection, inservice inspection and routine testing

Foremost is the need to develop more experience with equipment aging processes and their impact on overall plant performance The management of equipment aging issues can make a significant impact on the growing maintenance budgets and plant capacity factors Maintenance analysis and decision making tools such as reliability centered maintenance (RCM) and condition based maintenance (CBM) need to be developed The maintenance tools must be supported by information about the process equipment The type of information is not only the traditional variables such as pressures, temperatures, flows, etc but also more exotic diagnostic and conditions based measurements I&C systems are being called upon to supply this information either periodically (such as thermal imaging and lubricating oil analysis) or continuously such as stress analysis and life consumption monitoring and heat exchangers thermal efficiency monitoring

Finally, there is a need for effective monitoring and diagnosis systems , viz , vibration monitoring, signal noise monitoring, fatigue and stress monitoring, corrosion monitoring, transient monitoring for the plant process systems, and radiation monitoring

3.3.4. System surveillance

System surveillance is a key requirement in the plant Sufficient experience has been accumulated over the past 40 years of nuclear plant operation that most nuclear technical staff are now convinced of the benefits of equipment and systems surveillance Surveillance systems can help to reduce plant unavailability by early problem detection before serious damage is caused

The system surveillance program should have a data collection system consisting of test reports, maintenance and call-up data, and operation data It should also have a methodology consisting of equipment trend analysis, root cause analysis of failures or significant events, and results of performance evaluation The data collected should be compared with the safety and operating limits of the plants to ensure that the systems are operating within the safe operating envelope The operating limits are specified in the plant policies and procedures and must take into account operator action time under both normal and abnormal conditions

For example, system surveillance of a safety I&C system will require monitoring of instrument drift and tolerances Typically it will include calibration data collection, measurement of drift, drift statistical analysis, evaluation of equipment tolerances and margins, instrument error analysis, and calculation of instrument loop response time The drift data must be compared with the safety limits as specified in the safety analysis reports with information such as analysis limits, analysis uncertainty, impairment limits and instrument tolerances

3.3.5. Plant operation support

The nuclear plants must have adequate operator support systems based on the principles of human machine interface needs It should consist of operating procedures (paper based or automated), effective alarm message, clear and unambiguous plant displays, and appropriate training Documenting and processing event reports and equipment deficiencies is a time consuming task which relies heavily on manual handling and processing of paper-based forms Automation of many of the steps within an information processing system can result in significant savings This is particularly important for older plants which were not built with formal human factor program

The older plants need operator support retrofits including sufficient process measurements available for the operator to monitor the plant Also, during upsets and accidents the subsequent course of events is very dependent on the operator's ability to identify and correctly respond to the specific failure The amount of damage to process equipment depends heavily on the operator's ability to carry out those functions reliably

Better operator information and decision support systems are needed because of the complexity and inter-related nature of nuclear plant systems The decision support systems should collect both periodic (off-line) and continuous (on-line) information Systems that can present that information in a consolidated and inter-related way can make it much easier for technical staff to select the correct action Many nuclear plants have suffered significant losses that could have been avoided by these systems There is a growing interest in systems that can continuously diagnose and identify the location of non-routine behavior There is also interest in systems that can more reliably bring the operators attention to the correct response procedures These new systems must be developed with requirements from all users, especially the operators

Some utilities are also sponsoring research in expert systems and artificial intelligence that may some day provide operators advice on how to best respond to low probability serious events in the plant such as multiple failures during the course of an upset or accident

3.3.6. Maintenance and testing support

Maintenance support should include better diagnostics systems, maintenance and calibration tools, maintenance documentation, and provisions of training in new technology Reliability centered maintenance (RCM) program is essential and is growing in application Furthermore, risk-based maintenance and testing using the plant probabilistic safety assessment (PSA) models is also being proposed by some utilities, see Section 8 10

The majority of a maintainers time is spent on activities not directly related to fixing the problem, so called wrench time Typical wrench time is in the range of 10 to 20% of total shift time and it is associated with preparing and planning for the work There are needs for better information and planning tools that will eliminate much of this time These maintenance support tools can make significant contributions to lower maintenance costs by helping maintainers select the appropriate procedures, parts and work tools to execute the task They can also help by assisting the maintainer in completing their work reports

Improved plant status information systems can be used to manage the isolation of equipment for worker safety and to ensure that plant technical specifications are not compromised during repair of equipment

Testing support is also needed for better means of testing and recording of test results To this effect new testing tools, better methods and techniques for testing, testing documentation, automated testing system, and digital methods of testing for analog systems are needed

3.3.7. Engineering support

The engineering and material management support in the plant is very important for successful operation of the plant The operations staff depend much on the expertise and timely support provided by the engineering and the material management staff The engineering should provide engineering analysis, design and technical support, design requirement, technical specification, and design configuration management Furthermore, material specification, design documentation and operating documentation should be provided by the engineering staff

Plant engineering support is crucial with respect to plant changes which must be reviewed and approved by the engineering staff The cost of poorly executed changes to the plant's system and equipment can be significant Also, unexpected new failure modes can be introduced if the inter-relationship of the systems is not fully considered during implementation of the change

Various engineering tools including analysis algorithm and simulation are needed to provide engineering support for an operating plants Demand for easy to use engineering analysis and event simulation tools continues to grow Tools that will allow station real time data to be imported and analyzed to help in the model development are even more desirable Validation of computer models should be considered, although it can take as much time as the development itself and must be done with plant data

3.3.8. Configuration management

The plants must have effective configuration management with respect to all aspects of plant design, operation and maintenance This should include document management and maintenance of design configuration, operation configuration and maintenance configuration Changes must be implemented through rigorous change control procedure Design basis reconstruction has become an important licensing requirement

It is also required that risk-based configuration control is maintained to ensure that the plant remains within the safe operating envelope The plant risk models should be used as a supporting tool to verify that safe plant configurations are maintained under various operating and shutdown conditions

Therefore, the plants need modern configuration management tools and databases to have an effective configuration management The change control system must move from a manual system to a relational database management system Changes made in one document should be reflected on all other station documents electronically There are some commercial electronic document management systems available in the market place

3.3.9. Work management system

The plant must have an effective work management system to keep track of all work being carried out in the plant This will include the operations reports, the changes being made, the test reports, the deficiency reports, the significant event reports, equipment failure records, maintenance work report, maintenance call ups, calibration records etc This should be integrated with the plant document management system for configuration management

The work management system should be based on modern and proven information management systems that are now commercially available At present many work management processes are manual paper-based systems The few that have been computerized are individual projects with the main goal of producing work reports for plant management and regulators Enabling the plant staff to analyze the data conveniently can lead to improved work methods and lower frequency of non-compliance

The I&C technologies and information processing technologies should be coordinated so that the integrated plant information and management information systems can produce more effective decisions I&C systems already use many of the features needed in computer information technologies such as multitasking, large real-time transactional data bases, CRT graphic displays, etc Also, many off-line diagnostic tools are now being computerized This provides the opportunity to incorporate the equipment diagnostic data into the overall plant information systems to help improve maintenance decisions

4. CURRENT ADVANCED I&C SYSTEMS

4 1 INTRODUCTION

Instrumentation and control systems used in nuclear power plant have developed through a process of steady evolution during the last forty years The emphasis in the 1950's through to the 1980's was on having simple control and clear protection strategies, using conventional analog systems with proven sensors and instrumentation A conservative approach was taken to introducing improved sensing and processing principles In recent years the industry has introduced smart and digital sensor, digital electronics and communication systems, these have however been largely confined to conventional plant systems

Significant changes have occurred during the same period in the I&C equipment used in non nuclear industrial sectors where the benefits of digital and computer based systems have been acknowledged One consequence of the conservative approach adopted in the nuclear sector is that the nuclear I&C systems lag significantly behind those found in the non-nuclear industries This growth of this gap has been exacerbated by the lack, in a lot of industrial countries, of a significant nuclear construction program which has removed the financial incentive for I&C manufacturers to develop technically and environmentally qualified products specifically for nuclear power plants (NPPs)

Equipment that is, or is capable of being, qualified to meet nuclear standards is becoming common However, the current practice of using qualified analog technology and then moving to digital processing in a controlled environment will continue to be the norm for some time Major changes are however expected as original plant equipment that are approaching 20 years old become obsolete Rising maintenance costs make replacement attractive, despite its associated capital expenditure

Digital and computer based equipment has been successfully introduced in nuclear plants but its use in safety systems has resulted in some very onerous assessment by regulators The major issues of software reliability, software verification, system validation, digital product qualification and safety function classification have been considered and resolved in an acceptable way from the licensing point of view in countries using computerization for their systems important to safety But much work remains to be done in this area The success of this work is one of the keys to widespread deployment of modern I&C equipment on nuclear plant

4 2 INSTRUMENTATION

There is a great range of instrumentation on a nuclear plant, from specialized detectors and electronics to conventional systems for the control and protection of major components such as pumps, burners and turbo generators The current position is indicated below for a number of specialist topics

4.2.1. Nuclear instrumentation

There is a requirement to monitor the neutron flux over the full range of reactor power, about 14 decades This is currently achieved using three sets of equipment each covering about a third of the range with approximately one decade of overlap, the ranges are identified as start-up, intermediate power level and full power respectively It is customary to use different detectors and electronics for each range

There have been very few developments in detector technology, the methods of deriving the neutron flux from the measured signal, the detector physics and the analysis techniques are well proven However, some materials used in the detectors have changed e g from cobalt to platinum, to exploit new manufacturing techniques, reduce dose burden and give higher reliability

Typical instruments include Ion-chambers, Fission chambers, Helium detectors with their associated pulse counting, linear and logarithmic electronics An IEC standard (IEC 1468), for example, is actually in progress on self-powered neutron detectors in nuclear reactors

Experience has shown that neutron power instrumentation is very sensitive at low power and has caused reactor trips at several US plants, Zion, Harris, Robinson and CANDU plants, after long outages The origin of the problems include, calibration difficulties and signal noise pick-up Some older analog trip meters are very susceptible to electro-magnetic interference (EMI) and radio-frequency interference (RFI) from portable transceivers and cellular phones resulting in reactor trips

Recent developments have concentrated on improving accuracy and interference immunity reducing the maintenance burden and spares holdings This has, in the UK for example, resulted in the introduction of wide range flux measuring systems using a single detector with different electronics to cover the whole power range Typically a combination of pulse counting going over to DC signal Cambelling electronics are used with gamma compensated chamber to ensure measurement accuracy Analog and digital implementations have been developed the latter are gaining favor as the use of software allows a single design to be more flexible and potentially have a lower recalibration and retest burden The IEC 1501 project, actually in progress will deal with wide range mean square voltage neutron fluence rate meter for nuclear reactor control

SINUPERM N a digital neutron flux system from Germany was installed in Borselle NPP Netherlands and uses extended filter algorithms to overcome problems caused by low leakage refueling strategies Analog and digital variants of wide range flux system have been introduced on the UK gas (AGR) and water cooled (PWR) reactors respectively Digital flux equipment has been introduced on a number of BWRs including those in Sweden

4.2.2. Process instrumentation

Process instrumentation covers a wide spectrum of activities required to monitor and control both the reactor and the balance of plant The instrumentation covers the route from sensor through to initiation and display of events and varies according to the requirements of the plant

The process sensors include

- transmitters/switches - pressure, flow, level, temperature, load,
- temperature detectors - resistor temperature detectors (RTD), thermocouples,
- flow elements - annulars, nozzles, orifices,
- humidity detectors,
- gas detectors,
- moisture and leak detectors,
- fire and smoke detectors, infra red detectors,
- conductivity cells,
- motion sensors and load cells

The process monitors include

- samplers, analyzers, gas chromatography, oil-in-water or water-in-oil detection,
- vibration and signal noise monitors,
- seismic instrumentation,
- data loggers,
- video cameras

The other process instruments, essentially for indication and display include

- indicators, meters, gauges - pressure, level, temperature, flow-, flow integrators,
- switches-pressure, level, temperature, hand, limit-, push buttons,
- chart recorders,
- displays, CRT monitors, color Visual Display Units (VDUs),
- power supplies

4.2.3. Controllers and actuators

There is a considerable range of control and actuation technology in use on a plant This includes analog devices based on mechanical, pneumatic, electrical and electronic technologies These analog technologies are proving increasingly costly to maintain and replace Consequently there has been a move away from conventional pneumatic and electrical, e g relay based, control to solid state and programmable electronic devices This trend has not been so prevalent for actuator technology where physical limitations e g component size, and environmental constraints have reduced the penetration of modern technology

The introduction of electronic controllers particularly PLCs has, in many cases, been followed by the introduction of smart sensors and data concentrators, e g multiplexors These can ease the testing burden and often lead to significantly reduced cable requirements, although this is, in many cases, in direct conflict with diversity and independence requirements in safety systems

Finally, there has been a significant change in control strategy with a move from single term to multi term and adaptive control strategies Fuzzy logic control has also been introduced for example for feed water control during start up of the Fugen reactor in Japan

4 3 SAFETY SYSTEMS

The discussion of safety is considered in three parts philosophy, safety systems and safety support systems

4.3.1. Safety philosophy

Safety philosophy and safety practices are well established within the nuclear field and are captured at the highest level in IAEA safety documents (codes and guides) These documents are supported by international, national and company standards that give detailed requirements The key criteria include the principle of defense in depth, measures to ensure that systems defend against both single and common mode failures and requirements derived from good engineering practice The interpretation of the criteria is, because of nuclear licensing convention, carried out on a national basis, further the means of demonstrating compliance can be individual to a piece of equipment or a particular plant The national practices, the analysis techniques, e g failure modes and effect analysis, and the means of justification are very similar

While there are no major challenges to current philosophy, significant issues arise from the need to interpret the philosophy for new and novel technologies In particular there is a need to develop the equivalent means of system analysis and safety demonstration as the practices for conventional technology For example an analog system of discrete components is amenable to single failure analysis whereas a modern system based on integrated circuits is not, consequently requires a new form of analysis

4.3.2. Protection systems

The plant protection systems are those of the highest safety grade providing the essential safety functions for the plant These functions might include measures to ensure the chain reaction can be terminated under all circumstances, core cooling is maintained, and radiation isolation is guaranteed for all design basis accidents

The safety significance of the protection functions has resulted in the application of computer based solutions being very controversial Despite this there are a considerable number of examples of computer based and other digital systems used for protection and control of nuclear power plants The number of years of experience with these systems around the world is increasing, for example in Canada, France, UK and the USA

There are a number of well documented examples of the application of computer based systems, these include

- CANDU digital systems as deployed at Darlington and Wolsung with variations and being developed for other reactors,
- EAGLE 21 system as installed in reactors in the UK, and USA and are currently being deployed in Ignalina and Temelin,
- ISAT and PCL systems as used on UK gas reactors and variations being developed for other plants,
- SPIN systems as used in the French 1300 MWe and 1400 MWe reactors

Other examples include

- PWR ISAT system in the UK,
- German TELEPERM XS system for reactor protection and control,
- A range of BWR protection functions in Finland, Sweden and USA,
- Microprocessor and solid state protection being developed for the RBMK and WWER reactors

A number of these systems have already been deployed and operated in passive mode on target plants

In addition to these major systems, there are many examples where computer technology has been used to form part of the protection system Aside from those above these are essentially experimental and including wide range digital flux instrumentation, trip logic and sequence control Many of these systems use common technology e g multiplexing and data concentration plus fiber optic communications to ensure signal isolation between channels and to reduce the potential for electro-magnetic interference

4.3.3. Safety support systems

There are a large number of safety support systems in use in nuclear plant, these include service systems e g water and power supplies Many of these systems require the use of simple logic that was mostly implemented using relays The overhead imposed by these systems and the increasing complexity of tasks that they are expected to perform places further strains on the safety demonstration techniques available This is particularly significant as support systems are often used for data reduction e g alarm handling, consequently are vulnerable to error propagation

Despite these difficulties the successful application of digital technology to nuclear power plant to enhance their operational efficiency and safety remains one of the key developments necessary to ensure the long term viability of nuclear power in many countries

4 4 CONTROL SYSTEMS

Control will be discussed in terms of philosophy and the control of nuclear and conventional equipment

4.4.1. Control philosophy

Nuclear power plants have traditionally used the closed loop Proportional and Integral (PI) control concept for continuous processes, combinatorial logic for drive control and sequential logic for batch processes Reliability is usually achieved by use of redundancy combined with use of failure revealing design and proof testing of items that are not in continuous operation Whilst base load operation was the norm for nuclear power plant, the changing power supply regime and overcapacity, notably in the western world, has led to the adoption of load following regimes These must inevitably make provision to compensate for Xenon poisoning and related effects

Digital control equipment is preferably located away from the severe plant environment and has been successfully used to implement complex control strategies for reactor control systems since the early 1970's These systems are usually implemented in the form of a fault tolerant architecture to allow continued plant operation in the event of failures

In the 1960's and 1970's the typical approach to the deployment of computer control was to use central dual redundant computer control systems for plant but not usually reactor control During the 1980's programmable controllers, PLCs, were more widely used and for simple functions remain the obvious choice of technology, although for complex functions and integrated system control the use of distributed control systems with networking capability is becoming the preferred choice Digital control systems have been used extensively in the UK, often as original equipment, to automate the operation of the AGRs The Canadian CANDU reactors also make widespread use of digital control including for reactor power Digital computer systems have also been installed in Bruce A plant to replace analog control of the standby generators and the turbine governors Similar changes have or are being considered in Germany and the USA In France, the I&C of 1400 MWe NPPs is based on an architecture of digital control systems

The switch to digital systems can be onerous, as the approaches to design, licensing, operation, maintenance and technical support of digital equipment can be quite different from that for analog and relay technology Special care must be taken, for example during upgrades, to ensure that existing functions, sensors and interface devices are replicated in the new system and where changes are necessary all staff need to be made aware of the changes There are a number of well established problems, for example digital systems have particular difficulty interfacing with spring loaded hand switches to position servo motors and torque or position switches that signals the end of travel for a motorized valve

4.4.2. Nuclear system control

The nuclear process control systems include those for the core power/flux and the heat transport system parameters of pressure, flow, temperature and inventory Dependent on reactor type, there will also be control systems for the boiler parameters of pressure, level and flow, the moderator parameters of temperature and level, and other auxiliary nuclear processes Although most of these controls are based on analog control, digital control systems have been used successfully in many countries Digital reactor control systems were installed as original equipment in both CANDU and AGR reactors

Programmable controllers have been used in German PWR's since 1983 to improve performance and permit automatic

- load following and power maneuvering,
- optimize core power distribution,
- minimize boron and demineralized water consumption following Xenon transients,
- burn up control via an integrated Xenon simulation

At Ontario Hydro's Bruce B station steam generator level control system was converted from analog to a direct digital computer controller and contained a number of fault tolerant features allowing the plant to continue operating even under certain fault conditions e g a faulty signal level

There are a number of proposals for replacement of existing analog systems by stand alone PLCs on older UK reactors, to follow those plants where the systems were installed as original equipment

A fault tolerant digital system for PWR Steam Generator Feedwater Control was installed in US at the Prairie Island plant in 1989 The experience gained from this digital system was a milestone for the US utilities who are moving to specify, install and test similar digital systems for plant retrofits [4 1]

4.4.3. Conventional control

The control of the non-nuclear portion of the plant including the turbo generator, the feed, condenser cooling and service water plus other auxiliary systems were some of the earliest to use digital technology Much of the equipment was adopted directly from and contains the same features as the equivalent systems used on fossil power plant The performance and optimization of these systems is an important issue in terms of plant economics, both performance and availability Digital control are also consistent with current strategies for plant monitoring and system surveillance playing a significant role in proactive system changes to improve for example maintenance

Some of the early control systems are now obsolete and are being replaced by plug-in compatible replacements that match the function of the present controllers However, the operator interface is usually different e g CRT displays are now quite common, so care has to be taken to not complicate the operator interface and controller functionality and so introduce new failure modes The flexibility provided by these systems is also being used to uprate station electrical generation without changing the reactor thermal performance

4 5 PROCESS MONITORING AND DIAGNOSTIC SYSTEMS

The nuclear power industry has a quite long tradition for on-line monitoring of mechanical components because of the restricted accessibility to vital mechanical components and the safety issues involved should these components fail Therefore considerable efforts were put in developing diagnostic systems which are able to detect arising mechanical problems at an early stage In general the diagnosis methods are aiming at

- providing a warning,
- enabling a localization of the deficiency,
- providing assistance for decisions on further plant operation,
- helping to prepare measures for the regular inspection to come,
- assisting to prepare for repair work to be performed

There are a significant number of mature diagnostic systems available to provide on-line information and monitoring of

- loose parts (see 4 5 1),
- vibration (see 4 5 2),
- leakage (see 4 5 3),
- dynamic fatigue (see 4 5 4)

Other examples of diagnostic systems are given in 4 5 5

Computers and display systems are increasingly being exploited to provide higher level information on process behavior, such as

- early indication of the deviation of the process from normal conditions,
- rapid identification of the root cause of any disturbance,
- prediction of the evolution of a disturbance,
- operator aid through computerized help e g on-line manuals,
- scenario prediction for development of countermeasures

These systems are primarily introduced in control rooms adjacent to the main control room The systems deployed usually deal with some of the items described above depending on particular plant concerns, the availability of appropriate sensors and include success path monitoring, disturbance analysis, critical function monitoring and computerized operational handbooks Many of the systems are classified as process diagnostic systems related to plant operability although they do have an impact on safety at term The integration of these systems into the main control room and the assessment of their impact on operator performance and control room practice remains a significant challenge

4.5.1. Loose Parts Monitoring (LPM)

Accelerometers tuned to detect the audible structure born sound generated by a loose or loosened mechanical part provide the input to LPM systems The system then identifies operational noise e g as generated by control rod movement, and uses it to distinguish new noise sources, locate them and to estimate the weight of the part The sensors are attached to the surface of the mechanical structures, outside the pressure boundary, and located close to areas where loose parts are expected e g the bottom of reactor vessel or steam generator, control rod guide tubes, valves Optimum coverage is achieved by careful placement of the sensors Loose parts monitoring systems are widely used in all types of NPP and this has lead to various national standards e g IEC 988 which includes

- loose parts monitoring techniques,
- system requirements,
- initial start-up,
- surveillance program

Vibration monitoring systems have, for many years, aided the early detection of problems, however, operational problems including false alarms and the difficulties of interpretation of events on site have led to acceptance problems The number of false alarms has been significantly reduced by the use of dynamic thresholds and careful investigation of the background noise, although the detailed analysis and interpretation still remain with the specialist This is still under investigation and one approach has been to develop a tool for automated acoustic burst classification using neural networks A short description and first results with operational data is given in Section 8 1

Digital technology does not easily lend itself to the capture of high frequency transient signals however the processing power it provides is important for signal analysis and interpretation In general detailed signal analysis is an off-line activity requiring complicated analysis tools and that can seldom be performed in real time Despite this, such systems are coming as for example the KUS95 system described below

This system consists of a multi channel transient recorder, a super-high-performance PC and a standard software package for data acquisition and analysis When an event occurs, the system records data from all channels, individual events and event sequences with a high event frequency

The software is configured for MS-Windows applications, has user-friendly statistics analysis and graphics functions giving the expert comprehensive information and a range of tools for analysis and assessment of the event Automatic self-checking and calibration of the system is achieved by

- background noise measurement, i e the continuous noise level in the plant,
- checking the instrument chains by input of a defined electrical signal,

- remote-controlled, reproducible test impacts from automatic impact hammers

The KUS 95 system can be networked, allowing signal data to be transferred locally, to an evaluation computer within the plant, or to other locations via a modem link The software package considerably improves the diagnostic capabilities, with the main features being the following

- automatic on-line evaluation,
- event diagnosis on the basis of known events,
- approximate classification on a triggering pattern basis,
- exact classification by comparing noise patterns with that of known events,
- filtering similar sequential events,
- alarm reduction,
- multimedia functions with acoustic output of stored events

EDF are currently developing a loose parts detection system DCE designed to be connected to the PSAD structure (see 4 5 6) The use of digital technology allows advanced signal filtering techniques to be exploited and the calculation of smart signal descriptors, automatic signal classification, reduction of false-alarm rate and aids operator diagnosis

The Canadians have developed signal noise monitoring as a means of detecting the incipient failure of flux detectors

4.5.2. Vibration monitoring for PWRs

Vibration monitoring is a well established part of the surveillance concept for early failure detection and on-line diagnosis of primary circuit components in pressurized water reactors The monitoring of the reactor vessel internals for abnormal vibration behavior is performed in PWR plants all over the world, on a regular basis to comply with regulatory requirements and when triggered by specific events Mature analysis techniques enable the use of ex-core and in-core neutron signals to follow the vibrations of the reactor pressure vessel and its internals and very often additional vibration sensors or accelerometers of loose parts monitoring systems can be used to support these measurements However in some countries e g Germany and Russia, integral vibration monitoring of the overall primary circuit is performed using the actual loop vibrations, thermal-hydraulic effects and the pumps acting on the entire system which mutually influence the vibrational behavior of the mechanical components to be monitored An example of vibration monitoring in a typical 4-loop PWR in Germany is described in detail in Appendix B

In France, PWR reactor internals are monitored by a system called SIS/KIR which is based on neutron noise and vibration analysis [4 13, 4 14] The signatures for all systems are collected by EDF on a national basis and a data base corresponding to about 400 fuel cycles has been created It is possible to use this to diagnose problems based on a very important statistical knowledge of the actual behavior of the reactor internals

A new reactor internals monitoring system, SSI, is under development by EDF The new system is also designed to be connected to the PSAD structure (see 4 5 6), to aid plant operators in diagnosis

The coolant pumps on French reactors are equipped with vibration, speed and displacement sensors installed on bearings, shaft line, coupling, motors and shell bolt [4 15] In addition to the classical monitoring based on threshold oversteps performed by plant operators, periodic advanced analyses are performed every three months by an expert center, for all EDF's coolant pumps A new monitoring system, connected to the PSAD structure, has been developed and its prototype is under evaluation at Tricastin, in France An expert system, called DIAPO, will aid the operators to perform coolant pump diagnostics

4.5.3. Leakage monitoring

Leaks can lead to the release of radiation from the plant as well as loss of coolant Large leaks are defended by the action of the reactor protection system In the case of the PWR's the system reacts to signals arising from pressure increases or activity increases in the containment, level drops in the pressurizer or the reactor pressure vessel However, the leak detection systems are also used for detecting small leaks in pressure-retaining components in support of the leak-before-break concept for the containment, main steam and feedwater, auxiliary systems building, annulus and valve compartments The LDS is intended for the detection of "unidentifiable leaks"

Public debate in Germany on "pipe cracking" in NPP's has brought the subject of early leak detection to wide attention Demands from the licensing authorities have led to the development of an upgraded leak detection system, LDS

Several on-line monitoring systems were developed in France to detect leaks in various types of components, EDF has developed a system, called VAMCIS [4 16], to continuously monitor leaks in PWR steam generators It is based on the detection of Nitrogen 16 which goes from the primary circuit to the secondary side of the steam generator in case of a leaking tube Such a system enables a quick detection of leaks, it evaluates the leak rate and is an efficient way to prevent rupture of steam generator tubes in operation Another system detects leaks in steam separators/reheaters, its operation is based on the use of helium which is injected in the heating steam In case of leakage through one or several tubes, traces of helium can be detected in the reheated steam A calibration procedure is used to enable an assessment of the leak rate The reheaters in-service tests are performed every three months

The SEXTEN system [4 17] performs a continuous monitoring of the containment vessel (reactor building) leak rate It is possible to detect a leak of about 5 m^3/h after 1 day and a leak of about 1 m^3/h after 20 days The system uses temperature, absolute pressure, hygrometry and compressed air flow rate sensors The system is installed in all French PWRs and Ringhals, in Sweden It has been in use since 1984 and has proved effective finding several containment leaks

IEC 1950 gives technical requirements for leak monitoring systems

4.5.4. Fatigue monitoring

Plant life extension programs include a comprehensive review of all factors that affect plant performance and for continued operation the plant has to comply with all current safety requirements and to compete economically with alternative sources of power Degradation of plant performance may lead to increased operating costs and can pose significant environmental and safety concerns There are several aging mechanisms which contribute to limitation of component life including fatigue, corrosion, erosion, thermal aging, wear and, specifically for the nuclear power stations, irradiation In general, degradation of plant performance may be related to aging of individual plant components, as the applicability of the various mechanisms and their relative influence varies according to the component and its location For example, irradiation embrittlement may be an important degradation mechanism for the reactor vessel beltline in PWR's but not for the steam generator Determining the dominant mechanisms for each component and location requires an understanding of the basic mechanisms as well as understanding of the operating conditions The information derived from these systems can contribute to building an integral system for power plant maintenance management

In order to keep track of all the fatigue effects and to estimate the residual life time of the various components, it is necessary to follow carefully all the relevant parameters in a consistent way One system FAMOS (FAtigue MOnitoring System), developed in Germany, calculates the component fatigue based on records of transient thermal stresses evaluated from surface temperatures and process data

In France, SYSFAC [4 18] is a system devoted to transient logging and fatigue monitoring of the reactor coolant boundary The main objectives are to satisfy regulatory requirements for data collection and to detect and analyze the main actions that have an effect on the expected life of the plant The system is fully automatic and it is composed of three modules a functional transient detection module, a mechanical transient detection module which collect the general transient data and a fatigue monitoring module performs a precise surveillance of five specific zones, particularly sensible to thermal fatigue

4.5.5. Other examples of diagnostic systems

EDF has developed a system CLIP [4 9, 4 10] to monitor the efficiency of PWR plants The reactor thermal power and the measured thermal efficiency of the non nuclear portion of the plant are compared with a calculated nominal efficiency for a plant in good condition using plant model that takes into account current values of parameters like temperature of cooling water, flow rates, etc If a discrepancy between the actual and nominal efficiency is detected, the operators investigate to see if there is any plant degradation or faults The system is now used in many EDF plants and it has already contributed to point out steam leaks, faulty steam by-pass and heat-exchanger fouling

A reactor core surveillance system SCORPIO [4 4] was developed by the OECD Halden Reactor Project, Norway, and is in operation at the Ringhals PWR, Sweden, Sizewell B PWR, UK, Catawba and McGuire Units, USA The Halden Project has also developed two other applications leakage detection system surveying the high pressure re-heaters, and signal validation system which explores the feedwater flow sensors for the Loviisa PWR, Finland The system allows operators to easily identify sensors deviating from normal and also provides an overview of the state of the feedwater system and aid maintenance activities

4.5.6. Common architecture for process monitoring and diagnostic systems

The process monitoring and diagnostic systems installed in a plant are generally independent and do not exchange data Some functions of these systems are common and are redeveloped for each new monitoring and diagnostic system

- acquisition of data from the network of the plant,
- data management and storage,
- signal and data processing (statistics, Fast Fourier Transformation (FFT), cross correlation, etc),
- data exchange between different computer workstations, especially on a national level

EDF has developed PSAD [4 19-4 22] an open evolutionary system, which performs all these functions and can act as a host to several different monitoring and diagnostic systems It is based on the following recognized standards

- ORACLE for data management and storage,
- Ethernet TCP/IP for communication protocols,
- X-MOTIF for man-machine interface,
- ADA for computer software

A prototype is currently under evaluation at Tricastin NPP and it incorporates two monitoring systems surveillance of turbogenerator sets and reactor coolant pumps Three other monitoring systems are under development and will be integrated to PSAD detection of loose parts, vibration monitoring of reactor internals and monitoring of turbogenerator inlet valves

4 6 CONTROL ROOM AND INFORMATION DISPLAY

In addition to the automatic trip and post trip sequencing equipment many of the control room information and display systems are important to safety The effectiveness of these systems impacts on

both the immediate response to an upset condition and in the event of a major accident to the management of that accident

4.6.1. Control rooms and instrument rooms

In most plants, the control room systems rely on external safety and control systems housed in instrument rooms These rooms often contain multiple channels of support equipment and, in the case of safety equipment, the required level of separation and channelization is achieved by the use of separate rooms The Human Machine Interface (HMI), control panels and displays are often subject to significant change but being classed as auxiliary systems can be subjected to the least scrutiny

There are several generations of design of control rooms and the impact of new technology is obvious, as VDUs and touch screens replace chart recorders and analog instruments The newer control room designs maintain some of the old features, while incorporating many of the latest human factor features

4.6.2. Plant process computers

The plant process computer system (PPCS) gathers data and in many cases provides the operators with critical operating parameters in normal and emergency situations These systems are increasing in size and now take the form of distributed systems designed to acquire large amounts of data, from field sensors located throughout the plant, on a real time basis, for the purpose of performing calculations and other functions

The application software is categorized into scan, log and alarm, plant monitoring and performance, and HMI functions The scan, log and alarm functions sample the plant instrumentation inputs and log each current value into the database The processes include converting the signal to an appropriate engineering unit, checking the values against various alarm limits to ensure the signal is valid and identify if action is required Data is also selectively archived for subsequent retrieval to support engineering analysis of historical events Many plant monitoring and performance functions can access the database to support other operational monitoring and performance functions The HMI provides the interface to the system for controlling these functions as well as to access information from them [4 2] In many plants these functions are controlled centrally e g CANDU, Sizewell B and French N4 NPPs

4.6.3. Safety parameter display systems

The TMI-2 accident investigation identified serious deficiencies in information presentation and resulted in the development of the safety parameter display system (SPDS) SPDS is designed to indicate deviation of defined safety parameters and provide the subsets of important measurements to assist the operator in reaching the safety goals The system is computer based, uses colour graphics and contains application software modules for signal validation, emergency procedure monitoring, and integrates the rule-based control functions with the SPDS

The use of on-line computer systems for the SPDS in control rooms has two main goals in support of the operators information presentation and information generation VDUs are normally used for information presentation usually in the form of system diagrams with inserted parameter values and plant states, trend curves showing the history of important physical parameters, and listings of plant alarms in groups or according to their priority

These system functions have often been implemented as stand-alone systems or operator aids, driven by the operational needs of a specific plant or by licensing requirements Typical examples are core power mapping systems, process system operating limit diagram (stress), load following advisors and safety parameter display systems These systems are increasingly being integrated into the total station data processing and display system [4 3]

4.6.4. Plant display systems

Plant displays are used to communicate the state of the plant equipment and the activity of the plant to the operator Information displayed includes plant transients, history and diagnostic information e g post accident analysis The information has to be accurate and displayed in a timely fashion in a manner that can be easily assimilated to allow correct and timely response by the operator The HMI are mostly cathode ray tube (CRT) based, driven by the plant process computers and are used for both normal and abnormal operating conditions

The processing in an integrated alarm system may be divided into three stages alarm generation, alarm structuring and alarm presentation

Alarm generation All new alarms generated from process measurements should be generated by this module including conventional alarms, function-oriented alarms (see more information on function-oriented alarms in 8 5 1) and model-based alarms (i e alarm generation by application of on-line process models) The advantage of having different types of alarms available when the operator investigates the status of the plant, is the diversity in the underlying methods, which contributes to a broader view and possibly a more robust system Model-based alarms may be more sensitive than conventional alarms, and useful in dynamic situations as well, while function-oriented alarms are most useful in large transients or accident situations

Alarm structuring In order to avoid operator cognitive overload, for example from alarm cascade in upset conditions, the alarms must be structured into a hierarchy This includes filtering of conventional alarms to reduce the amount of information automatically presented to clarify the disturbance situation A toolbox named COAST has been developed at the Halden Project to facilitate implementation of an integrated alarm system as described, see [4 23]

Alarm display Displays must be set out to reflect the alarms structure mentioned above and so draw the operators attention to those alarms considered to be of highest priority A number of systems have been deployed including CAMLS and PRISCA The CANDU annunciation message list system (CAMLS) has been developed and validated in the training simulators and resolves the annunciation overload problem by providing alarm suppression, prioritization and precise messages for abnormal conditions The PRISCA system in the German KONVOI plant integrates the alarm annunciation and logging, the indication of systems status (operation, warning, faults, etc) and safety parameter display functions by diagrams for safety relevant protection goals

4.6.5. Computerized operating procedures

A number potential and actual problems in the nuclear industry are related to the quality of operating procedures particularly emergency operating procedures A considerable amount of work has been done in recent years to improve their quality This applies to most aspects related to procedure production, procedure structure and contents, procedure implementation and procedure maintenance Many of the identified problems can be directly addressed by developing computerized procedure handling tools, thus, there is a growing interest in taking modern computer technology into use for improving today's practice in procedure preparation, implementation and maintenance

COPMA-II is a computerized procedure system developed at the Halden Project [4 8] The system has two main components the procedure editor (PEDII, which is off-line) and the on-line procedure following system PED-II, is a tool designed to be used by the procedure writer during procedure preparation and procedure maintenance Procedures to be used with COPMA-II must be expressed in a formal, general purpose procedure language, PROLA The COPMA-II on-line procedure following system, is the tool developed for supporting the process operators during retrieval and execution of procedures The system is designed to work with a live data communication link to the process

computer, simulator, or any other external software component It is intended that this system replace the traditional system of paper based procedures

4.6.6. Emergency operation and post accident monitoring

Many plants have a secondary control room for emergency operation in addition to main control room The secondary control rooms are essential for emergency operation and post accident plant monitoring in case of unavailability of the main control room, and are usually seismically and environmentally qualified to ensure availability following an accident

Some plants also have separate radioactive and plant monitoring facility for analysis of post accident samples should the main plant become inhabitable All UK and French plants have or are being equipped with emergency indication centres remote from the plant The Canadian Pickering station has a mobile radioactive analysis facility for post-accident radiation monitoring

4 7 OPERATION, MAINTENANCE, TESTING AND OUTAGE SUPPORT SYSTEMS

4.7.1. Operation support

There have been many attempts to develop advanced operator support systems, the most successful being improved CRT displays and integration of the information required for a given operating function or plant condition Limited success has also been achieved in providing more analytical information for critical parameter displays However, regulatory pressures are increasing the need to adopt formalized approaches to verify and validate operator interface systems before use, some rapid standardization is required if high costs in providing these displays is to be avoided

The use of LAN networks is resulting in work management information systems finding applications in the main control room, a move that is expected to facilitate the introduction of additional advanced functions in time

True expert systems and advisory displays are still in the development phase and one major obstacle to their acceptance remains the means of qualification and the effort needed to gain regulatory approval for their use Some plants are sponsoring several display, process diagnostic and analysis projects to gain further experience with advanced operator support systems

The Canadian industry has developed an advanced process analysis of control system (APACS) [4 3] to assist the operator during abnormal situations A prototype system has been built for the Bruce B feedwater system Recent advances in artificial intelligence, process control and simulation have made possible this new technology for real-time supervisory control APACS essentially consists of a plant analyser, monitoring, diagnosis and HMI It is a system that detects, predicts and identifies faults in a process system

In some plants it is normal practice to develop and test advanced control and display systems in an operator training simulator before they are introduced in the plant's main control room This allows system functions and malfunctions to be tested under stress and ensure to withstand equipment failures e g like those identified in early annunciation suppression schemes that lacked sufficient fault tolerance

4.7.2. Maintenance and outage support

Considerable effort has gone into providing support for maintenance and outage activities particularly for older plants The activities are driven by financial considerations with the objectives of improving record keeping and activity tracking including minimizing and managing spares holdings, particularly or scarce items, exploiting improved calibration and diagnostic tools, managing calibration, maintenance and repair activities to optimize efficiency The records gathered also form the basis for adoption of aggressive policy towards both reliability centered and risk based maintenance

Many plants have several maintenance support systems some with extensive on-line and off-line diagnostic systems built into their control computer systems that form the basis for the systems above Some plants have already adopted procedures for identifying equipment and issuing work permits and the associated procedures including process and equipment isolation status monitoring e g using hand held scanners and machine readable equipment identification tags

New plants and systems are adopting a policy of integrating the systems and providing automated test and calibration systems many of which are computer based The adoption of modern Distributed Control Systems (DCSs) makes it possible to conduct remote problem analysis and fault finding

Support tools are also being introduced for outage management particularly to ensure that the plant is maintained within its safety envelope and to ensure the radiological protection of the personnel Finally, risk-based outage management tools are being used e g in CANDU plants, and a range of software tools are used for major outage activities (SLAR)

4.7.3. Testing support

Safety system testing is conducted as part of the routine demonstration of system functionality and availability This testing, like that done in support of maintenance activities, can benefit from introduction of computerized tools both to automate the test procedure and preparation of the test report

Some safety systems already include automatic testing as part of their normal operation while others have tools for regression testing performance For example, Dungeness B AGR SCTS and the PCL guardline have included provisions for testing within the design and this testing is running as part of their normal operation The testing regimes adopted reveal faults and allow on-line maintenance Similarly in the CANDU computerized safety systems, tests are performed automatically by the computer

The performance of the repetitive proof testing of the redundant safety channels has been automated in German nuclear power plants The system uses an automated processor based arrangement to perform the repetitive tests and log the outcome including setpoints, parameters and test results, during power operation

It is noted that to achieve the optimum performance from these systems the testing strategy and facilities must be included as a requirement in specification and design particularly if the testing burden and channel down time is to be reduced and the interval between periodic testing increased

4.7.4. Post-mortem analysis

This type of analysis may be seen as a special but important subset of disturbance analysis for nuclear power plants Deviations from normal operation have to be analyzed to identify their cause and enable effective counter measures to be introduced An essential part of this analysis is to check the performance of the automated measures, which is done usually on the basis of protocols provided by the plant computer In order to reduce the work load of the shift personnel and to enable fast data checking, computerized analysis has been introduced in many plants An example of this is the NOVA system at Gundremmingen [4 6, 4 7] The system automates the check of recorded control action and plant behavior against the as designed expectation to ensure the automatic systems respond adequately to disturbances A typical example being, after a turbine trip, a complete check if whether or not the trip system has operated correctly can be performed automatically Therefore the down-time of the turbine can be reduced, a certainly important commercial aspect

The first step to develop NOVA was to identify the disturbance sequences and structure them so that the automatic measures exercised during the disturbance can be checked by the computer, using the

binary and analog data available from the plant Measures being connected by task or purpose have been gathered in areas, which are automatically checked to determine if pre-defined threshold values (initiating automatic actions) have been exceeded Lists of the sequential measures for the reactor protection system, the reactor power limitation system and other control systems have been generated They represent an image of the reference sequence of automatic actions initiated by plant disturbances, and have been validated on the basis of on-site experience The results of the automated checking are presented in two protocols

The overview protocol only presents deviations from the references, which considerably reduces the listing, while the sequence protocol provides detailed information on the

- potential initiating signals,
- actual signals,
- control signals and their time of occurrence,
- reference status,
- comparison of actual and reference status, with deviation explanation

4 8 RADIATION MONITORING SYSTEM

Radiation monitoring equipment is used extensively around the plant to provide

- personnel protection,
- plant protection,
- plant surveillance

Systems available for the protection of personnel include individual dosimeters, whole body monitors, to be used when entering or leaving controlled areas, and medical monitoring systems Significant progress has been made with the introduction of personal digital alarming dosimeters which provide an escalating set of alarms and an immediate display of the cumulative dose and current dose rate

Plant protection systems rely on the detection of activity often to indicate equipment or confinement failure The primary applications are for fuel failure and coolant leak detection, location and identification The systems are generally specially developed and usually rely on the increase in the signal in a specific energy band to indicate the presence of an isotope released by the failure Digital systems are having a significant impact in this area due to their flexibility in setting energy bands for counting and being able to use complex detection algorithms rather than simple threshold values

General surveillance instrumentation includes that for monitoring of condenser coolant, liquid and gaseous effluent and monitoring at the site perimeter These systems are widely dispersed within and around the plant Recent developments have relied on digital and computer based technology to improve the control of the counting process i e energy window sizing and discrimination However, the most obvious benefit has been the introduction of digital communications and VDU displays to give immediate access to current and historical information in an easily understandable form

Radiation monitoring systems are designed to protect the NPP staff and the general public This protection is provided by a combination of fixed, personal and job specific monitoring of the radiation dose levels for direct neutron and gamma radiation airborne activity e g due to aerosols, tritium, iodine and noble gas alpha and beta contamination This is achieved by the use of fixed detectors for area monitoring, personal monitors to provide immediate alarm and occupational monitoring, health physics checks prior to starting work in a designated area and long term monitoring of personnel Public protection is provided primarily by effluent, liquid and gaseous, monitoring and site monitoring and a long term program of radiological surveys The coverage is thus comprehensive providing the facility for immediate response e g to an unexpected release, through to long term protection against unexpected build up or concentration of radioactive materials, enabling dose uptake to be minimized

These systems are installed on all NPPs, however the most extensive systems are those on nuclear chemical plant e g Cap la Hague (in France) and Sellafield (in UK)

A personnel systems ADAS developed in Germany is in operation in the Phillipsburg PWR [4 4], [4 5] It monitors the radiation in designated areas of the plant using a combination of fixed sensors and up to ten mobile measuring units Each unit is equipped with eight measuring devices and a data acquisition computer allowing up to eight hours of data to be stored The measurements are transferred via a Local Area Network (LAN) to the health physics facility to provide on-line display of dose levels and alarm both locally and at the central station In addition a hierarchically organized floor plan visualization, including photographs of plant parts and plant rooms ensure an insight into the local measuring situation

The maturity of the measuring techniques and associated practices has allowed the IEC to initiate in 1993 a project IEC 1504, to develop guidance on the design principles and performance criteria for *radiation monitoring equipment and its application across nuclear site for personnel protection*

It is noted that while radiation detectors have received major upgrades the traditional hardware has worked well, although instrument drift and failures were noted Most changes appear to have been made in response to problems for example change in licensing requirements, unavailability of spares, rather than being part of an anticipated upgrade process

4 9 INFORMATION MANAGEMENT SYSTEMS

A large nuclear power plant has a number of management information systems including plant computers and some of the systems mentioned above The introduction of 'secure' networked systems is allowing both more data to be gathered and to be more efficient Workstations are replacing mainframe recording, monitoring and maintenance work management systems

4.9.1. Plant information

Plant data are available from a range of systems including protection, control and monitoring systems that are based on both analog and digital technology This is resulting in a move away from traditional arrangements where information was only available on a selective basis e g in the control room or plant directors office Engineering and performance data are now available to more staff via station computing networks allowing better communication during normal and abnormal operation, including emergency operation following accidents

4.9.2. Engineering, operation and safety information

The trend of engineering, operation and safety information is following that of plant information with comprehensive real-time information being made available to station staff along with the plant databases for operation and maintenance These facilities allow rapid access to all important station information including design data, maintenance data, safety analysis data, material management data, operational data and system surveillance data, and information supporting plant configuration management

4.9.3. Communication networks

The security of communications and measures to ensure the integrity of plant data and information are becoming more critical as greater numbers of staff have access to the information The security of the networking arrangements, including isolation of control and especially protection equipment from interference, is becoming of increasing concern In many cases unidirectional links and buffering are required because a hierarchical system of controlled access is not seen as being sufficient to ensure plant integrity and safety from either inadvertent or deliberate acts Data protection and the ability to alter data items must also be carefully guarded by both physical and administrative means

In addition to access, it is also necessary to ensure that essential communication channels and particularly those associated with control and protection have sufficient bandwidth to preserve their integrity during times of maximum load which is usually under fault conditions

The ability to remotely connect to many networked systems must also be seen as a potential threat e g due to the possibility of stealing data or potential for introduction of computer viruses

4 10 ENGINEERING SUPPORT

Much of the emerging engineering support has been described in association with the use of computer based systems for controlling and recording essential operation and maintenance activities and for recording essential plant configuration data A number of additional systems are pointed out below, these are plant simulators and engineering support and analysis tools

4.10.1. Simulator applications

Simulators are increasingly being used to perform plant investigation and perform activities related to instrumentation and control systems such as, integration testing, dynamic testing, engineering simulation, and verification and validation

Simulators can provide a cost effective method for design verification before the start of installation Depending on the accuracy of their computer models of the plant, both engineering and training simulators can be used for the analysis of plant dynamics, design evaluation and verification and validation of software products However, the model limitations must be clearly understood and activities must be restricted to the validated operational space of the simulator

4.10.2. Engineering and analysis tools

The engineering analysis tools currently available include Computer Aided Design (CAD) engineering tools, design analysis tools, safety evaluation tools, and verification and validation tools These coupled to the plant distributed information and configuration management systems give the engineers and technicians access to the means of devising and testing proposed plant modifications to systems and equipment Great care is necessary to ensure that the flexibility, and in some cases the ability to make on-line changes, is not used to perform experiments on the operating plant that could jeopardize plant safety and performance

REFERENCES

[4 1] ELECTRIC POWER RESEARCH INSTITUTE, Implementation of an advanced digital feedwater control system at the Prairie Island Nuclear Generating Station, EPRI NP-6758, Final Report, USA (1990)

[4 2] ELECTRIC POWER RESEARCH INSTITUTE, Guidelines for Plant Process Computer Replacement, EPRI NP Report, TR-101566, Vol 1, 2, and 3, USA (1992)

[4 3] ELECTRIC POWER RESEARCH INSTITUTE, Proceedings 1986 Seminar on Emergency Responses Facilities and Implementation of Safety Parameter Display System, EPRI Report NP-5510-SR, USA (1987)

[4 4] ADRIAN, H ," Development of a Data Sampling and Evaluation System for radiation monitoring (ADAS 2)" ("Entwcklung eines Aktivitatsdatenerfassungs- und Auswertesystems (ADAS 2))" GRS-Jahresbericht,Germany (1993/94)

[4 5] ADRIAN, H , FELKEL, L , "ProVision, a configurable laboratory and process surveillance control, archiving and visualization system", IAEA Specialists Meeting on Modernisation of Instrumentation and Control Systems in NPPs, Garching, Germany, (1995)

[4 6] BASTL, W , HOFFMAN, H , "Development Steps towards an Advanced Computer Aided Plant Information System for NPPs" ("Fortschritte in der Entwicklung eines rechnergestutzten

Informationssystems (RIS) fur den Betrieb von Kernkraftwerken Kerntechnik 50/2"), Germany (1987)

[4 7] STADELMANN, W , MUCK, M , "NOVA a computer-aided system to monitor proper behaviour of plant components and to indicate the plant status in the Gundremmingen Nuclear Power Plant", IAEA/ANL Interregional Training Course on Prevention and Management of Accidents in Nuclear Power Plant Operation, Argonne, Illinois, (1994)

[4 8] TEIGEN, J , NESS, E , "Computerized support in the preparation , implementation and maintenance of operating procedures", IFAC workshop on computer software structures integrating AI/KBS systems in process control, Lund, Sweden (1994)

[4 9] BRUDY, D , "A thermal performance monitoring system for PWR nuclear plants", Collection of EDF-DER Internal Documents (Collection des notes internes de la Direction des Etudes et Recherches) N° 93NB00089, EDF, France (1993)

[4 10] BRUDY, D , PREUD'HOMME, E , BRARD, B , ALBOUYS, D , "CLIP Performance monitoring in PWR plants" ("CLIP controle des performances des centrales REP"), EDF, Revue Epure, N°44, France (1994)

[4 11] MOREL, J L , PUYAL, C , "On-line acoustic monitoring of EDF nuclear plants in operation and loose part diagnostics", SMORN 6, Gatlinburg, USA (1991)

[4 12] BENAS, J C , COTTE, J P , VERNEY, D , "Experience feedback on loose part monitoring in France 54 PWRs Particular cases in the secondary of a steam generator and in the vessel", SMORN 7 Avignon, France (1995)

[4 13] TRENTY, A , "Operation feedback on internal structure vibration in 28 French PWRs", Collection of EDF-DER Internal Documents (Collection des notes internes de la Direction des Etudes et Recherches) N° 95NB00030, EDF, France (1995)

[4 14] TRENTY, A , KLAJNMIC, H , "Operation feedback on internal structure vibration in 54 French PWRs during 300 fuel cycles", IMORN 23, Nykoping (1992)

[4 15] CHEVALIER, R OSWALD, G P , MOREL, J , "Monitoring of large rotating machines at EDF", Collection of EDF-DER Internal Documents (Collection des notes internes de la Direction des Etudes et Recherches) N° 94NB00063. EDF, France (1994)

[4 16] DUBAIL, A , DUEYMES, E GERMAIN, J L , VERBRUGGHE, E , "Detection et localisation de fuites dans les echangeurs de chaleur des centrales nucleaires" ("Detection and localisation of leak in the heat exchangers of the nuclear power plants"), Revue Epure, N° 11, EDF, France (1986)

[4 17] GERMAIN, J L , JANNETEAU, E , "Permanent monitoring of containment integrity the SEXTEN system", Collection of EDF-DER Internal Documents (Collection des notes internes de la Direction des Etudes et Recherches) N° 94NB00089,EDF, France (1994)

[4 18] SABATON, M , MORILHAT, P , SALVODELLI, D , GENETTE, P , "French experience in transient data collection and fatigue monitoring of PWRs nuclear steam supply system", Collection of EDF-DER Internal Documents (Collection des notes internes de la Direction des Etudes et Recherches) N° 96NB00050, EDF, France (1996)

[4 19] JOUSSELLIN, A , "Diagnosis of faults in EDF power plants from monitor to diagnosis", ASME pressure vessels and piping conference, Minneapolis, USA (1994)

[4 20] MAZALERAT, J M , MOREL, J , PUYAL, C , MONNIER, B , ZWINGELSTEIN, G , LEGAUD, P , "PSAD, an integrated tool for global vibratory and acoustic surveillance of EDF nuclear plants in the near future", SMORN 6 Gatlinburg, USA (1991)

[4 21] MOREL, J , MONNIER, B , "Material monitoring and diagnosis of their mechanical status", EDF, Revue Epure N° 44, EDF, France (1994)

[4 22] JOUSSELLIN, A , TRENTY, A , BENAS, J C , RENAULT, Y , BUSQUET, J L , MOUHAMED, B , "Monitoring and aid to diagnosis of French PWRs", SMORN 7 Avignon, France (1995)

[4 23] BYE, A , MOUM, B , "Alarm handling systems and techniques developed to match operator tasks", IAEA Specialists Meeting on Experience and improvements in advanced alarm annunciation systems in nuclear power plants, Chalk River, Ontario, Canada (1996)

5. NEEDS AND FEATURES FOR ADVANCED I&C SYSTEMS

5 1 ADVANCED I&C SYSTEM NEEDS

The use of advanced I&C systems can bring great benefit However, the issues associated with their introduction must be addressed within the context of meeting advanced I&C features which are presented below

5.1.1. Reliability

The I&C system must offer high reliability according to operation or safety requirements As the use of modern technology increases and more functions are automated, the reliability targets for the I&C systems have become more stringent New technology has resulted in increased complexity of the I&C systems, but has allowed good on-line and off-line diagnostics and self-checking features These features are also important to achieve higher availability targets Testability of I&C systems is needed to provide a demonstration of required level of reliability, according to the importance to safety of the system (classification)

Advanced I&C systems should exploit a diverse system architecture, in accordance with their importance to safety This will allow higher reliability and maintainability as well

5.1.2. Maintainability

Maintainability is becoming a growing problem with the increased complexity of modern control equipment and the many different systems that are being developed to solve specific application problems Previous solutions such as standardizing on the cheapest initial cost supplier, carrying out most of the maintenance in house and stocking ample supplies of spare parts are becoming more difficult and costly

Nuclear plants are being forced to depend on several reliable and financially secure power plant suppliers in order to achieve lower maintenance costs and delay the replacement of obsolete equipment as long as possible It is increasingly important to choose suppliers that support their existing clients by developing new and replacement products that can be integrated with the older systems

The new products must be easy to maintain and the replacement parts or spares are commercially available The system downtime due to maintenance must be low and the I&C system should have low mean time to repair (MTTR) On-line repair and zero downtime are also desirable goals

Aging has become more important as many nuclear plants are entering the second half of their useful economic lives Any aging phenomenon that was not correctly predicted or anticipated at the start of plant life are now beginning to surface New methods to identify the problem and to compensate for it are going to be required One area of growing interest is the durability of electrical cables, electronic parts and elastomer components especially in radioactive environments after many years of operation Methods to reliably predict end-of-life of equipment would be particularly useful to help plan for the equipment replacement during an outage Alternatively, methods to reduce or eliminate the need for signal cabling would allow expired cables to be abandoned and new technologies used instead (e g fiber optics)

5.1.3. Functionality and flexibility

Instrumentation and control systems must provide additional functionality to satisfy the needs of the many teams who are developing special applications to improve plant performance and economics Some of the growing areas of demand are (i) better (standard) communication capabilities, (ii) modularity of functions to facilitate graceful future replacement, (iii) standard software engineering methods to facilitate maintenance, (iv) ability to incorporate new advanced functions, (v) flexible and

easy way to configure functions, (vi) development environment that is easy to use by plant staff, (vii) facilities (e g drivers) that allow integration with other products, (viii) future expandability in both size and functionality, (ix) better configuration control capability

I&C system flexibility to changing requirements is an important need The nuclear industry is faced with changing regulations and periodic lessons learned from incidents and accidents at nuclear plants Regulators require that nuclear plants implement the important new requirements or face losing their operating licenses, which creates significant pressure and costs associated with retrofitting

The importance of having a flexible control system is significant The use of software based control systems have a natural advantage over hardwired control systems because many of the changes can be accomplished without major rewiring and hardware changes that require a significant plant outage

5.1.4. Scalability

Scalability is a key requirement on advanced I&C systems and comprises different sub-items to assure the adaptability of a system in order to have an economical design for a specific application

The main sub-items of scalability are

- a scalable performance of processor and bus systems, to meet the requirements specific to a design
  - to optimize the allocation of application functions to processing units during the design,
  - to have the possibility of later system extensions or functional upgrades without redesign of the hardware architecture,
- an adaptable redundancy level to economically meet the required fault tolerance according to the safety categorization of the implemented functions (see Fig 1),
- a flexible design of the hardware architecture according to the functional scope
-

Scalability is strongly correlated to economic aspects as the system is adaptable without the risk of a system exchange if, in case of a later safety analysis, the safety categorization of functions is upgraded (investment protection)

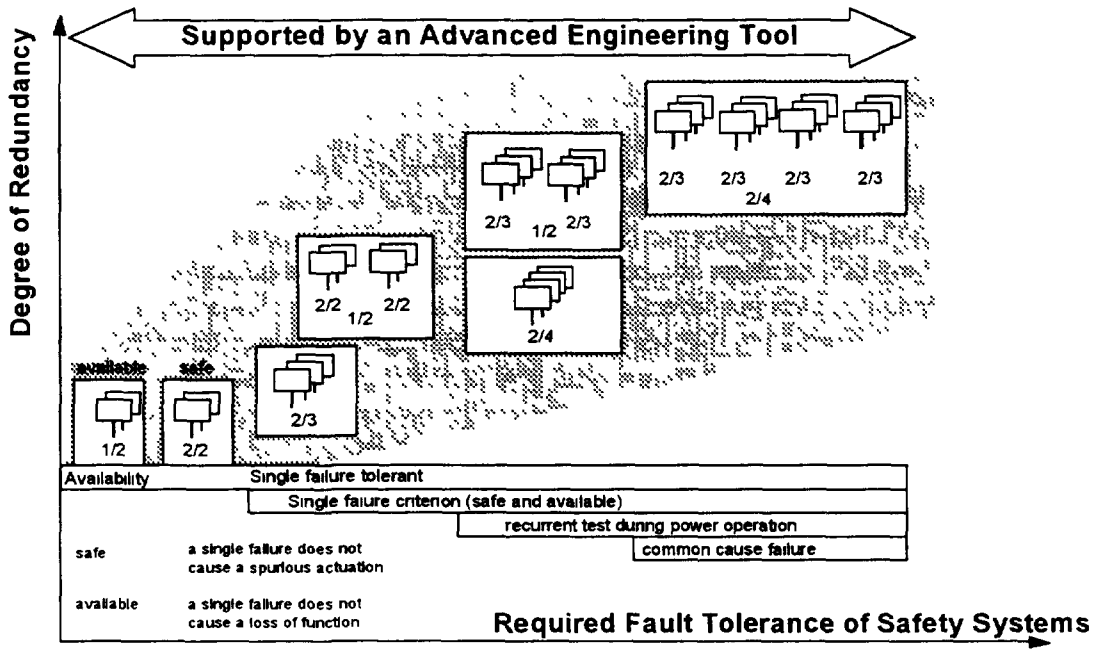


FIG. 1. Scalability of advanced control systems

5.1.5. Testability

To assure and maintain high availability and demonstrate high reliability of I&C systems, extended testability is necessary during operation and maintenance of the power plant Specifically, modern I&C systems allow

- integrity of the hardware modules to be tested by automatic self-testing procedures which are performed regularly by the processor system on a lower priority level (findings should then be presented on graphic displays),
- comparison of input and output data as well as intermediate results (between trains of redundant architectures)

In addition, typical recommendations are

- self-tests should be as complete and automatic as possible,
- functional tests should be done to confirm the consistency of the designed and the actual functions during plant operation and refueling outage

Testability of the I&C systems is also necessary for the verification and validation processes

5.1.6. Security

Administration and technical measures should be used throughout the life cycle of digital I&C to prevent security problem arising from errors introduced by unauthorized personnel, computer viruses, design or modification errors The system must also be protected from implementation of unintended functions

During operation and maintenance, it is necessary to continue to take into account security problems concerning I&C systems All unintended design configurations or disconnection in cabinets, which may be due to human errors during maintenance and testing, should be detected, preferably in an automatic manner

On-line diagnostics with built-in fail safe features are growing in importance as the control systems become more sophisticated and interconnected Security barriers which allow various users to interact with the system, but not interfere with high integrity functions, are also needed

5.1.7. Environmental qualification

The I&C systems must be environmentally qualified for operation during normal operation and during and after serious accident events as well as be able to withstand seismic events The worst case accidental environments are derived from the accident analysis, for example, main steam line break and loss of coolant events Many I&C products are available in the marketplace which are environmentally qualified This environmental qualification covers a wide range of areas, namely, radiation, temperature, vibration, humidity, electro-magnetic interference and radio frequency interference (EMI/RFI), power quality, grounding, chemical corrosion, and smoke The EMI and RFI requirements may include tests for electrostatic discharge immunity, radio frequency interference immunity, and transient interference immunity For seismic qualification, seismic tests should also be specified

Tolerance to electro-magnetic and radio frequency interference becomes increasingly important as low power, high speed circuits are used in the I&C systems The increased use of cellular telephone and other wireless systems inside the plant for communications will create additional demands on noise rejection for the control and protection systems

If the I&C devices are used in radiation environment, they need proper radiation environment qualification For example, advanced fiber-optical sensors and communication links require qualification concerning radiation monitoring for application in the radiation zones

5.1.8. Product qualification

The I&C products must go through a formal qualification process to demonstrate that they meet all the requirements as given in the technical specification (functional, performance and physical requirements), according to their importance to safety The products should also be shown to meet the required quality assurance level The product must be evaluated based on its operating history and the results of the acceptance tests

The application of off-the-shelf products designed for general industry purpose can be useful Results of previous type qualification and feedback on experience can be used and specific qualification tests will then be defined according to the requirements for qualification

Software product qualification should be very rigorous, according to the category of the function and system associated with the software

5.1.9. Verification and validation (V&V)

The I&C systems must meet the required level of verification and validation depending on the safety criticality of its application For a safety critical application, very structured and independent verification and validation processes are required (see IEC 880 [5 7], for requirements on safety critical software)

The application of advanced engineering tools for development, verification and validation can be very efficient The testability both during development and operation of the I&C system is important for the V&V processes

5.1.10. Cost

Many of the I&C systems developed by suppliers in the past led utilities to choose between a high capital cost with low operating cost or the reverse The new open international standards and third party products are permitting some suppliers to offer both low initial cost and low operating cost systems These systems typically are more modular and make better use of standard off-the-shelf industry standard components

New systems exhibit self-checking attributes and monitoring capabilities that allow the state of equipment to be known immediately This facility can be used to reduce manual intrusive checking of parts and, in conjunction with redundancy within systems, increases the availability of the system

Nuclear plants will continue to demand a high degree of standardization in their I&C systems in order to control both capital and operating costs The I&C related maintenance cost, outage cost and unavailability cost must be minimized Indirect cost due to licensing delay caused by a new digital system should also be taken into account

5.1.11. Configuration control

Configuration control is essential for the safety of the plant This control can be compromised by poorly executed modifications, inappropriate operating configurations, or incorrect maintenance work This latter includes inappropriate parts replacement, incorrect calibration or ill advised work protection isolation

The use of digital technology and computer based information systems can make the problem of effective configuration control more difficult than in earlier years because changes and 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

Security requirements concerning the possibility of configuration changes should be established Automatic system reconfiguration in case of failures of separate system parts is useful for providing system working ability

The matter of configuration management tools is a growing area of interest in nuclear plants Advanced I&C system should have its own configuration control and assists the nuclear power plant to implement a plant wide configuration management system

5.1.12. Modification

There are several reasons that bring about I&C system modifications in nuclear power plants Usually, the reasons for I&C modifications are technological changes, such as replacing old analog systems The activity in this direction should take advantage of the availability of "proven" advanced I&C technology being used in other industries Modification of I&C systems should allow new function fulfillment such as signal validation, drift elimination and self-testing Advanced I&C systems will facilitate advantages such as reliability improvement, high capacity, flexibility, less number of cables and cabinets, better stability and maintainability

Modifications concerning display and monitoring systems should lead to creation of more user friendly information and control environments, and simplify the human-machine interface Also, it is important to be able to communicate with plant information management and work management systems to help support better decision making

The requirements for future modifications should bear on the use of standard interface application, open system architecture and support from software & hardware suppliers

5.1.13. Human-machine interface

The new I&C systems often introduce new forms of human-machine interfaces (HMI), and, therefore, must go through rigorous and formal review to ensure that the human-machine interface is effective Existing I&C devices were not designed or chosen based on the same level of requirements or licensing scrutiny Because HMI problems have been recognized as having caused significant events in NPPs, this interface is now subject to much scrutiny by the regulators

The new I&C equipment must meet all the current plant requirements based on existing applications, interface with other systems, human factor issues, information display and the need for better operating, testing and maintenance procedures

Advanced HMI systems, when properly designed and introduced into the plant, should help to prevent incorrect actions of operators in all plant operating modes and enhance plant diagnosis and maintenance

5.1.14. Information management

The improved communication and information distribution facilities of advanced control systems, particularly those that are computer based, can bring significant benefit The design, maintenance and operating work environment should be supported by data base features such as instrument input/output lists, annunciation lists, calibration tables, hardware and software configuration tables, etc

These data bases should be designed to meet the needs of the operation staff, in order to ensure that the operation of the plant process is adequately taken into account In this way, the creation of separate data bases outside the system to help manage the work ought to be minimized

5 2 FEATURES OF ADVANCED I&C SYSTEMS

The state-of-the-art I&C systems provide considerable advantages to plant operation Over the last two decades, enormous development has taken place for digital I&C technology, whereas for analog systems, the variety of analog modules available on the market has been reduced year by year

The main advantages that can be gained using digital control systems in comparison with analog systems are

- reduced cabinet volume,
- cost reduction,
- strong correlation between actual functionality of the implemented system and the documentation,
- possibility of functional adaptations by software upgrades,
- reduced effort for recurrent tests by use of automated test and self-checking facilities,
- reduced maintenance work by means of diagnostic systems

5.2.1. Process control functions

The main design features required of advanced control systems include

- distribution of control tasks including hardware separation,
- bus technology application,
- single fault immunity,
- automatic reconfiguration in case of faults,
- scalable hardware and software features including redundancy of components

5.2.2. Human-machine interface (HMI) functions

The human-machine system carries out information tasks for operator activities The main features required of advanced HMI systems are

- operation and information facilities optimized by operators,
- task related flow diagram presentation of information (from a plant engineering, process engineering and I&C engineering point of view),
- decoupling of processing units from the operating terminals to permit highly flexible control room design,
- distribution of data and functions (representations and operation options of the entire plant are available on each monitor by means of a terminal bus),
- tasks clarification carried out using advanced engineering tools which support the operation engineering (e g alarm management and plant or system status displays) and perform the data management via a relational data base,
- integration of relevant standards such as UNIX®, X/Windows, OSF-Motif

Information on how to integrate advanced HMI systems in existing control rooms can be found into IAEA-TECDOC-812 [5 1]

The display equipment of advanced process control and information systems should meet the relevant HMI requirements (according to applicable standards, e g IEC 964 and IEC 1772) for the presentation which should include the following considerations

- high resolution and flicker free display,
- the integration in the control room should assure acceptable conditions for mirror and brightness effects,
- task related control room design by operator related displays (e g 50 cm screens) and wide screens (e g 2 m screens) for overview information All information presentations available at operator workstation can be displayed on the wide screen for overview information if necessary for plant operation,
- the parallel application of operator workstation and wide screen overview information require an arrangement in the control room that does not stress the eye-adaptation capability of older operators,
- window technique and zoom facility, to enable the presentation of detailed information on a relevant system

5.2.3. Advanced diagnostic systems for the I&C system and peripheral devices

Based on digital I&C systems, distinction must be made between the diagnosis of the I&C system itself and the diagnosis of peripheral devices, such as transducers or valve positioners and pump drives

5.2.3.1. Advanced diagnostic systems for I&C systems

To support service and maintenance work as well as fault analysis, diagnostic systems can be permanently linked to the control systems Main functions for advanced diagnostic systems are

- automatic recognition of I&C faults,
- conditioning of the recognized faults and compressed representation in graphical form,
- guiding the operator to the faulty component (localization) via the device structure in an interactive mode,
- representation of the faulty component including detailed information concerning repair (version management),
- logging, statistics and evaluation functions,
- support repetitive maintenance work on components (e g sensor calibration)

5.2.3.2. Advanced diagnostic systems for peripheral devices

An option of advanced diagnosis is provided by the application of field bus systems (see Section 5 2 5) in combination with computerized switchgear technology Typical diagnosis are

- diagnosis of sensor and transducer functionality by noise analysis,
- diagnosis of the operating behaviour of valve positioners (relation of torque via valve travel) and pump drives (power demand) to get the input data for condition based maintenance (Section 3 3 3)

5.2.4. Off the shelf systems

The need to reduce the cost for the development and implementation of advanced I&C systems drives the application of off the shelf systems designed for general industrial control purposes

The application of an off the shelf system requires many aspects to be considered Requirements to choose, assess and qualify an off the shelf system will be given in the future supplement 1 to IEC 880 (this supplement is presently at the stage of IEC Committee Draft with Vote)

Typical considerations of the off the shelf systems include the following

- Serial products generally show a dynamic product behavior It is crucial that the system manufacturer demonstrates a long term strategy with upwardly compatible components both for hardware and software A key item to this is a clear structured system of standardized interfaces
- The basis for the nuclear qualification, as a precondition for a licensing procedure, is the development and manufacturing documentation in accordance with relevant standards, e g ISO 9000 [5 2], or, in the future, IEC 1508 [5 6]
- The qualification is generally related to a "proven" control system with a document version index for all components (HW and SW)

An advanced I&C system is often based on a powerful standard processor This processor should have a world-wide usage to assure high reliability with high probability for the correct performance of all processing tasks and long-term availability It is highly desirable to have several second source suppliers on the market for the key components of the I&C system

5.2.5. System communication

5 2 5 1 Advanced cabling and multiplexing

The move to extend the level of monitoring of equipment and structures has given rise to a major increase in the number of cables, cable penetrations and junctions that have to be installed The number of cables and connections are reaching the point where installation of cables and their management are coming to dominate installation cost and be a potential threat to structure integrity because of the large number of penetrations Connections are a source of error and checking integrity presents a major load during maintenance In response to this, there is a move to introduce multiplexers and data concentrators in the field Once issues of equipment hardening and qualification are overcome this presents the possibility of greatly reducing the amount of field cabling, penetrations and junctions and introducing redundancy in cable routes However, the difficulties in managing the consequences of the loss of a multiplexer or data concentrator are still to be overcome

5 2 5 2 Networks

The system communication should be based on relevant standards according to the ISO/OSI (Open System Interconnection) Model, e g

- Ethernet IEEE 802 3
- Interbus S
- Profibus EN 5017

It should meet the design requirements at minimized costs Due to security concerns, it is generally considered that current open LAN architectures are not licensable for safety relevant systems, but the technical features for an open architecture should be met with respect to later enlargements Interface boards to perform links with other standard systems should be available The application of optical fibers as well as copper cables should be possible without impact on the software design The bus system used should meet fault tolerance to achieve high availability independent of the application of redundant bus architecture (e g by virtual ring technology)

5 2 5 3 Communication field bus

The introduction of field bus technology represents a major breakthrough in I&C technology, because it allows automation functions to be redistributed Simple functions, and particularly functions which directly address a specific field component, are shifted to that component, thereby reducing the burden on the automation processor The field bus takes over communication tasks and replaces a large portion of present-day cabling, decreasing the number of cables, cable penetrations, connections and I&C cabinets

This reallocation of functions can be viewed as a "downsising" of automation systems, and will break up the development, engineering and configuration, and commissioning Pre-processing in the field provides a high level of decentralization and real-time functionality (in particular for example, FIP bus allows the determinism of the communications) Field bus technology will close the gap between digital data communication and automation systems and field devices

Field bus technology is not yet applicable for systems in nuclear parts of NPPs with respect to radiation sensitivity of microprocessors Nevertheless, it will gain importance in the balance of plant systems with comparable requirements as for fossil power plants

5.2.6. Advanced engineering tools

For engineering support, advanced engineering tools are useful to cover the following main items

- Specification of I&C functions and hardware structure via an editor system based on graphical presentations
- Automatic code generation of source as well as object code for the control system, and a standard language code suitable for simulator tests
- Document management facility based on a data base applicable also for plant operation
- Support of the original engineering as well as all later modifications during plant operation

Moreover, the following needs appear on the I&C engineering, for ensuring usability and durability of the I&C applications

- The specification of I&C applications must be as independent as possible from the evolution of the equipment technology, in order to follow the evolution of technology more easily
- That independence is accompanied with the need to specify and design I&C applications which will be implemented using off-the-shelf products
- Engineering methods and tools should evolve to become more user-friendly This feature is necessary to improve the productivity and quality of the engineering studies

5 3 EUROPEAN UTILITY REQUIREMENTS FOR I&C OF LWR NUCLEAR POWER PLANTS

Seven European utilities have been collectively defined unified requirements for the next generation of European NPPs

These utilities are

- Nuclear Electric from UK
- Tractebel from Belgium
- Electricité de France from France
- Vereinigung Deutscher Elektrizitatwerke from Germany
- DTN from Spain
- ENEL SpA from Italy
- KEMA Netherlands B V from Netherlands

Since December 1995, Finnish producers (IVO & TVO) and Swedish producers (Vattenfall) became associated members

In the common requirements for Light Water Reactor (LWR) nuclear power plants, there is a chapter dedicated to I&C

The requirements define a classification of NPP functions, systems and equipment on a basis not in contradiction with IEC 1226, but more precisely taking into account feedback of experience Three

safety levels are defined following the defense-in-depth principle as well as design extension corresponding to post accident conditions after 24 hours

- Safety level F1, which includes two sub-categories
  - safety level F1A the safety functions needed to demonstrate that the plant can reach a controlled state for any design basis condition,
  - safety level F1B the safety functions needed to demonstrate that the plant can reach and be kept in a safe shutdown state up from design basis condition, for at least 24 hours
- Safety level F2 the safety functions needed to demonstrate that
  - the plant can be kept in a safe shutdown state up to 72 hours from any design basis conditions,
  - the plant can deal with the design extension conditions up to 72 hours,
  - the plant can withstand the internal and external hazards considered in the design over and beyond those included in the design basis analysis
- Non safety functions any other function

The classification of the systems and equipment is done according to their contribution to the functions important to safety with respect to the overall I&C architecture

Rules are defined concerning general I&C principles (main functional structure of I&C, main objectives of I&C functions, distribution of I&C functions) and overall I&C architecture Then, at a lower level, requirements are given on automation and protection systems, human-machine interface, applications connected to the main process information and control system, and off-site applications

Among the safety requirements of the systems and equipment, associated with the safety function levels they perform, one can note the following

TABLE I SAFETY REQUIREMENTS FOR DIFFERENT LEVELS

Requirement	*F1A*	*F1B*	*F2*
Single failure criterion	Yes	Yes	No(1)
Back-up on-site electrical supply	Yes	Yes	No(2)
Physical separation between divisions	Yes	Yes	No(3)
Automatic actuation	Yes(5)	No	No(4)

(1) Redundancy may be required for the case of equipment which is inaccessible or, if required, to meet probabilistic targets, or for certain hazards
(2) Yes for those functions which require electrical supply of high reliability in the relevant conditions
(3) Yes for specific hazards, for example fire
(4) For certain design extension conditions, there may be exceptions, to be considered on a case by case basis
(5) Some slowly developing accidents may be exceptions

At the end of 1995, these requirements were agreed among the involved European utilities Then, each utility had to discuss them with its licensing authority The requirements are in line with the studies in progress within the EPR project (French/German project for common basic design studies on a future nuclear reactor) Furthermore, during these studies, common EPR technical rules for control systems are established The EPR results are foreseen for 1997

REFERENCE

[5 1] INTERNATIONAL ATOMIC ENERGY AGENCY, Control Room Systems Design for Nuclear Power Plants, IAEA-TECDOC-812, IAEA, Vienna (1995)

6. ACCEPTANCE AND SAFETY JUSTIFICATION[1]

This chapter addresses the key items relevant for the acceptance of advanced I&C systems for all safety categories [IEC 1226 A, B, C, and NC] in nuclear power plants which are

- Staff involvement
- Training
- Documentation
- Licensing

6 1 STAFF INVOLVEMENT

The involvement of the plant staff and the means of meeting their needs is considered The key groups of staff must be convinced that the system will meet their needs The weighting of the significance of the groups acceptance will be dependent on the nature of the I&C system If the I&C system is important to safety the agreement of the licensing body is essential

6.1.1. Specification and dsign

The requirements specification, which is usually set down by the utility personnel, must capture, in addition to the required functionality, the constraints arising from the space and services available and reflect the plant operating procedures The involvement of the operations staff is particularly important for systems containing human-machine interface

The subsequent design process transforms the requirements and should generate the evidence needed to demonstrate that the required objectives have been met The staff participating in this exercise will include

- Plant management for safety, reliability and costs These staff are concerned with reliability and availability targets of the equipment in addition to the cost of implementation including procurement, licensing and maintenance costs
- Safety engineers for functionality and compatibility In addition to specifying and ensuring that the functionality of the system has been achieved, these staff will be interested in the consequences of failure of the system and thus the defensive features it contains Their input will include many non functional requirements to ensure that the system meets the requirements of the licensing body
- Control room staff for reliability of system, operability of system and interface with other systems The staff will be closely involved in specification of the system, understanding of the impact of the system on plant behavior and acceptance of the human-machine interface
- Maintenance engineers for work load and accessibility The staff will seek to minimize cost of ownership and ensure ease of maintenance by specifying requirements on fault diagnosis, accessibility, feasibility of performing on-line maintenance and repair They will also examine the proposed implementation with respect to component availability and long term support of the system

The output of the design process must meet the needs of the groups identified above and in addition be suitable for third party assessment in the case of safety systems Difficulties are anticipated with the recognition of the impact on the plant of introducing the system and ensuring that all safety implications have been identified Communication between the design team and the plant personnel can

---

[1]Chapter 6 gives an overview on the main items for the licensing procedure as well as for the acceptance by the plant staff More detailed information will be given in the IAEA-TRS "Safety Approaches for Implementation of Advanced Protection, Control and Human-Machine Interface Systems in Operating Nuclear Power Plants", which is presently under preparation and will be published in 1997

be facilitated by use of prototypes and animation to make the consequences from specifications and design transparent

6.1.2. Licensing

The responsibility for plant safety and consequently the safety demonstration for the upgrades lies with the plant owners and their safety engineers must take a leading role The safety engineers will require the support by the designers staff e g by safety analysis to complete the demonstration The nature of advanced technology with respect to complexity and novelty may require expert subcontractors to be used to support the demonstration process as the system is reviewed by the regulatory body The novel features of an advanced system must be regarded as a threat to successful licensing and, given the difficulty already encountered in introducing computer based systems for plant protection, the need to develop new safety arguments must be anticipated In the light of this communication with the licensing body is essential to ensure that there are no surprises late in the design phases or the safety demonstration

6.1.3. Operation and maintenance

The introduction of a new system will result in the need to review and revise operation and maintenance procedures Changes to operation can arise because of changes to the operator interface to the plant and changes in the plant behavior The operators must be informed and trained on the proposed changes and the documents on station procedures and new operating instructions and procedures must be prepared Similarly, maintenance personnel must prepare procedures and instructions for the new system and produce an impact statement Finally, all existing procedures and instructions must be reviewed to ensure that all consequences of changes as well for normal operation as for accidental conditions have been accommodated Failures to achieve this will have a significant negative impact on the utilization and reliance on the new system and consequently on plant safety

6 2 TRAINING REQUIREMENTS

The training program should include all persons involved in the use and maintenance of the new systems The training strategy will differ when replacing a system compared with that when applying advanced systems in a new plant In the former case training will be related to a changed process i e replacing the familiar old with the unfamiliar new In the latter case the new technology will be introduced as a part of the normal training programs

The programs will have to pay due consideration to the availability of staff In the case of an upgrade exercise many of the staff who will need to receive training will be involved in change activities on the plant The logistics of withdrawing the staff, providing training and then returning them to work with the new equipment becomes difficult particularly as the upgrade will occur during an outage when the demands on staff time are greatest If the system is essentially passive with little need for operator interaction, then it may be possible to train a core team for short term operation delaying training for the majority of personnel until after the system has gone into service If the system results in a significant change of plant behavior, or operator interactions it is recommended that the training program is planned as an integral part of the activities A stepwise introduction to the new I&C technology is preferably starting with auxiliary plant systems e g water treatment or the ventilation systems This gives the operator staff the opportunity from one outage to the next, to get familiar with new technology and the relevant operating procedures during daily work while the main plant systems are still running with the old I&C

Issues to be addressed during training should include an introduction to the technology and the consequences of its use The increased flow of information to the operator should not lead to information overload and loss of understanding The increased level of integration also requires operations and maintenance staff to be much more aware of the potential loss of functionality as a

consequence of taking a system out of service This requirement must be reflected in the training of the staff and active measures will be required to extend their scope of knowledge

The use of plant simulators for training operators provides the best way of increasing knowledge of system and plant behavior Functional simulators can be developed for separate parts of the technological process and used to help operators to understand the consequences of changes The use of full-scope simulators should also be considered when introducing new human-machine interfaces

6 3 DOCUMENTATION

The types of required documents and the criteria for the acceptance are the same for the replacement or upgrade of systems as required for the installation in a new plant However, in the case of replacement a review of all documentation will be required to ensure that all dependencies on and references to the replaced system have been dealt with Training material for a replacement system may contain some form of cross reference table to relate the old and new systems and functions, this material may be suitable for inclusion in the new procedure manuals

6.3.1. Design documentation

The design documentation package will be extensive including the descriptive material along with the verification, review, test and validation reports For simplicity the material has been divided into the three parts specification, detail design and test documentation

The plant system engineers will be responsible for checking the system aspects of the specification The operational staff is expected strongly to influence and finally to approve the human-machine interface The requirements for alarms with respect to equipment failures and close operation of the plant to operating limits will also be subject of agreement with the plant operators and safety engineers The format of the documentation must allow maintenance of the system over the total life cycle

The design documents will be in the responsibility of the designer, however the plant staff will have a significant input, the greatest being with the human-machine interface The documentation may be subject to several iterations at this stage as the final form of the interfaces are agreed with the operators e g as the result of an animation or rapid prototyping exercises It is important that, on the completion of this documentation package, the station staff reviews the documentation against the requirements of maintenance It is also advisable to ensure that, in addition to the mandated descriptions, there is sufficient information to identify important design constraints to ensure that they are not violated during some future design steps or next intended upgrades

The test documentation should report the successful completion of the validation and acceptance of the system and provide the basis for regression testing of the system and its software following any change i e adaptive or corrective maintenance activity User input is particularly valuable at this stage as advice on the expected operational regimes of the system This will allow testing with focus on stress and load testing of the system in a realistic manner

6.3.2. Licensing documentation

This documentation contains the justification that the system will meet the specified safety objectives for the assessment of the systems impact on plant safety The form and content of this package will depend on local licensing regime

6.3.3. Operation and maintenance documentation

The operation and maintenance documents and procedures are essential for the safe operation and maintenance of the plant The documentation will be system dependent and consist of two main components The first set of documents relate to the operation of the equipment covering start up, shut

down and periodic test schedules The second set of documentation will relate to fault finding and repair and will include manufactures manuals, data and drawings User input here is initial indicative of the expected document content and format which will be governed by current station practice hence station staff input is essential Finally, the existing documentation of other systems with interfaces to the new systems will have to be reviewed and modified to accommodate the changes introduced with the new system

Current practice for the development of operation documentation varies nationally In Russia, for example, operation documentation such as instructions, manuals is developed by NPP staff from the design documentation and must be agreed with design organizations In other cases for example in the UK the operation and maintenance documents are usually provided by the system supplier Given the complexity of an upgrade this activity should be undertaken jointly by the plant and suppliers staff

6 4 ACCEPTANCE IN THE LICENSING PROCEDURE

The safety issues and requirements for advanced control and instrumentation systems are in principle the same as those for conventional systems covering all aspects of the design, installation, commissioning, maintenance and operation of the systems The safety functions of the I&C systems should be classified according to their importance to safety and accordingly design, verification, qualification and validation have to be performed The system should be structured to minimize the size and complexity of the safety critical portions of the system and to keep the commonly accepted safety principles defense-in-depth, defense against common mode failure and compliance with the single failure criteria

Licensing process for advanced systems is currently less mature than that for conventional analog systems for demonstration that the system has met the functional requirements, reliability targets and does not impair plant safety The scope and nature of the demonstration will be dependent on the complexity, novelty and safety significance of the new system There are also differences within a backfit, as the case of a functional identical replacement, will differ markedly from the case where the new system is to provide additional functionality and improve plant performance In the former case confidence building through parallel running of the old and new systems will be possible In the latter case the approach will depend on the magnitude of the change to be made In some cases it may be possible to adopt an incremental upgrade strategy to migrate away from the original functions In other cases a complete revision will result and the implementation strategy must include appropriate consideration of all those affected by the change

System acceptance can be made easier by the use of field trial and demonstration, however, their nature will be dependent on the availability of suitable test harnesses and simulators Test harnesses will be required to check both the static functionality and the dynamic behavior of the system These checks should be a minimum requirement for the system and form a part of the acceptance tests The ability of the test harness to stress the relevant system features will be particularly valuable

Simulator testing is also very valuable as a complement to the field trials using a test harness The use of simulator generated inputs will allow the equipment to be exercised through a range of anticipated transients The successful execution will help to build confidence in the correct performance of the system Simulator based testing is valuable where there is a significant interaction between the operator and the equipment as, in addition to testing the performance of the equipment It allows to check and demonstrate the adequacy of the operational procedures and the human-machine interface

7. ENGINEERING PROCESS

This chapter addresses the essential engineering activities undertaken during design, manufacturing and installation of digital I&C used to carry out safety and control functions in a nuclear power plant A major objective of this chapter is to evaluate advanced system design methods and making use of software tools and reuse of software New aspects from these methods with respect to requirements, design, verification and validation are carried out

7 1 GENERAL CONSIDERATIONS

7.1.1. Requirements for engineering process

Deficiencies in the engineering process may result in design faults of a digital I&C system which could fail The safety problems that can result from these faults make it necessary to establish a proper engineering process containing active measures to prevent errors and detect faults Current thought is to structure the engineering process into different phases and to check the results of each phase to be a correct interpretation of the previous phase and subsequent requirements The effectiveness of these verification activities strongly depends on the engineering process and the representation of the results of the phases The use of formal methods in a tool based engineering process may reduce the importance of verification steps

The following standards contain which should be taken into consideration IEC 880 on software for computer in the safety system of nuclear power plants, IEC 1226 on nuclear power plants instrumentation and control system important to safety - categorization, IEC1508 on functional safety of I&C and ISO 9000 on quality management and quality assurance standards

Requirements concerning verification and validation activities are given in IEC 1508 (Part 1 paragraph 7 chapter 18) Adequate tools should be applied to the design and verification I&C systems according to their safety integrity level IEC 880 First Supplement, presently in draft status, should be consulted for the application of reusable software

In addition to the safety aspects, the engineering process can also contribute to an economic gain by a reduced design effort and simpler maintainability of the I&C due to better specification, easier configuration of the I&C equipment and better configuration management

7.1.2. Categorization of safety functions

To achieve an adequate level of safety for a specific application, it is necessary to define safety integrity levels for the safety functions to be implemented by the safety system A categorization of safety functions depending on the gravity consequences of malfunction is given in IEC 1226 Each category of safety functions has to be satisfied by a system of an equivalent integrity level In IEC 1508 the integrity level is defined as the probability of a system correctly performing the required safety function under all stated conditions within a stated period of time The design and qualification as well as the verification and validation criteria are derived directly from the allocated safety integrity level

7.1.3. Requirements gradation

To achieve sufficient reliability the requirements of safety functions are graded according to the categorization in IEC 1226, the A, B, and C categories important to safety The requirements for the three categories differ significantly

The basic requirements on failure rate require an accepted QA-System for all categories But only categories A and B require that the manufacturer is licensed by QA-audits and that it has to establish a module version (configuration) management system for hardware and firmware

Proofs are needed for all categories that the hardware system meets the requirements on robustness for NPP application regarding to seismic stress, environmental conditions (IEC 1226 / 8 4, e g temperature, humidity and pressure), power supply, electromagnetic compatibility Verification of relevant manufacturer data sheets is compulsory for A, and optional for B

The failure rate of the hardware system has to be evaluated to form the basis for reliability proofs The MTBF (meantime between failure) of the main modules (e g processor board) should not exceed a value of 10^{-5}/h The evaluation is compulsory for A and B, and optional for C

Single Failure Criterion as given in IAEA Code 50-C-D has to be met by the design of the system architecture That leads to compulsory design requirements for category A and to recommendations for category B Additionally, it is recommended that redundancy is used to overcome single failure during repair

To avoid common mode failures which cause unavailability of associated functions by hardware faults, the possibility of common initiating events on redundant channels/trains has to be excluded by an adequate design for category A This requirement is optional for category B The requirement leads to spatial separation of redundant trains and allocation to each train of separate equipment for environmental conditions (temperature, humidity, pressure) and of separate power supply, to electric isolation between the trains and other systems, to design against specified seismic stress, and to design against EMI (electromagnetic interference)

Faults due to errors in the I&C specification, originating from misunderstanding between process engineer and I&C engineer, can be overcome by the application of functional diversity This is required for category A systems (first supplement to IEC 880)

Regarding interference by the application software on hardware and firmware of the processor system triggered by input signal trajectories the cyclic processing of the application code including all data transfers is a key requirement This strict cyclic processing is up to the present knowledge the essential feature of the whole processor system to get rid of the problem of processor and bus load variations It is evident, that the huge variety of possible signal trajectories makes it impossible to prove sufficient processor and bus performance by tests This requirement is compulsory for category A and optional for B

For the processing of safety relevant control tasks according to category A, a reduced operating system kernel is sufficient This makes it possible to perform a type test by theoretical checks of the operating system itself Of course this system can be used also for other categories On the other hand it is possible to use a broadly applied proven operating system, also in other categories than category C To include dynamic checks for correct program processing the application of assertions should be applied, in all categories

7.1.4. Verification and validation

The verification activities should be applied to all phases of the engineering process The engineering process shall be designed such that weak links and potential deficiencies are avoided A qualitative analysis of potential error sources coordinated to the required integrity levels shall be used as a base to define an adequate engineering process and the associated verification activities The engineering process in combination with required safety integrity level is often used to determine the scope of the validation activity although the testing elements of this activity are also determined by customer-specified acceptance testing The quality of the engineering process can be credited to reduce the scope of verification and validation activities

7 2 FEASIBILITY STUDY FOR AN INTENDED I&C UPGRADE

One of the first steps undertaken in preparation for a proposed upgrade of an old hardwired I&C system is a feasibility study The main items in this feasibility study are described in this section

7.2.1. Interface to existing plant systems and impact analysis

An upgrade will require a good interface between the old and new equipment as well as interface between the operations staff and the new equipment Some of the issues to be considered are

- definition of functions to be backfitted and functions to be kept as they are,
- definition of functional upgrade within the scope to be backfitted,
- comparison of required and available space for cabinets,
- performance analysis of power supply and air-conditioning system,
- interfaces to existing I&C systems
  - measuring input signals,
  - other input signals,
  - output signals to the switchgear/actuators,
  - interface to the process information system,
- interfaces to main control room and emergency shut down station,
  - analysis of electromagnetic interference (EMI) between old and new equipment,
  - compatibility of signal stops,
  - sufficiency of damping performance of old cabinets,
  - noise interference,
  - special compatibility tests for arrangements of new and old equipment in the same cabinet,
  - interference via a common power supply,
  - grounding,
- installation and commissioning strategy,
  - time schedule for the backfitting,
  - definition of scopes depending on scheduled outage periods for installation and commissioning,
  - requirement of an on-line-open-loop period for operational experience,
    - comparison with old functions,
    - service experience of plant personnel,
- codification concept for the backfitted functions and the associated documentation in accordance with the existing plant documentation management for the upgraded I&C system,
  - during plant operation and in case of later adaptations,
  - including interface to the existing plant documentation,

7.2.2. Cost benefit analysis

The key items to be included in a cost benefit evaluation are

- the budget estimate for the backfitting,
- the cost-reduction for repetitive/routine tests of the new I&C systems compared with existing systems,
- the cost propagation of spare parts and services for old I&C systems in operation,
- advantages of functional upgrades e g
  - increased power level by reduction of processing inaccuracy and margin between operating parameters and safety set points,
  - improved plant power maneuverability under variable load conditions
- cost of training,
- cost of generating and completing the safety arguments

7.2.3. Safety and reliability evaluation

The work will usually have to demonstrate that the original safety requirements have been met and that changes, usually enhancements, in safety requirements will be met. Tasks will include:

- References to risk assessment and other safety analysis documents.
- Qualification of the system by independent experts of hardware and software (mandatory for category A and recommended for category B functions).
- Evaluation of availability and reliability figures.
- Justification of self-checking features and strategy for recurring/routine tests
- Data security concept to assure code and parameter integrity during the scheduled plant operation

The safety evaluation and the demonstration to comply with the safety requirements will form a major part of an upgrade.

7.3 REQUIREMENTS FOR SOFTWARE TOOLS

While there are many approaches to software development, it is widely accepted that the state of the art in software engineering development practice includes a clear subdivision of the whole process into different phases with a verification of the output of each phase against the inputs The process is completed by a final validation to demonstrate via tests and analysis that the system of software and target hardware fulfills the original requirements. Presently the engineering processes with the highest reputation are those based upon IEC 880 (Fig. 2)

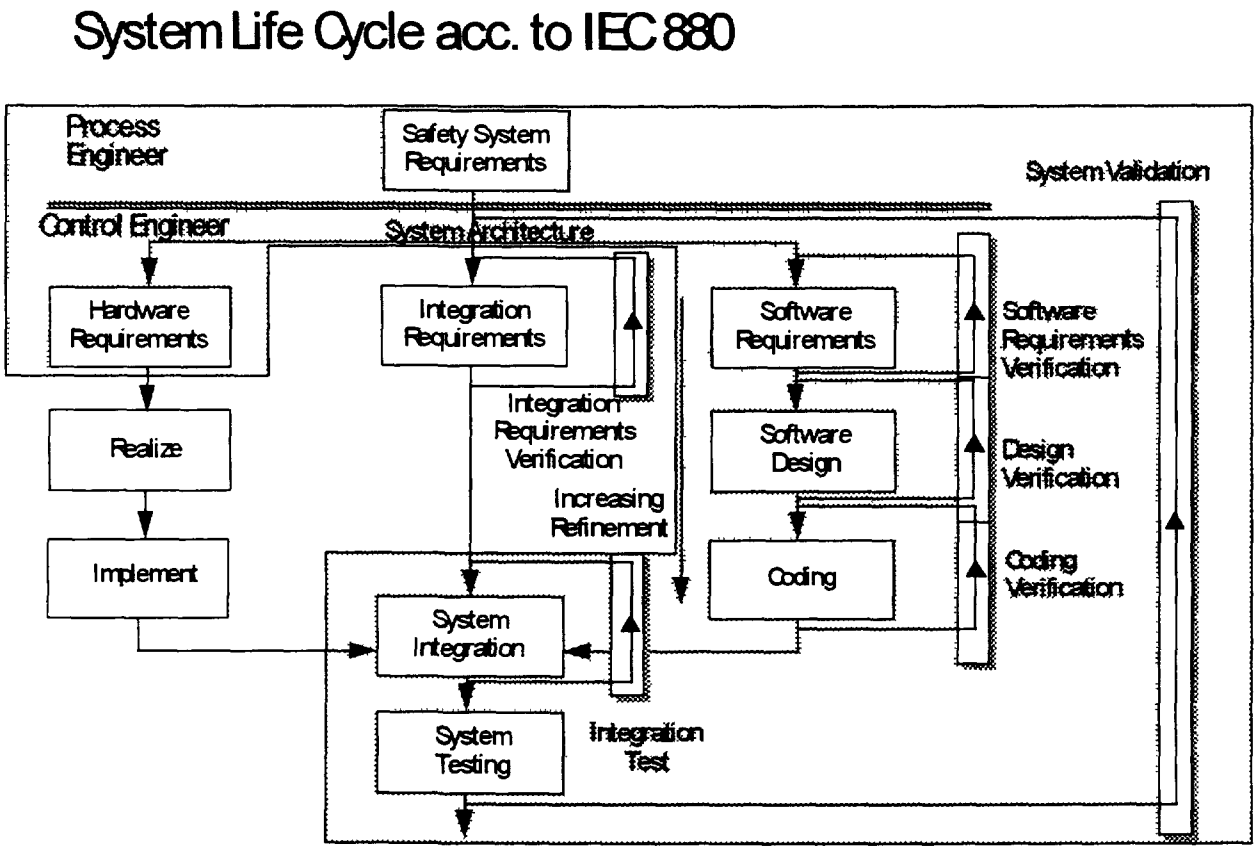


FIG. 2. System Life Cycle according to IEC 880.

Fig 2 shows the System Life Cycle according to IEC 880 for software development

The shadowed part from the IEC 880 engineering process is discussed in detail for tool based advancements

7.3.1. The IEC 880 engineering process

The IEC 880 engineering process is aimed at software products developed by task-specific software engineers The process is discussed in the context of plant modernization

The safety system requirements are elaborated and documented by the process engineers who are responsible for design of the process and the safety relevant process systems by means of the safety analysis methods The key requirements essential for plant safety are

- Safety parameters and their relevant limits
- Functional requirements such as
  - calculation algorithms,
  - automatic signal verifications,
- Response time tolerance
- Classification of the safety relevant functions
- Fault tolerance

These requirements are the basis for the engineering phases which are described in detail in the following sections

The safety and control functions are used by the I&C engineer to determine the system and software requirements This phase should show and document in the language of the I&C engineers that they understood correctly the requirements The verification to this phase performed by the process engineers confirms the correctness of the I&C engineers' interpretation of the requirements As a weak point has to be seen the relationship between the processor load and the bus load with the system performance The adequacy of this relationship according to the IEC 880 process has first to be estimated on the experience of the I&C engineer but can be proven in the later system integration phase at the earliest

In the software design phase, the overall software architecture requirements are defined The software is structured and the coding conventions are fixed The coding phase is performed by software engineers using the output documents from the software design phase The system integration phase can be performed in one or several steps The source code is compiled to produce the object code and tested on the target hardware system The hardware realization path is to be performed in parallel but independently

In the final validation the overall system behaviour of the hardware system with integrated software, within its operational environment, is checked against the original system requirements

7.3.2. Advantages of reusable software

The first supplement to IEC 880, currently under development, gives guidance on the reuse of software modules designed for use in systems important to safety in nuclear power plants The software modules integrated in a tool should be qualified according to the relevant national and international standards This means that the specification, design, coding, integration and verification of software modules performed in accordance with IEC 880 enables the pre-qualification Thus, in the plant specific licensing procedure these qualifications need not to be repeated but can be called upon as input to the validation and justification of the final system

By the introduction of reusable, qualified software modules, some advancement of the system development life cycle of IEC 880 is possible, because some components of the software are already

existing and need not to be designed and coded again This is however only possible if the system and software architecture can be structured to allow the modules to be used

There are advantages of reusable qualified software modules, because

- Process engineers have a good knowledge of the functional and performance behavior of such modules
- During the qualification procedure, independent and detailed, verification and validation procedures are performed assuring modules of a good quality
- With an increasing number of applications, there are feedbacks of experience from different plants both for safety and non-safety applications

7.3.3. Tool-based engineering by formal specification

The first supplement to IEC 880 also gives guidance to formal specifications and design methods and the corresponding tools The use of formal methods, by enabling various forms of analysis, aids in precise understanding of the system functions especially when supported by understandable graphics, thus contributing to the level of safety assurance

The use of qualified software tools, for the automized code generation based on formal representations, increases the confidence in the software implemented The precise notations, clear semantics and easy understandability supported by graphical representations enable more comprehensive checking to be performed than would be possible with a natural language specification

Appropriate and reliable tools should include the following benefits

- Demonstration of syntactic correctness of the software specification through the use of a suitable tool
- For syntactically correct descriptions, the demonstration of a degree of semantic correctness, e g absence of certain classes of type errors (as described in 7 3 5)
- Verification of code correctness (that is using mathematical proof techniques to show that programs conform to their specifications)
- Assistance of validation by means of animation (this could involve the derivation of prototypes to verify the behavior of the software on the host computer and provide references for the validation of the executable code)

By the introduction of formal methods integrated in an advanced tool (see first supplement to IEC 880) the engineering system life cycle of IEC 880 is again slightly improved Fig 3 shows in comparison the IEC 880 engineering procedure and an advanced tool based engineering procedure with integrated application of reusable pre-qualified software modules The design process (creating structured charts or flow charts) and the coding process (writing compiler statements) are replaced by automatically operating tool-procedures which generate the source code from the formal software specification The source code consists of a library of reusable qualified modules, which are controlled and linked together with lists of parameters and function calls in a sequence derived from the software specification

The use of advanced qualified software tools which are manufactured according to the first supplement to IEC 880, makes it possible to establish an economical and advanced software engineering process for high reliable application software This could enable the exclusion of several types of software faults, and by this way, also could simplify the licensing process

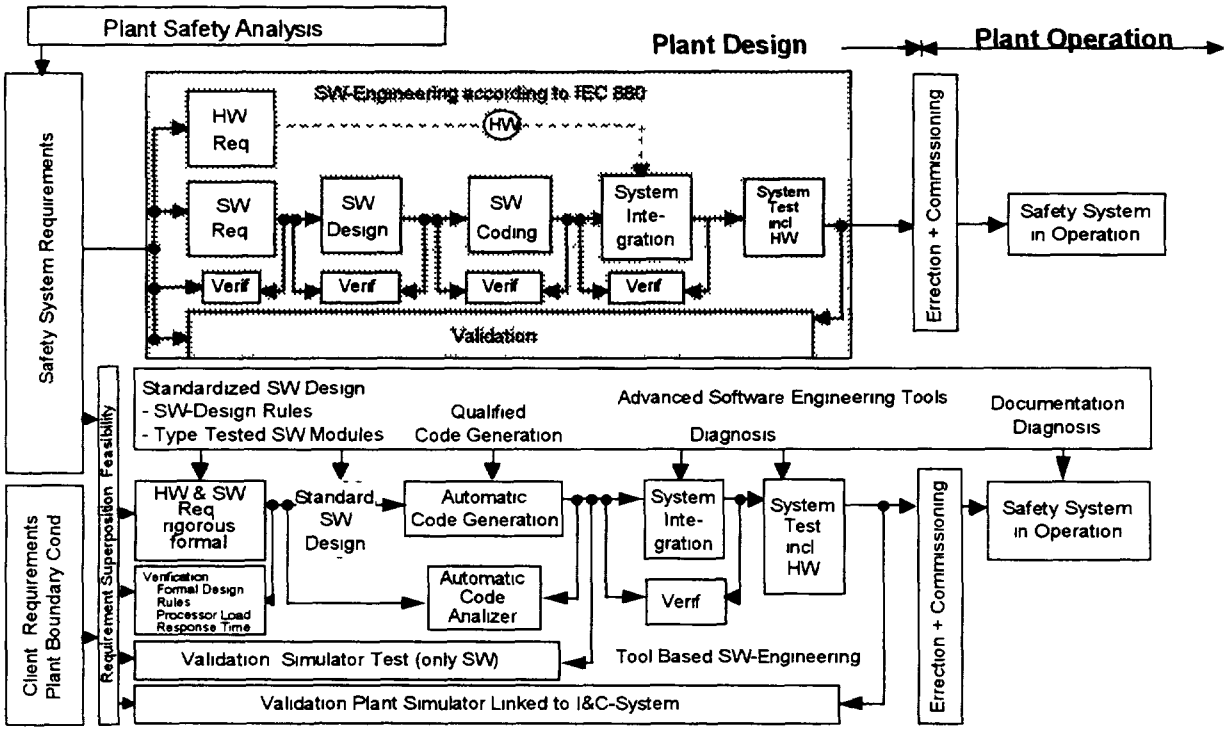


FIG 3. Structure of software engineering process for application software

7.3.4. Advanced software tools requirements

There are a number of features that advanced software engineering tools should have Most will be based on well established structured methods of software engineering To this, many features can be added from aspects of mathematically formal methods for specification and design Other features should include the following

- Provisions of a rigorous formal graphical specification language makes it possible to specify
  - the application functions via functional diagrams,
  - representing pre-qualified reusable software-modules,
  - proven software design rules that are integrated in the tool,
  - the hardware architecture,
  - the assignment of the designed functions to individual processor modules, verification of the specification and the generated code
- Provisions of automatic code generation for (see Fig 4)
  - the application functions,
  - the runtime environment for the application software including all communication functions
- Offer of the possibility for scalable redundancy according to different fault tolerance requirements The generation of the runtime environment software for the main redundancy architectures is performed automatically
- The code generated should be in a standard language, which enables the application of standard compilers to generate the object code for the target systems It can be linked directly to plant simulator codes for transient or disturbance analysis to test how the I&C functions respond to plant behavior
- For management of all design data a relational databank should be used, covering all relevant requirements for
  - the engineering phases,
  - the commissioning phases,

- plant operation,
- future functional upgrades

The experience from the Central Electricity Generating Board in the UK (PODS Project of Diverse Software) in the mid-eighties showed, that just the interface between the process system design and the I&C system design is the weak link, where faults arising in the engineering process have the highest probability
Therefore an advanced engineering tool should cover all engineering phases up to the service during later plant operation and essentially support the interface between process and I&C engineers

- All functions should be represented graphically, preferably by functional diagrams with standardized symbols to be well understandable by process engineers as well by I&C engineers
- The software requirement specification should be formal The functional behavior of the I&C system including response-time tolerances are defined precisely
- Clear relation between input data for each function (type and location of sensors related to process systems) and output data (correlated to actuators) should be represented in accordance with the plant codification concept for signals and functions
- All design data for the backfitted I&C functions should be administrated in a relational data bank, so that each design data is fixed only once but accessible with all relevant technical relations

Fig 3 shows in the shadowed part the original IEC 880 software engineering process for comparison with the tool base Main differences are the integrated and strict formal HW & SW requirement phase, the pre-defined requirements for the SW design, the automatic code generation, and the additional possibility for a functional software validation

7.3.5. Tool-supported verification of I&C specification

The specification of the hardware and software design has to be performed within the rules for a standardized software design As these rules are integrated features of the tool, the designers may not have the possibility to escape with tricky specialities The verification of the I&C-specification phase of the hardware and software requirements is supported by detailed checks The formal design checks should include the consistency check of data types of module inputs and outputs and the consistency of processed and used signals

The automized verification also should include the estimate of the load of all processor units and communication busses, and the resulting response time This feature is a very important advantage of the application of advanced software-tools The standard IEC 880 engineering process enables in comparison rough estimates after the software design and exact measurements during the system integration, which is significant later in the engineering process

A clear software structure as required to be elaborated during the software design phase according to IEC 880 is assured automatically via the grouping of I&C functions to functional diagrams or diagram groups according to single functional tasks, to which the above described software modules are pre-defined sub-tasks Thus the assurance of a clear software structure should be an inherent feature of an automatically generated code by use of an advanced tool

7.3.6. Automated code generation

The next phase in the tool based engineering process is the automatic code generation (Fig 4) In case of the application of a qualified tool, this is a procedural step which is already verified and validated in the design procedure of the tool This also assures the generation of qualified code without coding errors (coding errors in this sense are defined with reference to specification of the software requirements) Additionally, automatic code analyzers for the application code and the code for the runtime environment can be applied, to prove the absence of coding errors

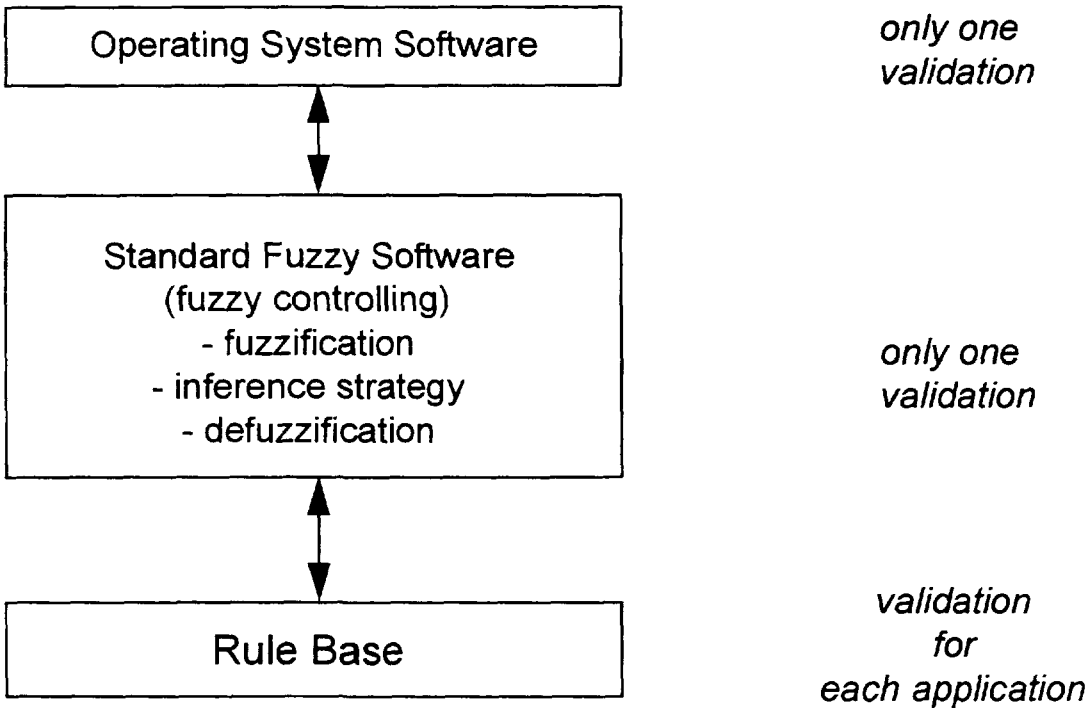


FIG. 4. Software structure for automatic code generation.

7.3.7. Tool based functional validation

The automatically generated code produced is a standard language so that it can be processed by standard PCs and Workstations for which standard compilers are available This feature opens the possibility of an early validation of the functional safety system requirements by means of transient and disturbance analysis on simulators This functional software validation does not replace, but is additional, to the validation of the final system This gives the possibility for an early error correction even after detection of errors in the safety system requirements In this way an advanced tool enables a well documented repetition of all earlier phases in a reduced time

7.3.8. Data integrity

Unintended modifications of verified software components or verified data have to be considered as a serious error source Therefore, provisions should be taken to avoid unintended modifications of verified software and data One or more of the following measures should be taken for high integrity systems

- to store verified data twice on independent memories and compare consistency before use,
- to store verified data together with a checksum (e g CRC check) and verify consistency before use,
- the protection of verified data against modifications by administrative means

The means that assure code integrity have to match with the functional categorization according IEC 1226 e g

- Category A Function Validated on-line code is stored in Flash-EPROMS connected to the redundant processor systems An upgrade is only permitted when the plant is shut down,
- Category B Function Code upgrade may be performed during power operation, if e g by a switch-over possibility between redundant trains or by timely limited operator actions, all functions necessary for plant operation are continuously assured

7.3.9. Document and configuration management

Requirements concerning documents and document management are given in IEC 880, ISO 9000, IEC 1508 etc Experience has shown that discrepancies between the documentation of an I&C system and what is built in the plant, as well as misinterpretations, are caused by various problems Therefore, new approaches in the engineering process should apply the following recommendations

- Software requirement specifications which are derived from the system requirement specifications should be formal, but understandable for process engineers as well as for I&C engineers
- Software code should be generated automatically from the software specification to assure consistency of documentation and implementation
- The system specification should be the reference for all modifications during the lifecycle
- All design data of the whole system-lifecycle, e g
  - structure and location of hardware,
  - input data, their functional processing and output data,
  - parameters,
  - allocation of functions to the hardware,

  should be stored in a relational data bank To achieve unambiguity, each data should be stored once in a strictly controlled data form The presentation and use of same data in multiple correlation should be possible

7 4 SOFTWARE REQUIREMENTS FOR I&C SYSTEMS

The software requirements specify the overall behavior of the I&C-systems relevant to plant control and safety The main source for the software requirements are the results of the process safety analysis, which leads to the specification of safety relevant functions

Experience towards the documentation of I&C systems for NPPs with 20 or more years of operation is that the documentation shows how the I&C systems are realized by solid state or relay technique but the software requirements and the related reasoning are not documented Thus, generally a re-engineering of the functional requirements is necessary to get the basis for the backfitting with computerized I&C systems Additionally, whether the existing functionality should be kept or upgraded, is an important point to be decided by the utility in consultation with the licensing authorities Also the possibility for a stepwise procedure should be considered, e g first changing the I&C technology by keeping functionality and later upgrading the functionality by a software exchange This described software requirements specify all safety relevant features of the safety system and form the basis for the next engineering steps

7 5 I&C SYSTEM DESIGN

The I&C system must be designed to realize safety relevant functions based on the categorization of these functions according to IEC 1226 The I&C system design forms the basis for the final system quality and correctness including hardware and software Fig 5 gives a general overview of fault and defect handling to achieve a strategy for I&C system design

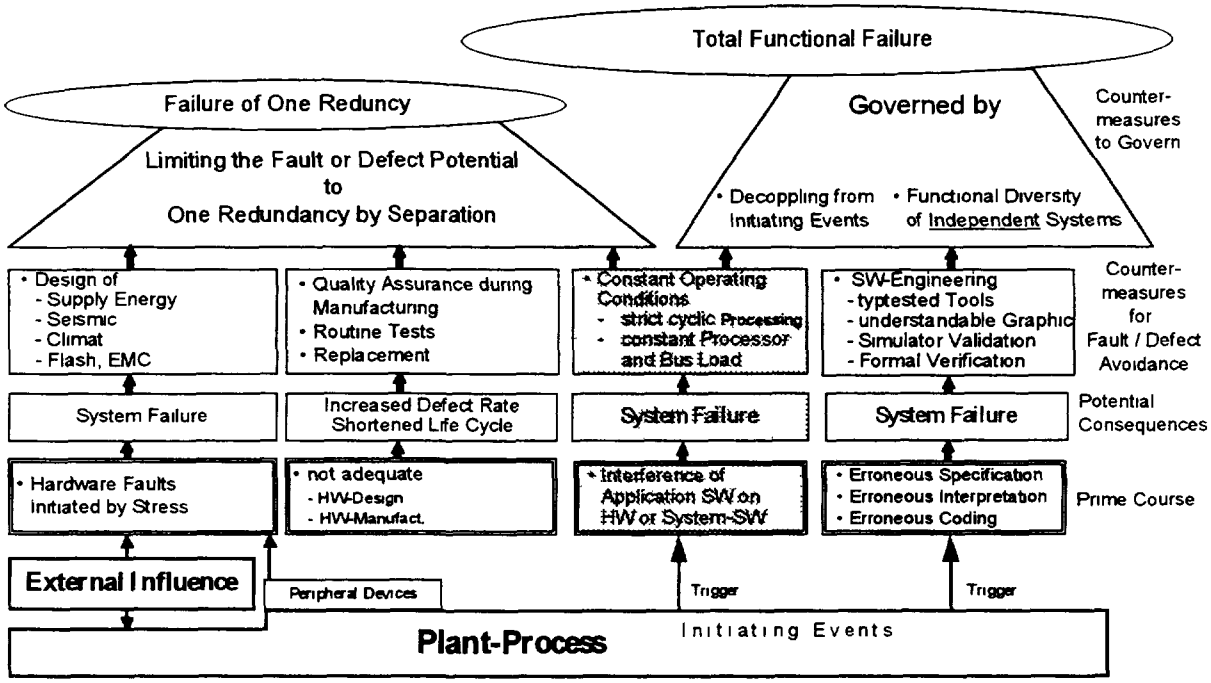


FIG. 5. Overview of fault and defect handling for safety relevant digital I&C systems. Different fault and defect modes are grouped according to four main types of prime course.

7.5.1. Effects of external events

External events such as seismic or lightning can generally initiate global consequences and also initiate postulated events. The design strategy against this stressing effects is the same for digital as for hardwired I&C systems by either to withstand the stress with all components (e.g. seismic) or to reduce the consequences by redundant structure and separation of the trains to the extend of a single failure This requirement leads to:

- spatial separation of redundant trains and allocation to each train,
- separate equipment for environmental conditions and (temperature, humidity, pressure)
  - separate power supply
  - electric isolation between the trains and to other systems, to protection against lightning,
- design against specified seismic stress;
- design against EMI (electromagnetic interference) and RFI (radio frequency interference),
- design of adequate grounding.

The justification to exclude that internal or external hazards cause common initiating events on redundant I&C trains has to be documented and proven for relevant plant operating situations (e. g power operation, maintenance and repair activities, refuelling). If safety relevant I&C systems with a seismic qualification are arranged in close proximity with equipment without seismic design, it has to be proven that no interference is possible in case of an earth quake

7.5.2. Aging and wear

The effects of aging and wear of the installed hardware will lead to an increased failure rate On the basis of qualified I&C systems with factory tests for all modules fatal defects just when the system

is installed are not to be expected But a poorly designed or manufactured hardware may lead to an increased failure rate not after about 20 years as expected but already after 5 or 10 years of operation The countermeasures to handle these failure types are quality assurance during the manufacturing and repetitive/routine tests for early detection and replacement Furthermore the design of a redundant structure assures that this defect type can course only single failures Design strategy and failure government against this failure type is the same for digital and hardwired I&C systems

7.5.3. Errors and faults

7.5.3.1 Software common mode failure

Design faults are caused by an erroneous safety system specification or a misinterpretation between process and I&C engineers or erroneous coding These are typically discussed as software faults with the potential to cause a common mode failure of the I&C system in case of a demand or even triggered by a random signal trajectory This is illustrated on the right side of Fig 5 where the design faults are grouped

To reduce the probability of software common mode failure as far as possible, the application of an advanced software tool for design specification, code generation, software verification and documentation management is essential

Starting the consideration on software fault types from the status that the software for all tasks in parallel is running on the distributed processor system, the only possible initiating events that cause a system failure by hidden software faults, originating from the engineering process, are the input signal trajectories given by the plant process Of course for a large and complex I&C system, it is impossible, that all possible signal trajectories can be covered by statistical tests in advance

7.5.3.2. Faults due to errors in the process system requirements

To reduce the probability for this fault type the I&C system specification, based on the process system requirements must be understood by the I&C and the process system engineers as interface documentation This fault type is not specific to the means of realization of the I&C functions whether it is hardwired or computer-based

By the application of a formal tool-based specification with automated code generation (see chapter 7 3) the potential for early fault detection by coupled simulator tests is increased When comparing hardwired and computer-based realizations, this forms an important possibility for fault reduction for processor-based systems

In spite of this improvement a remaining fault of this type cannot be excluded The requirement of functional diversity is the effective countermeasure to this fault type Functional diversity means generally that two protective functions based on physically diverse parameters and algorithms can act independently via independent I&C systems (independent power supply and without direct bus interconnections) on independent final elements, to meet a protection goal

7.5.3.3. Faults due to errors in the I&C specification

This fault type leads to the same consequences and requirements as that from an erroneous specification The only difference is, that this fault type originates from a unrevealed misunderstanding between process and I&C engineers The effective countermeasure again is the application of functional diversity

7 5 3.4. Faults due to errors in coding

Main strategy is to avoid error prone coding methods, although these methods have a broad application for standard programming This include

- avoidance of event dependent program flow, no event management by internal or external interrupts,
- no variation of program roots, depending on different data combinations,
- avoidance of a real time clock and avoidance of time dependent decisions,
- avoid as far as possible the use of long term stores,
- avoidance of a complex stack management

The application of a tool based automatic code generator should assure the absence of error prone coding and with an increasing amount of generated applications, the confidence in this procedure is increased Just opposite to this a human programmer with increasing experience may move towards more intricate and consequently less transparent coding principles

The goal of the above coding restriction is to assure that the processor system with the integrated software behaves as a deterministic logic machine The code should be processed cyclically without any feedback from the process which is controlled The way to realize these restrictions without the possibility for interference by programmers is the application of the tool based automatic code generation The application code should be composed of reusable software modules which each has a clear defined task and is small enough to be tested completely in a pre-qualificd procedure The avoidance of long term storage including a real time clock reduces the complexity of possible data combinations and thus increases the effectiveness of tests

7.5.4. Software-hardware interference

In Fig 5 the representation of this fault type is shadowed to point out that this fault type, known for digital I&C systems, has no equivalence for hardwired systems

When the software is running on the processor system, there are only signal trajectories that can trigger can an existing but known fault to cause a system failure

For category A safety systems, in addition to the cyclic processing of the application code , the avoidance of process dependent interrupts is necessary to achieve the decoupling of the I&C systems operating behaviour from possibly initiating events of the plant Standard digital automation systems apply generally interrupt techniques to achieve acceptable response times

As a further important cause for a possible interference from the application software on the processor system one has to be assured that no unpermitted data operations can be initiated The countermeasure is the strict application of encapsulated software modules with consequent inside permittence checks

For the processing of safety relevant control tasks, only a subset of functions of a standard operating system are necessary (about a tenth of a standard operating system kernel,communication function, hardware organization and interrupt handling due to hardware or software failures) It is preferable to apply such a reduced operating system (subset of a proven operating system) so that it is possible to perform type tests by theoretical checks Alternatively, it is possible to use a proven operating system with an extensive application basis for category B or C applications

To avoid software-hardware interference strict design according to the recommended rules leads to results acceptable for safety responsible applications, whereas by the application of redundancy or diversity this fault type cannot be managed

7 6 SYSTEM INTEGRATION REQUIREMENTS

The system integration according to IEC 880 chapter 6 consists of

- software-hardware integration
- verification of the system behavior by tests

System integration is performed application specificly However, integration can be simplified and the quality can be increased by assembling the whole system of pre-qualified hardware and software modules according to a set of rules describing how to combine these modules

The hardware integration shall be documented in a formalized hardware specification including the

- identification of each individual hardware module with state of revision, parameters, switches etc ,
- interconnection of the hardware modules,
- arrangement of hardware modules in racks, cabinets, rooms, etc

The manufacturing and assembling of hardware shall be based on proven manufacturing and construction rules

The software-hardware integration contains the assembling of the software modules by a linkage processor and loading of the software into the hardware This work should be based on tools which

- assure that proper revision levels are linked together,
- document the result of linkage for verification and maintenance purpose,
- verify proper loading

The correct system behavior shall be demonstrated by system tests The system test shall verify that

- software is capable of operating in the required hardware environment,
- functional requirements are met,
- independence requirements between different I&C functions are met,
- load behavior is met,
- maintainability requirements are met,
- response time behavior is met

A test harness should be provided to generate test data and to document the system response behavior For I&C systems of highest safety level, tests with realistic response behavior of the plant should be included The system test should include tests to demonstrate that the system is able to cope with anticipated faults on the inputs e g sensor out of range In parallel with the system test, the documentation relating to operability, maintainability, self-checking capability and routine tests should be verified

7 7 VALIDATION

7.7.1. Validation process

The validation has to prove that the behavior of the total I&C system consisting of the distributed hardware (processors with bus links and input/output modules) together with the integrated software (application software, operating system and runtime environment) fulfills the original safety requirements The main criteria for this validation are

- long term stable operation of the system,

- correct fulfillment of the functional requirements related to the design basis accidents,
- the resultant response time

The tests to be performed in the validation phase, have to be designed in advance and the results should be documented The application of a validated simulator for the plant process linked to the original I&C system supports the validation and creates a real confidence base for the designed I&C system But this requires real-time behavior of the simulator as a precondition, which usually forms a difficult barrier

The use of an advanced tool based engineering process opens the following new validation possibilities

- The relation of processor and bus performance with respect to the allocated functional tasks can be checked at the end of the design phase, as hardware and software design are integrated
- As the software design is standardized and the coding is performed using a standard language automatically, it is possible to perform early checks of the designed functions against a process simulation code This early confirmation of the designed functionality helps to avoid a late cost-effective redesign
- The final validation has then mainly to focus on the confirmation of the correct allocation of input and output modules with their functional processing

7.7.2. Validation of system requirements specifications

By the application of a simulator for the plant process including I&C systems, experience has shown that most deficiencies of I&C systems result from erroneous, ambiguous or incomplete system requirements specifications For this reason the validation of system requirements specifications shall be included in the V&V plan Application of simulator based functional software validation seems to be an adequate mean to exclude the relevant error types according to present experience

7.7.3. Requirements on process models used for validation

The modeling should be graphically driven to provide for easy understanding of the simulation models by the process and I&C engineers The use of standardized component models should be applied as far as possible All the model data and model component connections shall be stored in the model database Specific component models, if necessary, shall be extensively verified and validated in compliance with the principles generally adopted for nuclear plant analyzer codes The code should also be capable of calculating the proceeding of postulated malfunctions or accidents in the process The plant simulation model of the nuclear steam supply system and as far as necessary of the balance of plant systems should allow a reasonable time resolution adaptable to the processing conditions of the digital control system on an affordable workstation computer An example of such verified modular code is the Advanced Process Simulation Software (APROS) [8 74]

7.7.4. Factory acceptance tests

Before delivery to plant site, the factory acceptance test is generally performed with participation of utility and the licensing authority with independent expert The factory acceptance test has to prove that the I&C system meets the designed requirements, except those which can only be demonstrated in connection to existing plant systems If by these restrictions key functions of the I&C system are not testable, it should be considered to include original components of related systems in the factory acceptance test

7 8 SYSTEM INSTALLATION, COMMISSIONING AND IN-SERVICE TESTS

7.8.1. Commissioning and installation

Commissioning and installation depend necessarily on the nature of the system to be installed as well as on its physical arrangement in the plant However, commissioning and installation shall follow proper procedures which are in line with the overall QA-program Installation shall be performed by experienced specialists

After installation the on-site acceptance tests shall be carried out for final validation of the I&C system behaviour in normal operation, anticipated operational occurrences and as well accident conditions Generally, complete tests are impossible to be performed due to restrictions by plant conditions

7.8.2. Final acceptance tests

The final acceptance tests have to demonstrate the correct behavior of the integrated I&C system with plant The type of tests should be agreed upon between utility, supplier and licensing authorities Depending on the I&C upgrade also the repetition of original plant commissioning tests may be necessary For safety I&C systems the first performance of the routine tests is necessary as part of the acceptance tests

7.8.3. Routine tests

Routine tests shall be performed to demonstrate that the system is not degrading Routine testing shall be automated as much as possible to minimize the need for manual tests The test should overlap such that the whole chain from sensor to actuator is subject to testing This may require final actuators to be checked as part of the shut down procedure

7.8.4. Modification and maintenance

A formal modification procedure shall be established including verification and validation Reasons for modifications may be

- an anomaly report,
- a functional requirement change after delivery,
- technical evaluation

Generally, modifications should be performed using the same tools and the same engineering phases as applied during system design

8. FUTURE TRENDS

The application of new technology is accelerating in many industries This is mainly driven by advances in computer technology offering reasonable HW/SW solutions that can replace old analog systems The nuclear industry is conservative compared to other industries, which means that one must also look for applications in fossil power generation and chemical plants to learn how the deployment of new technology is progressing One advantage of being conservative is that the nuclear industry can avoid pitfalls and mistakes made by other industries and benefit from their successful experiences with advanced technology Careful analysis of the adaptation of new technology to nuclear applications must be made to fulfill specific nuclear requirements and safety standards

Nevertheless, there are several examples of the application of advanced technology in the nuclear industry which are described in the following sections The examples are partly taken from prototypes of future advanced plant designs and partly from planned or on-going retrofitting programs in existing nuclear power plants

Plant control is exercised by automatic control systems and actions taken by the operating staff, some actions are also performed by maintenance staff Advances are being made to improve control algorithms, information processing, man-machine interface and tools to support equipment testing and the duties of the maintenance staff The development trends in the various fields will be identified and full details can be found in the comprehensive list of references

8 1 ADVANCED SIGNAL PROCESSING TECHNIQUES

Redundant voting structures are used in order to achieve the required high reliability and to avoid the adverse impact of single failures for vital systems in nuclear power plants Hence important plant signals are measured by several (redundant) sensors The multiple signals can be subject to consistency checks to ensure that the correct signal is fed to the automatic system and to the HMI providing a basis for operator actions The extensive use of CRT is for visualizing complex situations, which are sometimes displaying as many as 300 sensor signals, makes signal validation even more important for information purposes A difficulty of resolving signal validation problems only by redundancy, is the possibly wrong interpretation when faced with deviations of redundant signals Therefore methods have to be provided to identify the faulty signal(s) Another problem arises if insufficient redundancy is available or if several signals deviate from the true value at approximately the same time In order to provide an early diagnosis in these cases and to identify the faulty signal, additional redundancy can be generated by means of a mathematical description of the process This is called analytical redundancy method This has been demonstrated by a number of organizations using a range of complexity of models from simple analytic and logic models through to fuzzy logic models

One example of such a system is LYDIA [8 1,8 2], a system for early sensor and process fault detection and diagnosis The system has three layers of signal handling, the analysis/alarm layer, the diagnosis layer and the fuzzy layer acting as an interface This system is described to demonstrate how different algorithms can be combined in order to achieve a practical application

The *analysis/alarm layer* consists of three fault recognition modules, which act independently and execute in parallel Redundant measurements are analyzed as follows There is the Hardware redundant Fault Detection and Isolation (HFDI) module which uses a parity-space procedure The second validation is by the NFDI (Non-temporal analytical redundancy Fault Detection and Isolation) module In this case the value to be compared with the actual measurement is calculated from other physical values available from measurements (e g using the correlation between pressure and temperature in closed systems) The IFDI (Instrumentation Fault Detection and Isolation) module makes use of process knowledge provided by simulation models which are linearized around the actual working level to make them simple and fast enough for real time conditions Since the models use actual measurements as input, it is necessary to check these measurements for their correctness This is done by means of a parameter estimation procedure which stops further calculations if faulty import signals should appear

The output signals of the models are monitored by *Software Detectors* using different algorithms including Kalman filtering, generalized likelihood ratio, etc Four different *Software Detectors* are applied to complete the following tasks

- checking the correctness of the input signals,
- checking for an abrupt sensor failure,
- checking for "slow" drifting of the signal,
- checking for simultaneously appearing faults

The task of the *Diagnostic Layer* is to allow an exact diagnosis of the fault origin The alarm levels delivered from the analysis/alarm layer, have to be properly combined This is done by a selection of the three module outputs according to a distinct fault type or a distinct component, which are then combined to a fault pattern The diagnosis is completed on the basis of a classification of the pattern Because of the learning ability and the tolerance for input errors, neural networks are used as a classification tool [8 3-8 6]

8 2 ADVANCED CONTROL ALGORITHMS

The reduced cost of computers and advances in the development of control techniques enables the implementation of more advanced control algorithms, which can be used to optimize plant performance, for example, sub-systems can be optimized using multivariable optimal control techniques Advanced methods such as genetic algorithms, predictive control algorithms, etc will be applied in the future [8 7, 8 8]

8.2.1. Hierarchical control systems

Current control systems are arranged such that each subsystem is controlled on an individual basis A global optimization may be obtained by enhancement of hierarchical distributed control algorithms which exchange parameters in a network, so integrating the behaviour of the control loops

Fig 6 shows an example of a hierarchical supervisory control architecture [8 9, 8 10] The supervisory controllers form a network of distributed expert systems which is interfaced with a real-time simulation of the plant, the plant's automatic controllers, and the human operator The primary goal of the supervisory controllers is to maintain plant operation within safety envelopes while optimizing availability, and minimizing stress to components and operators *Fault detection* and *diagnosis* are embedded into the control philosophy so that if a failure occurs, the control system changes over to another regime and isolates the failed component or system

The philosophy of operation for each supervisory module is the same Child nodes are viewed as processes to be controlled according to goals specified by the parent node, to which it reports when the goals are achieved The supervisory modules contain sets of rules that interact with the plant simulator, operator, and automatic controllers and demonstrate the benefits of supervisory control for multimodular systems Because their rules have access to all data, the supervisory controllers can monitor the performance of the plant and controllers, and modify operational goals and control laws when necessary

Every supervisory module allows operator interaction through human-machine interfaces The operator is informed of actions being taken by the supervisory module The supervisory modules regard the operator control actions as a "manual" optional control generator constrained just like the automatic controllers to act within operational and safety envelopes set by the parent supervisor

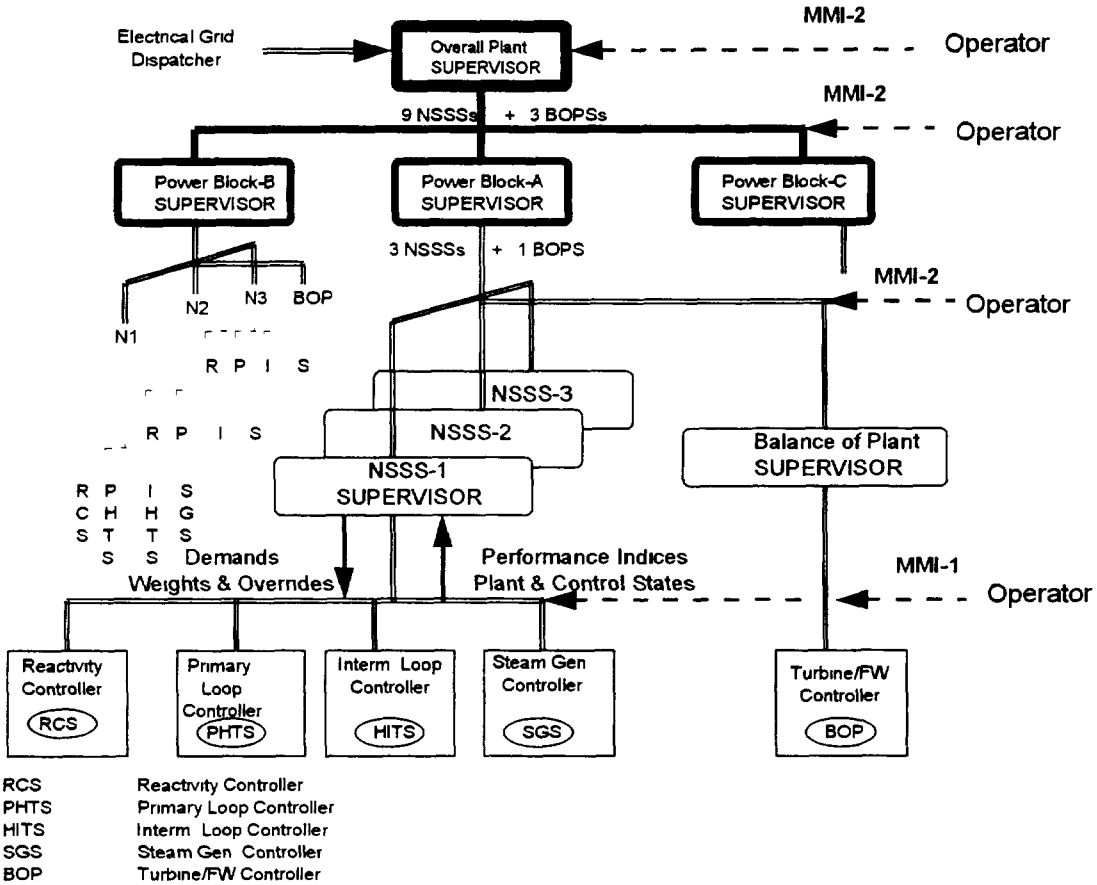


FIG. 6 Hierarchical supervisory control architecture.

This is one example of a hierarchical distributed control system where more knowledge is built into the algorithms Whether future systems will contain all the functions mentioned remains to be seen, but several features described here can be recognized in modern control systems

8.2.2. Optimal core control

Model based control systems are emerging The reactor control model contains a xenon model which is used to minimize the change of boron content in the coolant Applications using more comprehensive models will be a natural evolution for many modern control systems in the future Core control optimization can be made with constraints on local power density, limits on axial offset, maximum dilution and boration rates etc The obtained controller sequence is optimal in the sense that a given objective function is minimized subject to the constraints considered

Several methods exist for predictive optimal core control many of which were developed at a time when the expectations of the nuclear growth were high and the need for load-cycling was foreseen Another motivation for improved reactor control is that large reactor cores may be unstable with respect to xenon oscillations The main drawbacks with the method based on the Multistage Mathematical Programming (MMP) [8 11], were that the use of linear models were too simple and the centralized solution methodology was too computer demanding

However, newer methods apply hierarchical decentralized optimization techniques [8 12] Thus instead of solving a large centralized mathematical problem, several sub-problems are solved interactively using co-ordination parameters to ensure an optimal global solution Non-linear models are applied The new methods are less computer demanding and will be easier to implement in the future

8 3 FUZZY CONTROL AND NEURAL NETWORK APPLICATIONS

The essential advantage of the Fuzzy Logic (FL) approach is that it is based on *knowledge engineering* techniques and is thus suitable for all those high sophisticated technical control systems which can not be modeled mathematically FL uses knowledge in a linguistic, approximate way that leads to easier development and maintenance The use of adaptive membership functions facilitates an efficient use of FL in non-linear processes

Fuzzy control has been demonstrated in many prototype applications and has the potential to provide robustness to control systems Although Fuzzy Logic theory was introduced 30 years ago (Lotfi A Zadeh, 1965) [8 21], its usefulness in industrial applications has been recognized only in the last 10 years, with an increasing number of real implementations around the world, including the nuclear field

Neural Networks have mainly been demonstrated for signal validation applications and there is a number of successful examples in the field The key issue in future is to make this technology available for non-experts to avoid the same problems that have been experienced in some of the noise analysis systems, where a lot of effort may be needed for data interpretation

Artificial Neural Networks (ANN) became very popular in the technical world after Rumelhart and Hinton derived the easy way to implement Back propagation algorithm for ANN learning [8 13] The main characteristic of ANN are their powerful ability to learn and generalize from examples when a physical model of the process is not completely known

The interest of the technical community in these two emerging technologies is such that it is valuable to summarize the current status of research and applications in the nuclear field and indicate where FL and ANN are heading

8.3.1. Fuzzy logic and nuclear applications

The natural field of application for Fuzzy Logic is fuzzy controllers, but in the last four years an increasing number of fuzzy oriented methods have also been suggested in other fields. like Decision Support Systems, Pattern Recognition and Fuzzy Database

Fuzzy controllers are mostly successful where highly non-linear processes make it difficult to optimize and tune conventional PID controllers This is demonstrated in work by KAERI (Korea) when developing a self-tuning water level controller for a PWR [8 14, 8 15], and the feedwater controller developed by PNC (Japan) for the Fugen Advanced Thermal Reactor [8 16]

Power control of nuclear reactors is another area of investigation, because the power depends on many unmeasurable parameters, such as burnup, xenon-dynamics, and thermohydraulics, which affect reactivity with different time constants Fuzzy logic controllers in this context are seen as one candidate method to implement the qualitative reasoning currently applied by trained operators in both BWRs and PWRs for power control [8 17] An application of this technique in a Belgian research reactor is described in [8 18]

Early fault detection and state identification by fuzzy logic is another topic that has been studied over the last three years by many organizations worldwide A number of papers have been presented in nuclear technology conferences such as SMORN (Avignon, June 1995), ANS meetings (Philadelphia, June 1995 and Philadelphia, June 1996), FLINS (Mol, Belgium, Sept 1994) and IAEA specialist meetings (Halden, Norway, September 1994)

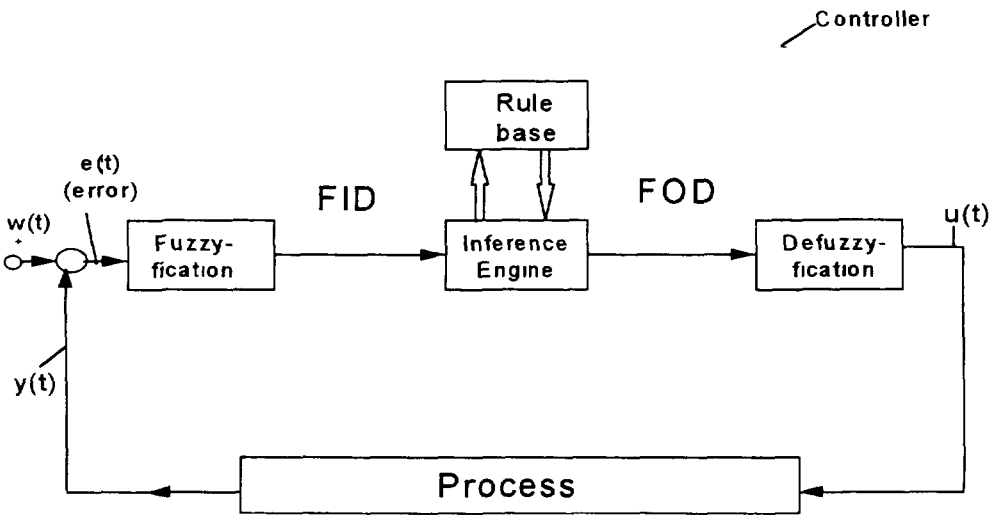
Decision Support Systems combine quite well with the fuzzy logic ability to perform a functional mapping from approximate rules, defined by human experts, and quantitative information, handled by computers Examples of such applications can be found in [8 19] and [8 20]

A safety critical application of fuzzy control is discussed in reference [8 21] This research focus on changing from conventional programming to knowledge based techniques This provides a more transparent description of system behavior and facilitates controller adaptations by modification of the knowledge base Scientific research and industrial experience have shown that a fuzzy controller can be applied to vital process control because of its inner structure, which is more transparent and based on *knowledge engineering* Fundamentally, there is a real chance for successful verification and validation procedures of the rule base in comparison to a conventional PID-controller which is based on differential equations with partwise constant coefficients

8.3.2. Functionality of fuzzy controllers

The inner structure of a fuzzy controller is shown in Fig 7 as a block diagram Analog *(Crisp)* input values are fed to the *fuzzyfication* module, which converts input values into fuzzy values corresponding to well-defined *membership functions* These fuzzy values are then fed to an *inference engine*, in which several inference strategies may be implemented for decision making The inference engine cooperates with the rule base and checks which rules may fire The inference engine generates a certain fuzzy result which is fed to an action module for *defuzzyfication*, because an actuator needs a certain crisp value for process control Within the defuzzyfication module different algorithms like *Maximum -Height-Algorithm, Mean-of-Maxima-Algorithm* or *Center-of-Gravity-Algorithm* should be implemented

An essential module of a fuzzy controller is the rule base comprising a certain number of rules To date it has been found that the number of rules necessary to control a technical process is limited to a certain upper boundary For example about 85 rules are sufficient to control the temperature and steam pressure of a conventional reactor Because the content of the rule base is a certain modeling of technical process and consists of certain simple rules like



Legend

variable		*type of variable*
w(t)	desired value	analogue value (sharp or "crisp" value)
e(t)	w(t)-y(t) error	analogue value
u(t)	control signal	analogue value
y(t)	measured value	analogue value
FID	Fuzzyfied input data	fuzzy value
FOD	Fuzzy output data	fuzzy value

FIG 7 Fuzzy controller, block diagram as a part of a control loop

IF Error is P_Small and Var_Error is zero THEN Power is P_Small, ELSE
IF Error is Zero and Var_Error is Zero THEN Power is Zero ,

There is a fundamental advantage in modeling the technical process by such a rule base

- The content of the rule base can be validated by an expert such as an experienced operator, who has a lot of technical knowledge of the process he is responsible for, but no deeper knowledge on computer science
- The real-time behaviour can be judged better than for conventional PID controllers This is because the real-time behaviour may be *tuned* [8 22] by the modification of
  - content of the rule base by editing certain rules,
  - certain membership functions,
  - certain scaling factors during the fuzzification process,
  - the inference algorithms

8.3.3. Safety features of fuzzy control

In safety techniques there exist certain fundamental principles like *dynamization principle* i e applying periodic control signals to reach a safe system state in case of any failure, *monitoring function, watchdog function,* and *quiescent current principle* i e to hold any control device at higher energy level than necessary for operation [8 23] The implementation of these fundamental principles into the inner structure of a fuzzy controller should be done [8 24]

The implementation of a fuzzy controller comprises hardware as well as software so the fuzzy software remains to be validated Fig 8 shows the necessary software structure comprising *Operating System Software*, a so-called *Standard Fuzzy Software* [8 25], and a *Rule Base* Operating System Software as well as Standard Fuzzy Software used to be validated only once, whereas the content of the rule base has to be validated for every new application Thus, the fuzzy technique assists the necessary verification and validation processes

The structure of a fuzzy technique may lead to successful verification and validation and to provide a better real-time behaviour of such a knowledge based system Because, some theoretical knowledge for stability proof is available there would exist a real chance to extend the scope of application of fuzzy controllers to NPPs

Deeper knowledge on stability of fuzzy controllers is being developed and is gradually becoming available This should be applied due to the state-of-the-art [8 26]

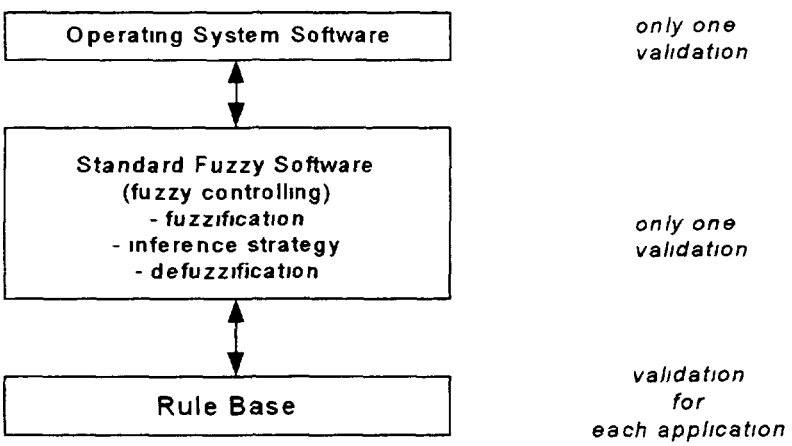


FIG 8 Software structure for fuzzy control

8.3.4. Neural networks

The number of artificial neural network applications for state identification, fault detection and data validation has grown over the last five years, as a number of development tools has become available The great popularity of ANN applications is because of their ability to approximate non-linear functions to any degree, learning by examples Since knowledge of the physical model is not needed, this approach is recommended whenever a large amount of experimental data is available but the physical behavior of the process is not well understood or is too difficult to treat with ordinary differential equations Another advantage is that they can adapt their behavior to accommodate changes in model parameters, so that an ANN is a natural choice for non-stationary processes

Extensive work has been completed by a number of organizations and prototypes exist in some research reactors The prototypes include the work done at Tractebel [8 27] which is to be tested in a Belgian PWR and at Korea Advanced Institute of Science and Technology [8 28], where ANN techniques have been used to detect and classify anomalies in nuclear power plants

Loose parts monitoring [8 29, 8 30], in PWRs and BWRs by means of acoustic signal bursts associated with metallic impacts of loose parts has proven to be a powerful method for assessing, on-line, the mechanical integrity of components in the primary circuit In order to process the relevant burst data and to prevent unnecessary or false alarms a classification and trending of acoustic signatures is needed Therefore the analysis of signatures has to be automated in order to avoid time consuming manual procedures Known and minor relevant signatures can be classified accordingly and will not be considered for further alarm handling This requires that the patterns must be investigated before determining their real meaning At the same time the monitoring system still has to remain sensitive to all incoming acoustic events of unknown origin

In order to achieve automatic classification the burst signals of 40 ms period are captured and digitized with 100 kHz by a transient recorder They are then fed to a PC for further signal processing, especially the exact determination of the burst arrival time using the Page-Hinkley algorithm For burst type classification the signal is sent to a multi-layer perception neural network with one input layer, two hidden layers and one output layer

The interpretation of the results provided by the neural network has been performed by a neural network based classification and trending software module (NNLT)[8 31] The module delivers an on-line trending and display of the classification results Up to now the classification method has been successfully demonstrated by laboratory and on-site tests In the laboratory the 16 tape stored signals of a loose parts monitoring system have been fed into the system The capacity of the alarms (up to 30 per day) were known to be caused by mechanical contacts of vibrating components and by flow noise burst signatures As a result of the tests with the trained neural network, 97 % of the patterns were classified correctly Further, promising results have been achieved in a 6 weeks test of the pilot system installed in a PWR plant During that time the 32 alarm patterns analyzed by the system have been classified correctly Presently the NNLT module is used for enhancing the laboratory analyses of burst events Further work is focused on a module which can be reliably used on-site

ECN (Holland) has developed a combined expert system - ANN model for real time plant monitoring, that has been installed and tested at Borssele Nuclear Power plant [8 32] Other theoretical studies have been performed recently to demonstrate that a significant improvement in fault diagnosis capability can be reached by using an ANN technique [8 33-8 35]

Data validation is another field where ANN have been studied with very encouraging results R E Uhrig (ORNL), E Bartlett (Univ of Tennessee) and B R Upadhyaya (Iowa State Univ) have pioneered this research since 1990 [8 36, 8 37] Recent advances can be found in work at KINS [8 38] and the Halden Reactor Project [8 39]

8.3.5. Future trends in artificial neural network and fuzzy logic

Until two years ago, the scientific community were working on the FL and ANN topics separately More recently one has recognized that the two methodologies can be considered complementary Completely new approaches where the advantages of combining both methods are now emerging

There are many ways to combine FL and ANN The goal of this approach is to attempt to maintain the linguistic property and rule-based approach that FL has and to take advantage of the learning and generalization capability that ANN exploits Examples are fuzzy systems with membership functions generated by an ANN, fuzzy systems with rules generated by example, adaptive fuzzy systems where some parameters are changed adaptively by an ANN

Much work on neuro-fuzzy applications has been presented over the last two years, and it is predicted that this is the direction which artificial intelligence research will take in the next decade The *results achieved in Japan, [8 40, 8 41], and other organizations in Germany, France and Poland* [8 42-8 44] are particularly impressive From this work, it can be argued that neuro-fuzzy systems are capable of using prior knowledge in the form of fuzzy rules, adapting it to the actual situation reflected in the data, and creating new fuzzy rules from the data They are an excellent tool for knowledge acquisition A referenced paper [8 45] summarizes the future perspective of this new emerging technique

8 4 ADVANCED SYSTEMS FOR MAINTENANCE SUPPORT

In the future, various kinds of expert systems will appear to assist plant staff in equipment diagnostics and early fault detection Two fundamental techniques may be applied

- *Backward chaining:* Based on a certain sequence of alarms an algorithm is triggered in order to find out which component failed This goal can be reached relatively easy for diagnostic purposes
- *Forward chaining:* Based on a certain sequence of alarms an algorithm is triggered to derive a prognosis in order to describe what will happen next But this method is much more sophisticated

There are several factors influencing this development trend, the essential ones are

(a) An early indication of component failures is important for plant safety and availability If a problem can be identified and diagnosed before the ultimate breakdown of a critical component, it will leave sufficient time for the plant operators to take the necessary preventive actions
(b) The operation philosophy can gradually change to condition based maintenance as the maintenance staff obtain more detailed information about the performance and state of critical components, so one can make prioritized replacement schedules
(c) The components of advanced control systems tend to become more complex and the expert knowledge necessary for system diagnosis will be difficult to maintain for all plant systems by plant staff Consequently, expert systems possessing domain knowledge will play an increasingly important role in the future
(d) The systems in this category are not important to safety, which means that expert systems for equipment diagnosis can be introduced without licensing requirements
(e) A number of expert system tools are available which facilitate knowledge capture, encapsulation and maintenance which do not require extensive training to handle

One example of an implementation of such a system is an intelligent chemistry and corrosion monitoring system [8 46] Control and reduction of the transport of feedwater corrosion products into steam generators will reduce material and thermal performance degradation, and increase the life of steam generators The new system uses on-line plant data to detect and diagnose chemistry excursions, and corrosion models to estimate the rate of crud generation and transport into the steam generators

Noise analysis techniques have been applied with success in several places, as reported in several SMORN conferences Typical areas of application are vibration monitoring of key plant components like turbines, main circulation pumps, generators, etc In the future the systems based on these techniques should be developed towards improved user-friendliness

8.4.1. Computer aided maintenance

In order to assist maintenance personnel staff an Object Oriented Database System has been developed [8 47] It contains at least two kinds of information

(1) Static information about every device including

- vendor,
- date of first installation,
- part number (ID),
- part list of the device,
- last maintenance service,
- name of service technician,
- who did the last maintenance service,
- list of failures in the past,
- list of neighboring devices (some kind of chained list),
- location of the device (e g room number),
- necessary keys to enter the room,
- number of spare parts available.
- where to get the spare parts, etc

(2) Graphical information about the device like

- block diagram,
- functional description,
- logic diagram,
- technical data,
- technical drawing of the device (e g derived from CAD),
- scanned photo of the device to be held in the database (e g as a bitmap file)

8.4.2. Plant maintenance optimization

Efficient maintenance is important to reduce costs, enhance safety and improve performance of process plants A key to continuous improvement is to exploit the information hidden in historical operation and maintenance data The main aim is to optimize maintenance tasks through the utilization of process models and plant measurements Real-time systems are being developed for Model-based Condition Monitoring (MOCOM), living Reliability Centered Maintenance (RCM) analysis based on Life Cycle Cost (LCC) models, and Computerized OPeration MAnuals (COPMA) system on industrial maintenance tasks

MOCOM systems calculate real values from process measurements whereas fault-free values are obtained from measurements and process models They may exchange data with relational database management systems and may be linked to conventional maintenance systems In the case where there is a considerable difference between the derived real and fault-free values the system can automatically generate work orders for the maintenance staff Such a system is currently being tested against plant data from one of the test loops at the Halden Reactor [8 48]

A maintenance program is established by selecting a maintenance strategy for process equipment The three main strategies are *corrective maintenance, time-based preventive maintenance* and

preventive maintenance, based on inspection and/or condition monitoring The strategy may be decided based on a criticality study of the plant components and systems Reliability Centered Maintenance is a technique to establish the criticality of components, systems and plant with respect to maintenance The RCM study makes a trade-off of safety, economy and regularity against the maintenance cost for components and systems The recommendations from the study should be updated frequently based on reports from plant production and maintenance activities The consequence of the update may be to change the maintenance strategy, change the interval for time-based preventive maintenance or the maintainability of the equipment Important parameters used in the LCC models are *mean time between failures, mean time to repair, total man-hours to repair, cost of spare parts,* and *cost of deferred production* The parameters of the life cycle cost models will be automatically updated when new reports are included to enable continuous re-evaluation and optimization

Maintenance work involves personnel safety hazards During plant revisions, alarm and utility systems may not be functioning, and potentially dangerous situations may then develop undetected and harm maintenance workers or destroy plant equipment Even more important is that maintenance jobs are being performed more frequently while the plant is in operation due to the large cost of deferred production Safe procedures for both mechanical and electrical work on plant equipment are then imperative COPMA may be used to ensure that procedures become clear and unambiguous and to support the execution of the procedures [8 49]

Written maintenance procedures can be quite bulky when brought into the field by station staff to carry out operations An example where new technology has been used to overcome this problem, is a computerized system that has been developed to support the execution of maintenance procedures [8 50] It consists of a front-end PC-based tool for creating and editing procedures that are then down-loaded into a light-weight, hand-held, computer for use by station staff Information collection during the execution of procedures can be collected on the hand-held computer to be transmitted to other computers and users

8 5 ADVANCED OPERATOR SUPPORT SYSTEMS

Operator Support systems are gradually being developed However the current status is that there are still many prototypes under investigation, these have the potential of becoming industrial in the years to come The operator needs should be carefully analyzed before developing a new support system to obtain operator acceptance A key issue that must be resolved is how to integrate the various new systems in an appropriate way, to avoid confusing the operator with different HMI practices If this occurs many of the potential advantages of these systems will be lost in the confusion Given the multiplicity of developers, potential manufacturers and lack of standards this will be difficult to achieve in practice [8 51]

IAEA is developing a specialized database of operator support systems [8 52] This will serve as an information source for vendors, authorities and possible users of operator support systems The main motivation was to keep interested parties well informed in a field which is changing rapidly worldwide, due to the application of advanced information technology A good overview of the status in this area can be found in reference [8 53]

8.5.1. Advanced alarm handling

Special attention should be given to the integration of various alarm handling systems Although alarm handling has received considerable attention for many years, it continues to cause a number of problems A typical problem is the number of irrelevant alarms issued in disturbance situations and during normal process transients, e g start-up and shut-down, that is, how to identify irrelevant alarms in disturbance situations Another problem is how to integrate alarm information with other information systems The human cognitive capacity is limited, and is strongly negatively influenced by situational factors like stress and time pressure With complex alarm situations, the information presented to the operator can exceed his mental capacity Vital information about the process can be overlooked or not

understood, with the consequence that the operator makes erroneous assessments of the situation and executes incorrect responses or fails to respond Accidents in process industry have shown this to be a major contributing cause to human errors, as described by Reason [8 54]

Several methods and systems are being tested to cope with the problems related to alarm handling [8 55] For instance various alarm filtering techniques have been proposed In the future, more sophisticated alarm handling and alarm filtering techniques will be available

There is also an increased interest in early warning systems with the purpose of detecting problems before traditional alarm systems are triggered, thus contributing to greater plant availability

In case of major disturbances in a plant, a function-oriented approach is in many cases used to monitor plant safety status Instead of looking at single systems or variables and alarms within the system, one monitors whether critical safety functions are challenged and diagnoses the cause of the challenging of critical safety functions

Various presentation methods have been proposed, such as integrating alarm information in process mimic displays, presentation of high-level prioritized alarms on large overview screens in the control room, and the possibility to search alarm lists using different criteria

In the future, an integration of the various alarm system techniques is foreseen, where the alarm processing and presentation are designed to match the operator needs The alarm presentation will adapt to the plant state and provide more processed information to the operator [8 56]

8.5.2. Future trends of operator support systems

The main focus will still be on systems that assist operators in their status identification task, such as *integrated alarm systems* and *diagnostic systems* However, there are ongoing activities for providing predictive and prognosis type systems These systems can be used for early detection of plant excursions, for example towards a trip limit, and the operators can then execute corrective actions before the trip occurs

The level of automation is increasing Systems supporting operations planning and optimization are becoming more important as the role of the operator is changing towards more supervisory control Fig 9 illustrates how the various methods and techniques are applied versus the operator tasks, and the research activities are expected to focus more on how to implement planning functions and provide support in deriving strategies

An additional task for control room operators is to understand the functioning of the plant automatics An automatics system analyzer should provide support to the operator about the plant control system, interlocks, etc Such a system will require representation of the plant automatics knowledge in the operator support system and access to information from the automatics system during execution

As more operator support systems are developed and implemented at nuclear power plants, there is a need for developing good integration methods of new systems and harmonization of user interfaces to avoid confusing the operator in the future Standards should be developed to facilitate reuse of knowledge and software modules This is important to reduce the maintenance cost associated with operator support systems

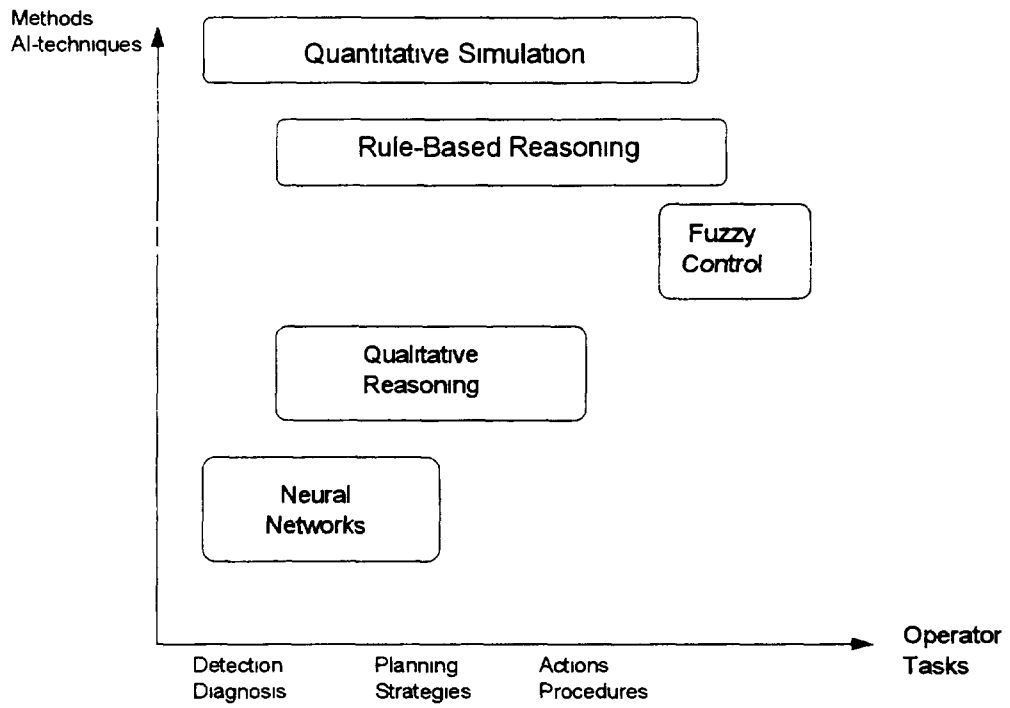


FIG 9 AI-techniques applied versus operator tasks

8 6 ADVANCED USER INTERFACES

The user interface will be one of the key technologies to be developed if many of the advanced systems currently under development are to be deployed

8.6.1. Innovative display designs

Old control room information systems are normally based on the principle of the single-sensor-single-indicator system on conventional panels When introducing CRT-based systems, very often the same methodology is applied, without taking full advantage of the new technology The tasks of the operators vary and the plant state changes consequently the display systems must support the operators during dynamic plant conditions and in abnormal situations The goal of the displays must be to provide the operators with the *right information at the right time in the right way*

Traditional display systems contain conventional mimic diagrams, which are simplified drawings of the plant system with the measured values of temperature, pressure etc indicated in digits at the position where the parameters are measured This kind of display system is often combined with trend curves of selected parameters The advantage of a mimic diagram is that the operator has a drawing of the plant and thus knows how the components are combined to perform a required function, and where the sensors are The disadvantage of a mimic diagram is that it is difficult to get an overview of a situation due to the digital appearance of the parameters The operator is not always interested in the parameter values, but is also interested in deviations from normal values and rates of change Information regarding deviations is provided in trend curves like the information on paper recorders in older control rooms

This type of mimic presentation has proved insufficient for handling the requirements of operators of modern complex plants New design proposals have been made providing advanced display systems for operators A short description of some new ideas for display systems follows

The importance of trend curves vs time for some measured values has resulted in a computer aided display concept where the history of many signals from different plant sections could be displayed vertically by color coding and/or varying the intensity For instance the type of information could be deviation from steady state in case of a disturbance, alarms, etc This display should allow scrolling all data for a user-defined history period Such systems could assist the operator for Early Fault Detection (EFD) [8 56]

One concept [8 57] uses a Multi-level Flow Model (MFM) to design display systems for a PWR-simulator MFM uses the mass flow and the energy flow to set up constraints for the correct function of the plant The MFM look at functions in the plant and every function has an icon, which in shape has nothing to do with conventional icons for components The function icon is used to present mass flow and energy flow on separate displays Further on, the activity of the control system is shown

Another method [8 58] is based on the use of polygons to present the plant temperatures was developed for a sodium-cooled reactor The corners of the polygons represent, in the horizontal direction, the position of the measuring point and, in the vertical direction, the value of the temperature A diagram of the plant underlies the polygons in the display

A third idea is based on the PWR heat engine diagram represented with the Rankine cycle [8 59] It provides an easy overview of the temperatures and the condition of the medium in a PWR plant The condition of the medium changes between water, saturated steam, superheated steam and a mixture of water and steam For information about the primary side, the distance between the actual conditions and the saturated condition can be observed from the diagram

Another example utilizes the relationship between temperature, specific heat and energy to draw a graphical interface, where the angle of some lines show the situation [8 60] The difference between *flow in* and *flow out* is also represented graphically

Future display systems should prioritize information and suppress non-relevant information in order to reduce the density and complexity of displays for the operator [8 61] However, detailed information should be accessible on demand by the user

8.6.2. Large screens

One drawback often mentioned about computerized systems for control rooms is the limited screen size which gives limited space for information display Many operators complain that they lose the geographical overview they have with conventional panels New large screens may be developed based on LCD color display Operators often wish to watch all displayed elements within the same optical distance to avoid unnecessary eye accommodation

New large screen technology offers a way to overcome the problems They also offer more flexibility than the conventional panels, which only have a static configuration

There are two main areas of application of large screens One is as a replacement of the back panels, the old mosaic instrument wall The second is as an overview display, centrally placed in the control room, to present overview information and high priority alarms like challenge to critical safety functions Large screens are used in most new reactor concepts like, the NUCAM 80+, ABWR, AP600 and N4 Several retrofitting projects for old control rooms are proposing to use large screens

8.6.3. Multimedia

Multimedia consists of many things, so defining *what is* and *what is not* multimedia is therefore difficult Multimedia is, essentially, the integration of multiple communications media [8 62] The assumption is that many media can convey complex concepts better than one or two

The use of multimedia is not just about integrating text, graphics, sound, pictures, video and animation, it is also about incorporating natural language, image processing, databases, expert systems, virtual reality, and other technologies into the user interface in order to improve their overall power [8 63]

User interfaces that exploit multimedia components are particularly suitable for tasks that involve searching for information and learning [8 64], but they are also appropriate for a variety of monitoring and control tasks Video surveillance combined with image processing can facilitate telepresence, enabling the effective remote control of robotics to perform delicate maintenance operations in hazardous environments Systems using such techniques are currently being developed for the remote control of robotics inspection during operation and maintenance in the nuclear field

The challenge for designers of multimedia human-computer interfaces is to create better interfaces using a variety of media, while not overwhelming the user with too much information

8.6.4. Virtual reality

There is a number of different definitions of virtual reality (VR) Virtual Reality can be simply defined as a " computer generated world with which the user can interact The interaction can vary from simply looking around to interactively modifying the world" [8 65] The user interface is three-dimensional and may be presented to the end-user via a head-mounted display (HMD), projection onto large screens, or a computer monitor The choice of display technology is usually governed by the application and cost Similarly, a variety of technologies exist for interacting with virtual environments, including tactile gloves, joysticks, keyboards, mice and various 3D pointing devices The potential of applying this novel technique can be seen mainly in the area of design and maintenance

Virtual Reality is particularly interesting because it can be used to create first-person user interfaces that can realistically' demonstrate the operation of dangerous or remote processes It is also to provide interesting ways of presenting scientific data, with the aim of imparting a greater understanding of the processes involved to end-users In the case of engineering design [8 66] virtual reality can be for prototyping A computer generated prototype of a control room, for example, is much cheaper to produce than a full-scale mock-up, and can be more easily modified The Advanced Engineering Section of British Nuclear Fuels (BNFL) has successfully used virtual reality in the development of the control room layout for the Sellafield Mixed Oxide Plant [8 67]

Another example of how virtual reality is being used in the nuclear industry is a system that has been developed by the Research and Development Division of Electricité de France (EDF) for nuclear reactor maintenance planning [8 68] A maintenance engineer puts on a head mounted display and enters a detailed virtual reality model of the interior of a reactor building Within the model, the engineer performs the actions appropriate to the required maintenance activity while the computer calculates the theoretical dose of radiation that would have been received had the engineer performed the actual operation This information allows more efficient procedures to be developed to reduce the overall radiation exposure of engineers performing actual operations

The apparent potential of virtual reality for presenting and interacting with information in an effective manner is one that should be investigated in order to identify how the technology can be appropriately exploited Possible advantages of using virtual reality to enhance conventional systems for training and simulation are particularly interesting

8 7 SIMULATORS FOR ON-LINE APPLICATIONS

The application of on-line simulation in process supervision is still uncommon and few industries have taken advantage of the possibilities offered by this technology There are exceptions, it has been applied to core surveillance systems, where limited instrumentation and complex dynamic behavior require the implementation of on-line simulation models

An increased interest in on-line simulation is being observed, partly due to the rapid development of computer technology and low cost high performance computer hardware There is a number of international projects addressing on-line simulation, for instance related to signal validation problems, fault detection, and diagnosis

APACS [8 69], a project for the monitoring and diagnosis of complex processes is a typical example where traditional numerical simulation components play a major role The design has three varieties of plant simulation (1) a tracking simulator that uses a parameter adjustment algorithm to keep its output matched to the plant, (2) an unadjusted model that provides the expected behavior of the plant and determines when measured values are not behaving as expected, and (3) a verification model that can determine how well a hypothesized fault matches reality

The tracking simulator is useful for two reasons First, the adjusted parameters can be checked periodically to determine if the plant characteristics are changing slowly due to plant aging Second, the diagnostic value of the tracking simulator is very useful Simulation results have shown that when there is a fault in a plant there is a dramatic shift in tracking parameter values as the tracking simulator attempt (and usually fails) to adjust parameters to match the plant The nature of the changing parameters allows the diagnostic module to focus efficiently and search for faults within a limited set of candidate hypotheses

Nuclear plant operators are developing Severe Accident Management Guidelines (SAMG) which is showing the need for computerized support Computerized Accident Management Support (CAMS) [8 70], is an area where on-line simulation and prediction becomes important The predictive simulator can explain what will happen without operator intervention or forecast the consequences of certain actions In such abnormal situations the signal validation becomes important for plant state identification as well as energy and mass balance calculations The simulators will be important for running realistic training scenarios

8 8 TOOLS SUPPORTING UTILIZATION OF NEW TECHNOLOGIES

The increased use of complex computerized systems requires test and maintenance tools that can be handled by the plant staff There are already a number of systems which enable operators to create their own user interfaces User-friendly graphical editors allow the operating staff to generate their own displays which match their needs and tasks A number of innovative display proposals have been generated and the operating staff often like to have the flexibility to develop their own display formats without changing the rest of the computer system

Many of the new systems for equipment diagnostics and operator support contain knowledge that has to be maintained by the operating staff Future systems must provide functions for easy knowledge maintenance allowing accumulated operational experience can be entered When plant modifications are made, the information systems must be updated with new process parameters and during operation, parameters must be obtained from recalibration of equipment and systems

A problem with on-line plant simulators has been the difficulty encountered in modifying the simulator if plant modifications are made Modern simulator generating tools have built in equation solvers and graphical editors which can be used for simulator configuration and parameterization These facilities ease the task of keeping simulators updated in accordance with the current state of the plant An on-site simulator that represents the current state of a plant is important for the verification of changes made to information systems at the plant, including diagnosis systems

The number of different tools used in a plant should be kept to a minimum and the way to operate and interfaces with the various systems should be unified and standardized to avoid errors and reduce the additional training needed when introducing these new systems For instance the same expert system

should be applied for different diagnostic systems if the functionality offered is adequate Examples of tools are provided in references [8 71-8 74]

8 9 INTEGRATED PLANT DATABASE

A great deal of data is produced during the life-cycle of a plant, ranging from descriptions of the original requirements for the various systems up to the design documents and drawings, and the modification history following first installation When new changes have to be made, or a retrofitting project is initiated, decades may have passed since the original requirements and design were completed Even if the original drawings are available, much of the real reasoning behind the old design is usually lacking and the new design team often have problems reconstructing the details of the system design In certain cases this may lead to the introduction of weaknesses when replacing systems in existing plants

Modern technology with relational database techniques etc can be utilized for knowledge repository Document handling and the management of related information can be managed under a new standard, the Standard Generalized Markup Language (SGML) [8 75], which is a system for defining structured document types and markup languages for representing instances of those types It integrates information of different formats and allows coded text to be reused in ways not anticipated by the coder If such techniques are utilized, the reconstruction and searching of stored information in various formats will be made much easier in the future

Knowledge representation is a highly relevant aspect when constructing Computerized Operator Support Systems (COSSs), since the same piece of knowledge is often duplicated in several types of COSSs As an example, causal relationships may be useful both in diagnosis and prognosis systems Today this common knowledge is not directly shared among different systems due to the lack of a common knowledge representation method In Artificial Intelligence (AI) research, ontology represent a means to overcome problems that have to do with re-use of knowledge It is envisaged that the application of such representation techniques will facilitate verification and validation of different COSSs and the maintenance of the consistency of the represented knowledge when the plant is modified

8 10 RISK MONITORING

A large amount of systematic work has been invested in the probabilistic safety assessment (PSA) of plants Recently, a novel concept of monitoring the plant's risk on-line has evolved Risk monitoring based on PSA techniques has been suggested by GRS, Germany, see [8 76] Northeast Utilities, USA, has reported on use of a risk monitor to support on-line maintenance and technical specification relaxation [8 77]

A risk monitor is a module which will perform a simplified probabilistic safety assessment based on the current state of the plant That is, the safety assessment will be updated when a component becomes unavailable because of a fault, because it is taken out of service for test, or maintenance, or because the state of the plant does not permit its use

The risk monitor will have a knowledge base containing results of a plant-specific PSA These results comprise event trees, fault trees, and the plant-specific data to be applied to them The event trees are categorized according to initiating events Each event tree has the initiating event frequency and branching probabilities The support systems for each branch are taken into consideration, and the dependencies are logically calculated The system unavailability are calculated from the fault trees reflecting the current state of the plant [8 78]

When the plant is operating normally, the risk is constant and equal to the pre-calculated PSA If a component becomes unavailable, the event tree is re-calculated and the current risk is displayed

If an initiating event occurs, the event tree is re-calculated and the PSA module follows which systems of the plant operate normally If the plant responds to the event in the normal way, the plant

will be shut down and come to a safe state However, if some functions do not work, the PSA module generates another path and gives suggestions for alternative success paths

With the Probabilistic Safety Assessment (PSA), nowadays the appropriate technology is available that can be used during the design phase to optimize the risk impacts of the considered installation PSAs are also used at the design certification process to maximise the safety implications of the various requirements of the plant's Technical Specifications, such as Surveillance Test Intervals (STIs) or Allowed Outages Times (AOTs) [8 79, 8 80]

During the construction phase a considerable number of changes in components and systems can occur, and further on during the subsequent operation phase due to a continuous change in the plant configuration and the operating procedures These changes may stem from planned activities like test or preventive maintenance, or from unplanned occurrences like corrective maintenance, resulting from random failures of components or systems As a result we get a fluctuation of the risk level over the operating time, which is denoted as the risk profile of the installation or plant [8 81]

An adequate computerized tool is able to calculate this risk profile, and it can be used to optimize the plant operation with respect to the minimal risk level [8 82] Based on "what happens if" questions inputted to that system it is also possible to generate a prognosis if changes of configuration, test, maintenance, and repair strategies have to be considered and planned [8 83, 8 84]

Most of the developed computerized management tools today are named "Risk Monitor" (RM) but also "Safety Monitor" or other system names are used [8 85-8 88] Recently, risk monitoring based on PSA techniques has been suggested by many organisations, like Nuclear Electric in U K [8 89-8 91], EPRI [8 92], NUS [8 93], SAIC [8 94], PLG [8 95], Southern California Edison [8 93], Northeast Utilities in USA [8 96], PNC in Japan [8 97], KAERI in Korea [8 98], Nuclear Power Station Dukovany in the Tschech Republic [8 99], JRC [8 100] in Italy, GRS [8 82, 8 84], and TUV Hamburg [8 101] in Germany

These systems are also used to reevaluate the adequacy of technical specifications and licensing requirements with respect to the Surveillance Test Intervals (STIs) and Allowable Outage Times (AOTs) [8 102, 8 103] By means of a risk-based quantification an unbalanced situation will be detected Relaxation and/or tightening of those requirements on specific components or systems can be the result of such an optimisation process [8 102, 8 104]

A RM is by principle a computerized system which will perform on-line, during one computer session, a probabilistic safety assessment based on the current state of the plant The safety assessment model will be updated by the user when a component becomes unavailable Additionally many specific plant insights (derived from the implemented knowledge base) and parameters (importance, optimal repair sequence) are displayed and calculated [8 105]

As an important task the responsible safety analyst of the plant staff has to consider the regular update of the RM if a specific system layout would be changed, and to perform the update of the generated failure statistics (failure rates) for the components

Normally, the current situation in a plant is much more complex as illustrated above It is not only the problem that one out of a huge amount of risk relevant components modelled in a PSA is out of order, in practice a complex set of components installed in different systems may fail or be out of service In this case a RM is the only tool to show the safety/risk impact immediately and to support the plant management in restoring the plant configuration as soon as possible (down to the base-line risk level)

In addition, it is possible to utilize the RM for realizing a time dependent bookkeeping during the operating year with all the component failures, outages and incidents Thus, precursor or plant performance studies can be supported substantially

REFERENCES

[8 1] BOUFERT, J et al , Nuclear Power Plant Condition Monitoring by Pattern Recognition, Institute for Safety Technology, ISTec - A - 107, (1995)

[8 2] PROCK, J , "Conceptions and Applications of Different Methods for On-line Identification of Sensor and Progress Faults in Real-time", Proc of SMORN VI, Gatlinburg, Tennessee, vol 2, USA, (1991) 64 01-64 11

[8 3] GERTLER, J J , COSTIN, J J , XIAOWEN, F , HIRA, R , KOWALCZUK, Z , QIANG, L , Model-Based on-board Fault Detection and Diagnosis for Automotive Engines, Contr Engineering Practice, Vol 1, No 1, (1993) 3-17

[8 4] TURKCAN, E , "Sensor Failure Detection in Dynamic Systems by Kalman Filtering Methodology", Proc of Dynamics and Control in Nuclear Power Stations, London (1991) 133 - 139

[8 5] BERNARD, J A , HENRY, A H , LANNING, D D , MEYER, J E , Closed-loop Digital Control of Reactors Characterized by Spatial Dynamics, MITNRL-041, MIT, (1990)

[8 6] FRANK, P M , Fault Diagnosis in Dynamic Systems Using Analytical and Knowledge-based Redundancy - A Survey of Some New Results, Automatica, Vol 26, No 3 (1990) 459 - 474

[8 7] ZHAO, Y , LEE, K Y , "Genetic Algorithm Based Feedforward and Feedback Control for Wide Range Operations of Nuclear Steam Generator", ANS Meeting, NPIC & HMIT, Pennsylvania (1996)

[8 8] KIM, C H et al , "Design of an adaptive GPC with input feedback structure, application to steam generator ANS Meeting", NPIC & HMIT, Pennsylvania (1996)

[8 9] OTADUY, P J , BRITTAIN, C R , ROVERE, L A , GOVE, N B , "A Distributed Hierarchical Architecture of Expert Systems for Supervisory Control of Multimodular Nuclear Reactors", An American Nuclear Society Meeting AI91- Frontiers in Innovative Computing for the Nuclear Industry, Jackson, Wyoming, September (1991)

[8 10] BEN-ABDENNOUR, A , LEE, K Y , "Supervisory Control with Fault Detection and Accommodation for Power Plants A Mixed Fuzzy Logic and LQG/LTR Approach", ANS Meeting, NPIC & HMIT, Pennsylvania, May (1996)

[8 11] HAUGSET, K , AND LEIKKONEN, I , Nuclear reactor control by multistage mathematical programming, Modeling Identification and Control, vol 1 (1980) 119-133

[8 12] LEIKKONEN, I Pressurized water reactor control by the hierarchical method, Modeling Identification and Control, vol 8, NO 2 (1987) 69-89

[8 13] RUMELHART, D , HINTON, G , WILLIAMS, R , Learning representations by backpropagating errors, Nature (1986) 323

[8 14] NA, N , KWON, K , HAM, C , BIEN, Z , "A study on water level control of PWR steam generator at low power and self-tuning of its fuzzy controller", FLINS 94, (1994)

[8 15] JUNG ,C H , et al , "Fuzzy Controller for the Steam Generator Water Level Based on Real-Time Tuning Algorithm", ANS Meeting, NPIC & HMIT, Pennsylvania, May (1996)

[8 16] IIJIMA T , NAKAJIMA Y , NISHIWAKI Y , "Application of Fuzzy Logic Control System for Reactor Feedwater Control", FLINS 94, (1994)

[8 17] VAN DEN DURPEL, L , RUAN, D , "Fuzzy Model Based Control of a Nuclear Reactor", FLINS 94, (1994)

[8 18] RUAN, D , YIN, X , VAN DEN DURPEL, L, D'HONDT P , "Development of a Fuzzy Logic Controller at the Belgian Reactor BR1", EUFIT 95, (1995)

[8 19] AVERKIN, A A , "Fuzzy Logic Acquisition and Simulation Modules for Expert Systems to Assist Operator's Decision for Nuclear Power Stations", FLINS 94, (1994)

[8 20] CARLSON, C , FULLER, R , "Active DSS and Approximate Reasoning", EUFIT

95, (1995)
[8 21] SCHILDT, G H , "Safety Critical Application of Fuzzy Control", IAEA-IWG-NPPCI-95/4, (1995)
[8 22] CHOU, C H , Lu, H C "A heuristic self-tuning fuzzy controller", Fuzzy Sets and Systems, Vol 61, (1994)
[8 23] SCHILDT, G H , Fundamentals on Safety Critical Comparators (Grundlagen von Vergleichern mit Sicherheitsverantwortung), Siemens Forschungs- und Entwicklungsberichte, Braunschweig/Erlangen (1980)
[8 24] SCHILDT, G H , "A Fuzzy Controller for NPPs" FLINS 96, (1996)
[8 25] Aptronix Inc FIDE Fuzzy Inference Development Environment V 2 0 Application Note 006-920914, San Jose, CA, USA (1992)
[8 26] BUCKLE,Y J J , "Stability and the fuzzy controller", Fuzzy Sets and Systems, Vol 77 (1996)
[8 27] DE VIRON, F , DE VLAMINCK, M , GOOSENS, A , MONTEYNE, M , "A Prototype Neural Network to Perform Early Warning in Nuclear Power Plants", Int Journal of Fuzzy Sets and Systems (1994)
[8 28] CHUNG, H Y , BIEN, Z , "Real Time Diagnosis of Incipient Multiple Faults with Application for Nuclear Power Plants", FLINS 94 (1994)
[8 29] OH, Y G , et al , "Application of Fuzzy Logic for monitoring and Diagnosis of Loose Parts in Nuclear Power Plants", IASTED Pittsburgh, USA, April (1995)
[8 30] IAEA-Specialists meeting on "Monitoring and Diagnosis systems to improve NPP reliability and Safety", Barnwood, Gloucester, UK, May (1996)
[8 31] OLMA, B DING, D Y , "Operational Experiences with Automated Acoustic Burst Classification by Neural Networks", SMORN VII, Avignon, France, June (1995)
[8 32] NABESHIMA, K , SUZUKI, K , TURKCAN, E , "Neural Network with an Expert System for Real Time Nuclear Power Plant Monitoring", SMORN VII (1995)
[8 33] KISS, J , SOUMELIDIS, A , BOKOR, J , "Applying Artificial Neural Networks in Nuclear Power Plant Diagnostic", SMORN VII (1995)
[8 34] YOSHIKAWA, S , SAIKI, A , UGOLINI, D , OZAWA, K , "Nuclear Power Plant Monitoring and Fault Diagnosis Methods based on Artificial Intelligence Technique", SMORN VII (1995)
[8 35] JEONG, E , FURUTA, K , KONDO, S , "Identification of Transients in Nuclear Power Plants Using Neural Networks with Implicit Time Measure", ANS meeting, Philadelphia (1995)
[8 36] UPADHYAYA, B R , ERYUREK, E , MATHAI, G , "Neural Networks for Sensor Validation and Plant Monitoring", Int Fast Reactor Safety Meeting, Utah (1990)
[8 37] BARTLETT, E B , UHRIG, R E, "Nuclear Power Plant Diagnostic using Artificial Neural Networks", AI 91, Wyoming (1991)
[8 38] OH, S H , KIM, D I et al , "Sensor Signal Validation Method of Nuclear Power Plants using Neural Networks and the Inconsistency Index", ANS meeting, Philadelphia (1995)
[8 39] FANTONI, P F , MAZZOLA, A , "Transient and Steady State Signal Validation in Nuclear Power Plants using Autoassociative Neural Networks", SMORN VII, Avignon (1995)
[8 40] KOZMA, R , YOKOYAMA, Y , KITAMURA, M , "Intelligent Monitoring of NPP anomalies by an Adaptive Neuro-Fuzzy Signal Processing System", ANS meeting, Philadelphia (1995)
[8 41] KOZMA, R , SATO, S , SAKUMA, M , KITAMURA, M , "Detecting Unexperienced Events via Analysis of Error Propagation in a Neuro-Fuzzy Signal Processing System", ANNIE 94, Missouri (1994)
[8 42] FROESE, T , VOLLMER, N , "Predictive Control with Neural Network and Fuzzy Control", EUFIT 95 (1995)
[8 43] BEDZAK, M , DACA, W , "Intelligent Control by Fuzzy Neural Network Method", EUFIT 95 (1995)
[8 44] BIGAND, A , MESSAADI, A , "Industrial Plant Valuation for Fuzzy Adaptive

Control", EUFIT 95 (1995)
[8 45] NAUCK, D , "Beyond Neuro-Fuzzy Perspectives and Directions", EUFIT 95 (1995)
[8 46] LEPP R M , Instrumentation and Control in the Canadian Nuclear Power Program - 1995 Status, AECL, Chalk River Laboratories (1995)
[8 47] SCHILDT, G H , "An Object-Oriented-Database-System to Assist Control Room Staff", IAEA-Meeting on Monitoring and Diagnosis Systems to Improve Nuclear Power Plant Reliability and Safety, Barnwood, Gloucester, May (1996)
[8 48] MATHISEN, K , MOCOM Model Based Condition Monitoring, Halden Reactor Project, HWR-XXX (1996)
[8 49] TEIGEN, J , NESS E , HALL, R D , COPMA-III Discussion on Requirements and Design Issues, Halden Reactor Project, HWR-385, October (1994)
[8 50] LEPP, R M , Instrumentation and Control in the Canadian Nuclear Power Program - 1995 Status, AECL, Chalk River Laboratories (1995)
[8 51] HAM, C S , et al , "An Integrated Approach for Integrated Intelligent Instrumentation and Control System", Halden Reactor Project, EHPG meeting, Loen, Norway May (1996)
[8 52] DOUNAEV, V et al , "IAEA Activity on Operator Support Systems in Nuclear Power Plants" Proceedings of the IAEA Specialists meeting on Advanced Information Methods and AI in Nuclear Power Plant Control Rooms Halden, Norway, IAEA-12-SP-384 37, September (1994)
[8 53] Proceedings of the IAEA Specialists meeting on Advanced Information Methods and AI in Nuclear Power Plant Control Rooms Halden, Norway, IAEA-12-SP-384 37, September (1994)
[8 54] REASON, J , Human Error, Cambridge University Press, Cambridge, 1990
[8 55] KIM, I S , "An Integrated Approach to Alarm Processing", ANS Meeting, NPIC & HMIT, Pennsylvania, May (1996)
[8 56] BYE, A , NILSEN, S , HANDELSBY, F , WINSNES, T , "COAST-Computerized Alarm System Toolbox" 2nd IFAC Workshop on Computer Software Structures Integrating AI/KBS Systems in Process Control Lund, Sweden, August (1994)
[8 57] LIND, M , "Multilevel Flow Modeling of Process Plant for Diagnoses and Control " International Meeting on Thermal Nuclear Research Safety Chicago, U S A (1982)
[8 58] LINDSAY, R W , "A Display to Support Knowledge Based Behaviour " Advances in Human Factors Research on Man-Computer Interactions Nuclear and Beyond, Nashville, Tennessee, USA, June (1990)
[8 59] BELTRACCHI, L , "A direct manipulation interface for water-based Rankine cycle heat engines", IEEE Transaction on System, Man and Cybernetics, SMC-17 (1987) 478-487
[8 60] VINCENTE, K , RASMUSSEN, J , "The ecology of Human-Machine Systems II Mediating Direct Perception in Complex Work Domains " ECOLOGICAL PSYCHOLOGY 2(3) (1990)
[8 61] TAKIZAWA, Y , et al, "An Intelligent Man-Machine System for Future Nuclear Power Plants", Vol 107, Nuclear Technology, July (1994)
[8 62] LIESTØL, G , "The Digital Video Album On the Merging of Media types in Multimedia", Teletronic 4, Telenor, Norway (1993)
[8 63] WATERWORTH, J A , Multimedia Technology and Applications, Chichester, England, Ellis Horwood Ltd (1991)
[8 64] CHIGNELL, M H WATERWROTH, J A , Exploring Multimedia Information, Multimedia Interaction With Computers, Human Factors Issues Chichester, England, Ellis Horwood Ltd (1992) 113-139
[8 65] KOOPER, R , Virtually Present, Treatment of Acrophobia by Using Virtual Reality Graded Exposure Delft, Technical University of Delft (1994)
[8 66] RHEINGOLD, H , Virtual Reality London Mandarin Paperbacks (1992) 363-367
[8 67] Division Ltd Division Advances Frontiers of Virtual Reality in Engineering Design, Press Release, 11 June 1995, Bristol Division (1995)
[8 68] Division Ltd Designing and Testing for Hazardous Environments, Application Brief,

Bristol Division (1994)
[8 69] BENJAMIN, M E et al, "APACS Monitoring and Diagnosis of Complex Processes", Proceedings of the IAEA Specialists meeting on Advanced Information Methods and AI in Nuclear Power Plant Control Rooms, IAEA-12-SP-384 37, Halden, Norway, September (1994)
[8 70] BERG, Ø et al, "Analysis of Severe Accident Phenomenology and need for Computerized Accident Management Support", OECD Specialist Meeting on Severe Accident Management Implementation, Niantic, Connecticut, U S A, June (1995)
[8 71] ARNDT, S A, BARMSNES K, GRIFFIN J P, "The use of PICASSO in the Development of the Nuclear Engineering Workstation Simulator", Proceedings of the 1993 Simulation Multiconference on International Simulators Conference Simulation Series, Volume 25, Number 4, Arlington, Virginia, USA, March (1993)
[8 72] G2 Reference Manual Gensym Corp 125 Cambridge Park Drive, Cambridge, MA 02140, USA (1990)
[8 73] ABRAMOVITCH, A, "ROSE A Realtime Object Oriented Software Environment for High Fidelity Replica Simulation", NEA/CSNI/R(93)11, CSNI Specialist Meeting on Simulators and Plant analyzers Lappeenranta, Finland, June (1992)
[8 74] JUSLIN, K et al, "Recent Development of APROS towards the On-line Simulator", OECD NEA-Proceedings of the Specialist Meeting on Operator Aids for Severe Accidents Management and Training Halden, Norway, June (1993)
[8 75] GOLDFARB, C F, The SGML Handbook, Clarendon press, Oxford University Press Walton Street, Oxford OX2 6DP
[8 76] KAFKA, P, LUPAS, O, WU, J, ZIMMERMANN, M, "A computer aid for safety assessment and configuration management of complex systems based on PSA models", Proc of PSAM-II, San Diego, Cal, USA, March (1994)
[8 77] WEERAKKODY, S D, DUBE, D A, BONACA, M V, "Use of a risk monitor to support on-line maintenance and technical specification relaxation", Trans of the American Nuclear Society, Vol 73, San Francisco, Cal, USA, October (1995)
[8 78] BERG, U, "RELCON's Risk Analysis Software", PSA'95, Seoul, Proceedings KAERI, ISBN 89-950024-1-7-94550, November (1995)
[8 79] KIM, I S, et al, "Application of PSA to Define Technical Specifications for Advanced Nuclear Power Plants", Proceedings KAERI, PSA'95, Seoul, November (1995)
[8 80] LEDERMANN, L, NIEHAUS, F, TOMIC, B, "Probabilistic Safety Assessment - Past, Present and Future", Principal Division Lecture, Division M, SMiRT-12, Stuttgart (1993)
[8 81] VESELY, W E, BURLILE, G A, "System Unavailability Indicators applied to the past Histories of five Plants", Report, November (1988)
[8 82] KAFKA, P, ZIMMERMANN, M, "Operational Risk Management", Proceedings, ESREL 95, Bournemouth, June (1995)
[8 83] SAMANTA, P K, VESELY, W E, KIM, I S, "Study of Operational Risk-based Configuration Control", NUREG/CR-5641, U S Nuclear Regulatory Commission, Washington DC (1991)
[8 84] KAFKA, P, LUPAS, O, WU, J, ZIMMERMANN, M, "A Computer Aid for Safety Assessment and Configuration Management of Complex Systems based on PSA Models", Proceedings PSAM II, San Diego CA, March (1993)
[8 85] KAFKA, P, "Living PSA - Risk Monitor Current Developments", Paper IAEA TCM, Budapest 7-11 September 1992, IAEA TECDOC-737, March (1994)
[8 86] TUV Norddeutschland, "4th TUV Workshop on Living PSA Applications", Hamburg, May (1994)
[8 87] APOSTOLAKIS, G, KAFKA, P, Edts, "The Role of Personal Computers in Probabilistic Risk and Safety Assessment and Decision Making", Elsevier Applied Science 379-398, ISNB 1-85166-501-3
[8 88] KAFKA, P, KUNITZ, H, "Computerized Systems for high-level Information Processing and Decision Making in PSA", Reliability Engineering and System Safety

Vol 30 (1990)

[8 89] HORNE, B E , "The Essential System Status Monitor for Heysham Nuclear 2 Power Station", TCM, IAEA, Vienna, October (1988)

[8 90] Waddell, W B , "Operational Experience of a Reliability Based Maintenance Strategy for the Control of Essential Post Trip Cooling Plant in a Nuclear Power Station", Seminar on Operating Reliability and Maintenance of Nuclear Power Plant, U K, March (1990)

[8 91] EVANS, J N , "Experience in the Application of 'PSA Techniques to Operation of GEGB Nuclear Power Station" , 2nd TUV Workshop on Living PSA Application, Hamburg, May (1990)

[8 92] DAGAN, W J , KALRA, S P , "Outage Risk Assessment and Management (ORAM) A Computerized Tool to help Manage Plant and Equipment Outages", PSA 95, Seoul, Proceedings KAERI, ISBN 89-950024-1-7-94550, November (1995)

[8 93] MORGAN, T A , "Development and Use of the San Onofre Safety Monitor" , IAEA-*J4-TC-855 (1993)*

[8 94] PUTTNEY, B , RILEY, J , CRAGG, C , GOUGH, W , "Application of the EOOS On-Line Monitor", PSA 95, Seoul, Proceedings KAERI, ISBN 89-950024-1-7-94550, November (1995)

[8 95] EPPSTEIN, J , "RISKMAN A Program Demonstration", Post SMiRT Seminar No 7, Los Angeles (1989)

[8 96] WEEVAKKODY, S D , DUBE, D A , BONACA, M V , "Use of Risk monitor to support on-line Maintenance and Technical Specification Relaxation", Trans of the American Nuclear Society, Vol 73, San Francisco, Ca USA, October (1995)

[8 97] AIZAWA, K , NAKAI, R , "Living PSA Program LIPSAS Development for Safety Management of an LMFBR Plant", Reliability Engineering and System Safety, 44, Nr 3 (1994) 135-138

[8 98] KIM, T W , HAN, S H , CHANG, S C , KIM, S H , HA, J J , " Development of a PSA Workstation in KAERI", PSA'95, Seoul, Proceedings KAERI, ISBN 89-950024-1-7-94550, November (1995)

[8 99] PUGLIA, W J , DUBSKY, L , "Safety Advisor System (SAS) - Design Description and Implementation at the Nuclear Power Station Dukovany", PSA/PRA and Severe Accidents'94, Ljubliana, Slovenia, April (1994)

[8 100] POUCET, A , "STARS, Knowledge based tools for Safety and Reliability Analysis". Reliability Engineering and System Safety, Vol 30 (1990)

[8 101] BOHME, E , MUSEKAMP, W , NEUMANN, L , "SAIS A Software Tool for PSA and Plant System Safety Analysis", 4th TUV Workshop on Living PSA Application, Hamburg, May (1994)

[8 102] WONG, S M , HOLAHAN, G M , CHUNG, J W , JOHNSON, M R , "Risk-based Methodology for USNRC Inspections", PSA'95, Seoul, Proceedings KAERI, ISBN 89-950024-1-7-94550, November (1995)

[8 103] VESELY, W E , CHUNG, W , BUCHER, E J , THADANI, A C , "Risk Management Strategies - Qualitative and Quantitative Approaches", PSA'95, Seoul, Proceedings KAERI, ISBN 89-950024-1-7-94550, November (1995)

[8 104] EPRI Risk-based Technical Specification Program Site Interview Results, EPRI NP-7436, Electric Power Research Institute, August (1991)

[8 105] VESELY, W E , DAVIS, T C , DENNING, R S , SALTOS, N , "Measures of Risk Importance and their Applications", NUREG/CR-3385, Battelle Columbus Laboratories (1989)

9. CONCLUSIONS AND RECOMMENDATIONS

9 1 CONCLUSIONS

1 Fault tolerant digital instrumentation and control (I&C) systems have been demonstrated to be effective automation and control technology for nuclear plant applications These digital I&C systems use redundancy and signal validation methods, and provide a wide range of algorithms with more optimized performance and higher reliability than previous analog I&C systems They have been shown to reduce plant outages and trips, and reduce safety challenges to the plant

2 Computer-based systems for safety protection have been implemented successfully in several countries The extensive verification and validation required to provide assurance of software accuracy and integrity has been found to be very costly However, the need to address obsolescence of existing protection equipment and the attraction of better protection algorithms is expected to increase the number of digital protection applications

3 Applications of computer systems for display of the plant state to the operators is now a common form of human-machine interface technology Operator support systems that can improve human performance in monitoring and diagnosis are being implemented in nuclear power plants world wide

4 Large-scale application of computer technology has been implemented in nuclear power plants in Canada, France, Germany, Japan, and UK They will be intrinsic in future advanced nuclear plants Successful demonstrations of digital instrumentation and control systems in existing plants provide a real opportunity to exploit capabilities to the benefit of plant economics, reliability and safety

5 Technological trend shows that new techniques such as artificial intelligence, neural networks, fuzzy logic, expert systems, etc will gain increasing importance in the deployment of future systems in the nuclear power plants Most of these systems rely on knowledge-based techniques It will be a challenge to demonstrate that these systems are better than the conventional techniques when they are deployed to manage certain tasks in nuclear power plants

6 Diagnostic system applications at nuclear power plants for loose parts monitoring, vibration monitoring, process monitoring etc allow increase of reliability and efficiency of operation Computer technology applications will lead to more widely deployment of on-line diagnostic systems Neural networks and expert systems applications in the area of diagnostic systems will allow enhancement to the accuracy of diagnostic results

9 2 RECOMMENDATIONS

1 Backfitting of nuclear power plants is a continuing process for existing systems, including instrumentation, control, monitoring and diagnosis, and human-machine interface The designs for future reactors are being developed with fully digital I&C systems and computer-based control rooms Research and development effort is needed to ensure that the new technology provides the expected improvements in operational safety and efficiency

2 Reliability assessment is very important for advanced computer-based systems in order to ensure their applicability to safety and high integrity systems The development of an international guidance for quantitative reliability assessment for computer-based systems in nuclear power plants would be useful

3 Advanced operator support systems should include integrated alarm systems and diagnostic systems Future developments in this field should lead to prediction and prognosis of plant state, so that early detection of plant states approaching a trip limit is possible As such, operators can perform corrective actions before the trip occurs

4 Advanced display designs should support the operators during dynamic plant conditions and/or abnormal situations Future display systems should provide the operators with the correct information efficiently and effectively Such display systems should comprise large screens, multimedia, and virtual reality

5 Advanced simulators for on-line application will become a major interest in the future and it should contain facilities for signal validation, early fault detection and diagnosis Such simulators

will be able to predict what will happen to the plant without operator's intervention or forecast the consequences of certain actions

6 Tools for supporting the use of new technologies in testing and maintenance purposes should be developed This requires configuration tools for operators to configure their own display formats without changing the rest of the computer system Future systems should provide functions for easy maintenance of the knowledge base, where accumulated operational experience can be entered Modern simulators may comprise implicit equation solvers and offer graphical editors, which can be used for simulator configuration and parameterization

7 Integrated plant database should be used to capture the plant requirement specification, design documents and drawings, the modification history after the first installation, and operational experience during the life cycle of the plant System design for such integrated plant database should be based on knowledge acquisition and knowledge representation techniques

8 Risk monitoring should be developed based on probabilistic safety assessment corresponding to the current state of the plant That means, safety assessment may be updated when a component becomes unavailable because of a failure or is taken out of operation for maintenance reasons Advanced risk monitors should be developed based on the knowledge base of a plant-specific probabilistic safety assessment

9 Research and development are needed on the topic of intelligent signal processing under real-time constraints These include signal-to-noise-ratio analysis and plausibility checks of measured values

10 Diagnostic systems should be applied systematically to monitor the status of vital plant components to support condition-based maintenance

11 Various kinds of expert systems should be explored to assist plant staff in activities including equipment diagnostics, early fault detection, computer aided maintenance, plant maintenance optimization, etc

12 Advanced control techniques should be exploited to be fully integrated with digital control systems in order to optimize the plant performance

13 Fuzzy control techniques should be promoted for implementation into advanced control algorithms, because strong non-linear system behavior can be handled more efficiently by applying a knowledge based system approach compared to a conventional model description There are other advantages for applying fuzzy control including robustness, smooth system reaction, transparency due to knowledge-based linguistic description, and improved real-time performance in comparison with conventional controllers However, there are still problems to be overcome before these systems can be successfully exploited, in particular the development of a cost effective verification and validation process

14 Neural networks and fuzzy logic may be combined as new approaches to capture the advantages of both methods Advantage of learning as well as the generalization capability may be exploited in the next generation systems

APPENDIX A
NATIONAL STANDARDS AND GUIDELINES FOR ADVANCED I&C SYSTEMS

The structure of the international standards and guidelines was established in chapter 2 along with supporting material that is considered to have international consensus This material is valuable to those wishing to establish or develop a standards framework However, many countries have national standards that are particularly relevant to nuclear power plant systems as licensing and operation of nuclear plant are completed on a strictly national basis and the national licensing practices and regulations often appeal directly to national standards In many cases, the standards material is supplemented by guidance documents

The standards and guidelines recorded in the Appendix A merely represent a few national examples They are not meant to be exhaustive search of all standards and guidelines from all nuclear countries

A.1. Canada

The Canadian standards structure and the requirements for nuclear plant are linked through Atomic Energy Control Board (AECB) guides The standards are produced by the Canadian Standard Association (CSA) The use of the CSA standards has been mandated as part of the licensing process by the AECB These standards include

- N286 0 to N286 7 CANDU Quality assurance program
  General, procurement, design, construction, commissioning, operation),
- N290 1 Shutdown system requirement,
- N290 4 Reactor control system requirement,
- N290 5 Support power systems requirement,
- N290 6 Monitoring and display system requirement

The Canadian national standards are supplemented by a significant number of AECB guidelines and company standards The AECB guidelines specific to I&C include

- Shutdown systems,
- R10 Safety system,
- C99 Reporting requirements

The company standards are well known to the AECB which accepts their use within the licensing framework The standards include

- Software engineering for Cat I safety critical,
- Software engineering for Cat II safety related,
- Software engineering for Cat III other nuclear,
- Qualification of predeveloped software,
- Method of software categorization,
- Modification of existing software,
- Special safety system separation design guide,
- Safety related and process system separation design guide

Use is also made of additional standards coming from IEEE, ASME and ISA

A.2. Finland

Supervision of nuclear safety in Finland is based on the Nuclear Energy Act (990/87) The Finnish Center for Radiation and Nuclear Safety (STUK) is an authority and an expert in radiation and nuclear matters STUK sets detailed safety requirements, the YVL Guides, for construction and operation and verifies compliance with them through varied inspection programs STUK's research and evaluation projects in the field are published in the STUK publication series Example Guides relevant for control systems are

- YVL 1 4 Quality assurance of nuclear power plants,
- YVL 2 1 Safety classification of nuclear power plant systems, structures and components,
- YVL 5 5 Supervision of electric and instrumentation systems and components at nuclear facilities

A recent evaluation study is described in STUK-YTO-TR 93, "Feasibility of safety assessment methods for programmable automation systems"

A.3. France

The French Ministry of the Industry published „Fundamental Safety Rules" (RFS), guiding the interpretation of the IAEA codes and guides in France

The French association for the design of nuclear installations (AFCEN) brings together power utilities and industries to publish French codes for design, construction and maintenance of nuclear power plants These codes set up detailed rules, taking into account the technological state of the art and the organization between utilities (EDF), industries and the safety authority, in accordance with the RFS and relying on international standards The codes for design and construction of nuclear power plants are called RCC

The RCC-E "Design and construction rules for electrical equipment in nuclear island of NPP" (1987) is the French code dedicated to I&C It contains the rules on equipment and software aspects for all nuclear I&C important to safety and refers to applicable international standards, for example IEC 880 for safety critical software

A.4. Germany

The design and operation of nuclear power plant is based on the general requirements of the ministry for the environment (BMU) and the guidelines of the reactor safety commission (RSK) The RSK guidelines for I&C were revised in March 1996 The technical requirements for I&C systems, along with those for all other systems, are set by the KTA (Technical Association on Nuclear plants) Rules The KTA rules form the basis for the assessment completed in the course of the licensing process

The subset of the KTA rules relevant for I&C systems include

- 1401 Quality Assurance , general requirements (December 1989),
- 1404 Documentation of design and operation of plant (June 1989),
- 1501 to 1508 Radiation Monitoring and Protection,
- 2206 Design against lightning (June 1989),
- 3501 Reactor Protection system (RPS) (June 1985),
- 3502 Accident Instrumentation (November 1984),
- 3503 Type test of I&C modules for RPS (November 1986),
- 3504 Electrical drivers of the safety system,
- 3505 Type test of sensors and transducers for the RPS (November 1984),
- 3506 Tests of safety relevant I & C systems (November 1984),

- 3507 Factory tests of I&C systems (November 1986),
- 3904 Design of main control room, remote shutdown station and local controls in NPPs (September 1988)

The criteria used to assign safety functions to different categories are derived from the radiation protection rules The basis for the design of I&C equipment is a deterministic approach from the failure-tolerance requirements For the assessment of digital I&C systems additional IEC standards are applied to cover the open points

A.5. Republic of Korea

Regulating and licensing nuclear facilities in Republic of Korea is based on the provisions of the Atomic Energy Act of Republic of Korea and its Enforcement Decree and Regulation The notice of the Minister of Science and Technology based on the Atomic Energy Act states that nuclear facilities in Republic of Korea can be applied with national standards of reactor supplies if the application of such standards do not degrade their safety and performance Up to now, the utilization and regulations of nuclear power are carried out in accordance with the national standards of the suppliers on a case by case basis

Keeping pace with the international trend for the development of advanced reactor, the government of Republic of Korea and utility have conducted the Korea Next Generation Reactor (KNGR) program to develop the technologies for an ALWR from 1992 The KNGR will be an evolutionary reactor having some passive features and will be commercially operated in 2006 As a part of the KNGR program, the regulatory technical requirements for the KNGR will be developed by 2001 The regulatory requirements for advanced instrumentation and control systems will be developed as specific safety requirements and guides based on

- IEEE 7-4 3 2 - 1993,
- SECY-87-093,
- IEC 880

with the focus being on software reliability, defense against software common mode failure and software quality assurance

A.6. Russia

The key requirements for nuclear systems are captured in standards OPB-88 and PBY RUAS-89 These standards call up more detailed standards and codes of practice covering quality assurance, seismic, instrumentation etc The special standards for nuclear power plant I&C systems are supplemented by general industrial standards, codes of practice and by international standards The national normative documentation has a hierarchical structure The highest level contains general requirements for different aspects of I&C systems and its implementation The second level or tier of documentation contains more detailed requirements while the lowest tier are used to provide specific implementation details and practices In all there are over some hundred standards and normative documents to be applied during the development and deployment of I&C systems

The standards currently available are generally oriented towards traditional analogue equipment to be used in an industrial environment There is a limited amount of material available concerning the use of computer based systems however the IEC 880 standard forms the basis of most software work

The key standards related to NPP I&C systems include

- OPB-88 General regulations of NPP safety provisions during designing, construction and operation,
- PBY RU AS-89 Nuclear safety rules for the reactors of NPP,

- GOST 24 104-85 Control automated systems General requirements,
- GOST 29075-91 Nuclear instrumentation building systems for NPP General requirements,
- Special delivery conditions of equipment, devices, materials and goods for objects of nuclear power engineering,
- GOST 26843-86 Nuclear power reactors General requirements to reactor control & protection system,
- GOST 27445-87 Neutron flux monitoring systems for control & protection of nuclear reactors,
- GOST 25804 1-83 Apparature, devices, facilities and equipment of NPP technological processes control systems General regulations,
- GOST 25804 2-83 Apparature, devices, facilities and equipment of NPP technological processes control systems Reliability requirements,
- GOST 25804 3-83 Apparature, devices, facilities and equipment of NPP technological processes control systems Requirements to durability, solidity and steadiness concerning external influencing factors,
- GOST 25804 5-83 Apparature, devices, facilities and equipment of NPP technological processes control systems General rules for engineering samples and serial production testing and acceptance,
- GOST P50746-95 Hardware electromagnetic compatibility Hardware for NPP Technical requirements & testing methods

A.7. United Kingdom

The basic safety requirements for UK nuclear facilities are identified in the Safety Assessment Principles issued by the Nuclear Safety Division of the Health and Safety executive which provide a framework for the consistent application of the principles The principles can be identified as being fundamental Requirements and Policy, basic Principles and Engineering Principles

The requirements arising from these principles have been developed by the nuclear operating organizations rather than through the production of standards This is in part because of the nature of the UK regulatory regime which is not prescriptive also because the UK supports international standards in preference to national ones The company documents, for example the Advanced Gas Cooled Reactor Design Safety Guidelines, call up a significant number of standards, which are usually detailed and specific to some component or property

Nuclear Electric, formerly CEGB, have taken responsibility for the reduction of much of the guides and codes of practice material for nuclear installations The key documents relating to instrumentation and control include

- Control and Instrumentation General Technical Requirements Specification, US/76/10/GEN, GDCD/CIDOCS 0125, CEGB, Sept 1988,
- Alarm Annunciator Equipment Performance, Design and Test Requirements, NE/PROC/SPEC/500121, Nuclear Electric, Issue 1, Sept 1982,
- General Specification for Electronic Equipment, EES 1989, Nuclear Electric, May 1989,
- Guidelines for using Programmable Electronic Systems in Safety and Safety Related Applications TD/STD/REP/0240, SMSG/P(93)/43, Issue 2, Nuclear Electric, December 1993

The following documents are issued by the Health and Safety Executive who are responsible for industrial safety legislation The documents may not have the force of standards but they do in effect have the backing of the law The essential documents include

- HSE PES guidelines Part 1,
- HSE PES guidelines Part 2,
- HSE NSD Safety Assessment Principles for Nuclear Plant

A.8. United States of America

The key requirements for advanced I&C upgrade in the USA come from the US Nuclear Regulatory Commission As the regulatory requirements are still evolving, the initiation of these requirements in the form of standards has been undertaken by a number of institutions including the American Nuclear Society (ANS), American National Standards Institute (ANSI), American Society of Mechanical Engineers (ASME), the Electric Power Research Institute (EPRI) and the Institute of Electronics and Electrical Engineers (IEEE) The IEEE standards are those most relevant to the advanced control and instrumentation Some sample NRC requirements and technical guides as well as industry standards and guidelines that are relevant to digital I&C are listed below

US Nuclear Regulatory Commission:

- USNRC report NUREG/CR-6263, "High Integrity Software for Nuclear Power Plants-Candidate Guidelines, Technical Basis and Research Needs", two volumes, MITRE Corporation, June 1995
- USNRC Generic Letter 95-02, "Use of NUMARC/EPRI Report TR-102348, Guideline on Licensing Digital Upgrades, in Determining the Acceptability of Performing Analog-To-Digital Replacements Under 10 CFR 50 59", US Nuclear Regulatory Commission, April 26, 1995
- US NRC, "Final Safety Evaluation Report, Related to the Certification of the System 80+ Design", Chapter 7-Instrumentation and Controls, August 1994
- NUREG 800 Standard review plan for Nuclear power plant

US Industry Standards and Guidelines:

- American Nuclear Society (ANS), American National Standards Institute (ANSI), and Institute of Electrical and Electronics Engineers (IEEE) Standard 7-4 3 2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"
- IEEE Std 323-1983, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"
- IEEE Std 603-1971, "Criteria for Safety Systems for Nuclear Power Generating Stations"
- ANSI/IEEE Std 730-1989, "IEEE Standard for Software Quality Assurance Plans"
- ANSI/IEEE Std 828-1983, "IEEE Standard for Software Configuration Management Plans"
- IEEE Std 829-1983, "Standard for Software Test Documentation"
- IEEE Std 1008-1987, "Standard for Software Unit Testing"
- ANSI/IEEE Std 1012-1986, "IEEE Standard for Software Verification and Validation"
- ANSI/IEEE Std 1042-1987, "IEEE Guide to Software Configuration Management"
- ANSI/IEEE Std 1058 1-1987, "IEEE Standard for Software Project Management Plans"
- ASME NQA-2a-1990 Addenda, Part 2 7, "Quality Assurance Requirements of Computer Software for Nuclear Facility Applications"

APPENDIX B
ADVANCED VIBRATION MONITORING IN GERMAN PWRs

As an example for advanced vibration monitoring, comprising all important components of the primary cooling system, the vibration monitoring system installed in the German Konvoi plants (commissioning in 1988 and 1989) is described in the following

The sensors used for vibration monitoring in a typical 4-loop PWR in Germany are

4 absolute displacement sensors on closure head of RPV (A-signals),

16 relative displacement sensors, 2 below each main coolant pump measuring in two horizontal directions, 2 on each hot leg position near the steam generator measuring in horizontal and vertical directions (R-signals),

8 ex-core neutron sensors of the safety-instrumentation (X-signals),

5 pressure sensors, located in inlet/outlet pipes (P-signals),

8 proximity probes, 2 at each reactor coolant pump shaft measuring in two horizontal directions (W-signals)

Vibration analysis is performed in the frequency domain using FFT-algorithms and correlation techniques The monitoring principle is based upon the comparison of actual signatures (auto power spectral densities, coherence and phase functions) with identified and well understood reference signatures These signatures or „fingerprints" are plant-specific and have to be identified for each PWR prototype by comprehensive investigations When monitoring the primary system of a PWR, the need to observe two different type of vibrations led to a classification regarding the time dependence of mechanical degradation, i e

- Passive components like pressure vessel, vessel internals, piping systems, pump-housings and steam generators are mainly forced by static loads like pressure, dead weights or internal stresses - the propagation of mechanical defects is extremely slow
- Active components with a high energy conversion like pump-shafts, turbine rotors or motor-driven valves are primarily loaded by dynamic forces As these load cycles are extremely high, short-term degradation has to be assumed

Covering both types of failure characteristics, the COMOS system has been built, which in fact contributes a precursor to integrated diagnosis systems, taking care of monitoring all vital plant components to allow for condition based maintenance The system comprises two monitoring modes

TABLE II TWO MONITORING MODES OF COMOS

	Mode 1	Mode 2
Scope of monitoring	MCP-shaft crack detection	primary circuit vibration monitoring
Monitoring focused on	rotative frequency and higher harmonics	structural resonance + fluid resonance
Information condensed to	alert to the control room	printer output of relevant deviations

Up to now vibration analysis demonstrated its ability and merits, in many practical cases Examples are the detection of excessive core barrel movements, fuel rod and control rod vibration, early warning of developing cracks in main coolant pump shafts, etc On-line monitoring has to rely upon a restricted number of sensors, consequently extensive use of vibration measurement in the phase of plant commissioning and the development of special theoretical models is necessary to get a firm reference

basis for the healthy state Moreover continuous or quasi continuous measurement and analysis of the on-line data is necessary, because the trends of the observed parameters are the indicator for developing deficiencies rather than their absolute values In addition it is necessary to have available the history of the monitoring signals if an event is detected and has to be interpreted Operational experience with passive components can be summarized as follows

- The surveillance is based on frequency deviations of natural frequencies
- The development of mechanical degradation (from material fatigue, bearing influences, clamping conditions etc) is rather slow, normally in the time span of several weeks to several months
- Vibration monitoring has demonstrated the ability to detect and diagnose the nature of structural degradation Detection of reduced mechanical integrity e g of reactor vessel internal components in its early stages allows corrective action to be taken before major weakening or damage occurs
- Information on the condition of reactor vessel internal components supplements inspection and can be used when anticipated life time of major components is reached

Experience with diagnosis regarding shaft rupture of main coolant pumps (which to some extent can be certainly extended to pumps with horizontal shafts) gives the following picture

- The monitoring is based on amplitude trend analysis of rotation specific frequency components
- Changes of operation parameters (e g load change, primary pressure, primary temperature, seal flow, seal pressure, seal temperature, bearing temperature, pump head) may influence the shaft vibrations substantially
- Crack propagation has been observed to develop in the time span of several months

As mentioned above surveillance of shaft vibration could be extended to further vital pumps in the plant, e g the feedwater pumps, emergency core cooling pumps As a matter of fact basic investigations in this direction have been started in several countries In Germany two years ago the development of a diagnosis system for recirculation pumps in BWRs has begun, in the framework of refurbishment of these pumps in KKP-1, KKI-1 and KKB The essential point was the replacement of the two upper hydrostatic shaft bearings by hydrodynamic bearings, thus saving the high pressure system which had to provide the lubrication water for the old bearings In order to apply vibration monitoring to these pumps, the existing concept had to be modified because of the following facts

- due to the geometry of the pump rotors there are only small radial bearing forces acting for stabilization,
- therefore, in connection with the hydrodynamic bearings the so called whirl is of substantial importance,
- after pump shut down and pump switch on new vibration levels will appear, which are statistical by scattering

To control reactor power the pump speed is variable, this make frequency selective monitoring more difficult

Considering these facts and performing careful analysis of data gained from the factory testing of the pumps, the diagnosis system requirements have been developed

ANNEX

COUNTRY REPORTS

A FUZZY CONTROLLER FOR NPPs

G H SCHILDT
Vienna University of Technology,
Vienna, Austria

Abstract

A fuzzy controller for safety related process control is presented for applications in the field of NPPs The size of necessary rules is relatively small Thus, there exists a real chance for verification and validation of software due to the fact that the whole software can be structured into standard fuzzy software (like fuzzyfication, inference algorithms, and defuzzyfication), real-time operating system software, and the contents of the rule base Furthermore, there is an excellent advantage due to real-time behaviour, because program execution time is much more predictable than for conventional PID-controller software Additionally, up to now special know-how does exist to prove stability of fuzzy controller Hardware design has been done due to fundamental principles of safety technique like watch dog function, dynamization principle, and quiescent current principle

1 INTRODUCTION

Safety critical devices and control systems are used in the field of NPPs Up to now there is a certain threshold to apply software driven systems, because software will never be error-free But, nevertheless all over the world engineers are looking for new approaches to use software driven systems for vital process control To describe safety critical systems at first some terms of safety technique shall be introduced

- *Safety critical system:* control system causing no hazard to people of material in case of environmental influence or system failure
- *Safety:* property of an item to cause no hazard under given conditions during a given time, i e avoidance of undue fail conditions (e g Undue fail conditions may be caused by technical system failures or malfunction of an electronic device interfered by electromagnetic noise)
- *Hazard:* state of a system that cannot be controlled by given means and may lead to damages to persons
- *Safe system state:* property of a system state to cause no hazard to people or material
- *Fail-safe.* technical failures within an item may lead to fail states, which however have to be safe

In the field of NPPs items can be classified as follows

- Those structures, systems and components whose malfunction or failure could lead to undue exposure of the site personnel or members of the public This includes successive barriers set up against the release of radioactivity from nuclear facilities
- Those structures, systems and components, which prevent anticipated operational occurrences from leading to accident conditions
- Those features, which are provided to mitigate the consequences of malfunction or failure of structures, systems or components

Because up to now no fail-safe one-channel computer for vital process control is available, one has to choose a configuration of at least two computers running in parallel In this system configuration results of both channels are to be fed to a fail-safe comparator, whose output enables a safe gate in case of equivalent results, represented by corresponding command telegrams to be fed to the technical process Because of availability aspects one normally applies a three-channeled system with (2 of 3)-voter, so that the system configuration normally runs with all three channels in parallel, in case of failure or maintenance of one channel a *degraded mode of operation* is possible

Additionally, diversity principle could be applied in the field of NPPs Diversity may be defined as follows "Existence of different means of performing a required function" (e g different physical principles, different ways to implement the same task, different algorithms) [1]

Basically, there are typical problems due to diverse system design like

- *Sufficient diversification* within a n-version system (to be proved)
- *Unpredictable waiting times* for results/command telegrams that are to be compared
- *Certain tolerance zone management* when comparing measured values, results, or command telegrams

Therefore, it is an essential challenge to design a one-channeled software system running on a three-channeled hardware in order to manage hardware failures or electromagnetic interference

2 FUZZY CONTROLLER

We designed a fuzzy controller with an architecture as displayed in Fig 1 At the input side, there is a *condition interface* producing *fuzzy equivalents* of several input variables They are then subjected to an inference engine cooperating with a rule base The outputs from the *inference engine* are *fuzzy results* provided to an *action interface*, which finally performs defuzzyfication and process actuation

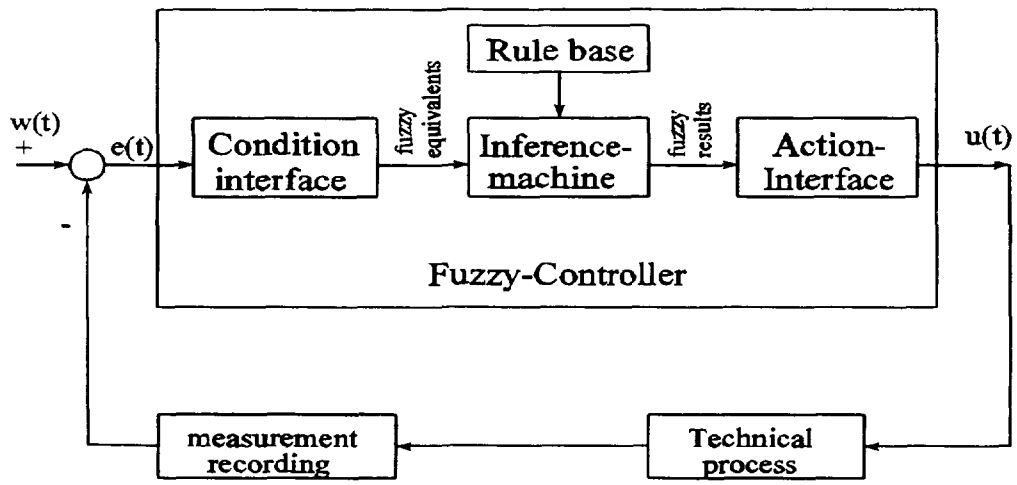


Figure 1: Block diagram of a programmable fuzzy controller

Analog input signals, such as temperature, pressure, water level are provided to the controller, however not directly, but in form of control errors, i e , differences between actual measured values and desired values For reasons of algorithmic simplification in the controller and in order to use proven hardware as widely as possible, these differences are determined in analog form with operational amplifiers [2]

2.1 Fuzzyfication process

The control errors are then fed to the condition interface, whose function is to fuzzify the input values Since mappings from these input data to values of fuzzy variables can be freely selected, we choose triangular membership functions because of simple description in a read only memory (ROM) (see Fig 2)

Grade (of membership)

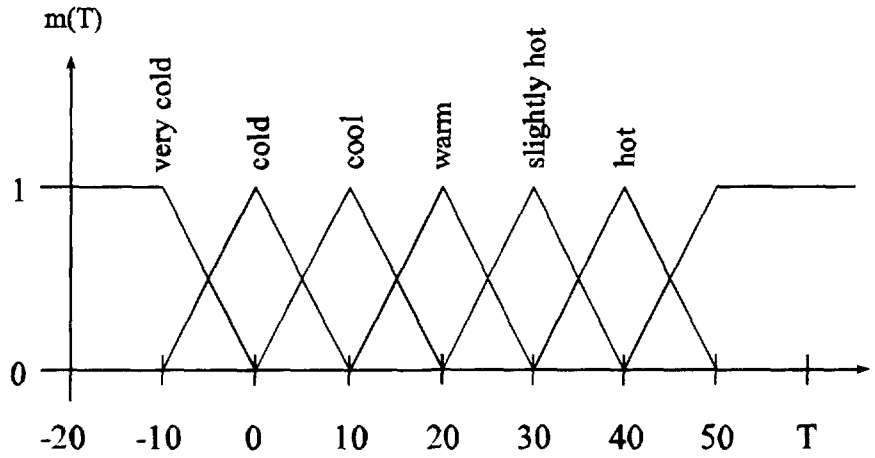


Figure 2: Membership functions (e.g. for temperature T)

If one uses simple triangles, they are easy to describe in source code For example , a value P_LARGE the description can be written as (@0 6, 0, @1 0, 1, @1 4, 0), and for ZERO the description can be written as (@-0 3, 0, @0 0, 1, @0 3, 0), and so on Note that all values of variables here are normalized into the range of /-1,1/ or /0,1/

2.2 Inference engine

The main component of the controller is the *inference engine.* It is operated under a strictly cyclic regime, such as in a *programmable logic controller* (PLC) In contrast to the latter, however, each loop execution takes exactly the same time, because the same operations are carried out in every iteration Thus, the controller's real-time behaviour is fully deterministic and easily predictable Every loop execution comprises three steps (1) input data generation by analogue-to-digital conversion in the condition interface, (2) inference by determine appropriate control rules and (3) control actuation via digital-to-analog converters in the action interface These steps as well as the overall operation cycle are strictly synchronized with a system clock

2.3 Rule base

The rule base contains a set of rules R_1, R_2, , R_n These rules form the *expert knowledge* how to control the technical process and can be described as follows

R_k IF $p_k(e)$ THEN $c_k(u)$

with p_k premise
c_k conclusion
e error
u output value

Necessary adaptation of fuzzy controller towards a technical process may be done by modifying the contents of the rule base Additionally, there is a real good chance of *tuning* the real-time behaviour of the controller by modifying defined membership functions There is an essential advantage of applying a fuzzy controller because of its predictable real-time behaviour Instead of calculation of high sophisticated differential equations one or more rules may fire Due to a certain strategy conclusions can be derived easily

Another essential advantage is the transparency of the rule base, so that even an expert without any background in computer science is able to validate the rule set

The rule set should be implemented as ROM or PROM for safety reasons A special development platform was used to generate a *definition section* and *rule base section* [3] Fig 3 shows both sections for an example of a combined temperature-steam pressure controller

FIU Source Code

```
$ FILENAME          temp/temp3 fil
$ DATE              09/18/1992
$ UPDATE              09/23/1992

$ Temperature controller  Three inputs, two outputs
$   INPUT(S)        Error, Var(iationOf)_Error, Pressure
$ OUTPUT(S)         Var(iationOf)_Heater, Var(iationOf)_Cooling(Valve)


$ FIU HEADER
fiu tvfi (min max)*8,


$ DEFINITION OF INPUT VARIABLE(S)
invar Error " "   -1 0 () 1 0 [
    P_Large             (@0 6, 0, @1 0, 1)
    P_Medium            (@0 3, 0, @0 6, 1, @1 0, 0)
    P_Small             (@0 0, 0, @0 3, 1, @0 6, 0)
    Zero                (@-0 3,0, @0 0, 1, @0 3, 0)
    N_Small             (@-0 6,0, @-0 3,1, @0 0, 0)
    N_Medium            (@-1 0,0, @-0 6,1, @-0 3,0)
    N_Large             (@-1 0,1, @-0 6,0)

    ],
invar Var_Error " "   -1 0 () 1 0 [
    P_Large             (@0 6, 0, @1 0, 1)
    P_Medium            (@0 3, 0, @0 6, 1, @1 0, 0)
    P_Small             (@0 0, 0, @0 3, 1, @0 6, 0)
    Zero                (@-0 3,0, @0 0, 1, @0 3, 0)
    N_Small             (@-0 6,0, @-0 3,1, @0 0, 0)
    N_Medium            (@-1 0,0, @-0 6,1, @-0 3,0)
    N_Large             (@-1 0,1, @-0 6,0)

    ],
  invar Pressure " "   0 0 () 1 0 [
    Large                 (@0 5, 0, @1 0, 1)
    Medium              (@0 0, 0, @0 5, 1, @1 0, 0)
    Small                 (@0 0, 1, @0 5, 0)
    ],


  $ DEFINITION OF OUTPUT VARIABLE(S)
  outvar Var_Heater " "   -1 0 () 1 0 * (
    P_Large             = 0 8,
    P_Medium            = 0 4
    P_Small             = 0 2
    Zero                = 0 0
    N_Small             = -0 2
    N_Medium            = -0 4
    N_Large             = -0 8

    ),

  outvar Var_Cooling " "   -1 0 () 1 0 * (
    P_Large             = 0 8,
    P_Medium            = 0 4
    P_Small             = 0 2
    Zero                = 0 0
    N_Small             = -0 2
```

```
N_Medium        = -0 4
N_Large         = -0 8
),
```

$ RULES

```
if Error is P_Small   and Var_Error is N_Large    and Pressure is Large    then Var_Coolmg is Zero,
if Error is P_Small   and Var_Error is N_Medium   and Pressure is Large    then Var_Heater is H_Medium,
if Error is P_Small   and Var_Error is N_Medium   and Pressure is Large    then Var_Coolmg is Zero,
if Error is P_Small   and Var_Error is N_Small    and Pressure is Large    then Var_Heater is N_Small,
if Error is P_Small   and Var_Error is N_Small    and Pressure is Large    then Var_Coolmg is Zero,
if Error is P_Small   and Var_Error is N_Large    and Pressure is Medium   then Var_Heater is N_Small
if Error is P_Small   and Var_Error is N_Large    and Pressure is Medium   then Var_Coolmg is Zero,
if Error is P_Small   and Var_Error is N_Medium   and Pressure is Medium   then Var_Heater is N_Small
if Error is P_Small   and Var_Error is N_Medium   and Pressure is Medium   then Var_Coolmg is Zero
if Error is P_Small   and Var_Error is N_Small    and Pressure is Medium   then Var_Heater is Zero
if Error is P_Small   and Var_Error is N_Small    and Pressure is Medium   then Var_Coolmg is Zero
if Error is P_Small   and Var_Error is N_Large    and Pressure is Small    then Var_Heater is Zero
if Error is P_Small   and Var_Error is N_Large    and Pressure is Small    then Var_Coolmg is Zero,
if Error is P_Small   and Var_Error is N_Medium   and Pressure is Small    then Var_Heater is Zero

if Error is P_Large   and Var_Error is P_Medium   and Pressure is Large    then Var_Coolmgs is N_Large,
if Error is P_Large   and Var_Error is P_Small    and Pressure is Large    then Var_Heater is P_Medium,
if Error is P_Large   and Var_Error is P_Small    and Pressure is Large    then Var_Coolmgs is N_Large
if Error is P_Large   and Var_Error is P_Large    and Pressure is Medium   then Var_Heater is P_Large,
if Error is P_Large   and Var_Error is P_Large    and Pressure is Medium   then Var_Coolmgs is N_Large,
if Error is P_Large   and Var_Error is P_Medium   and Pressure is Medium   then Var_Heater is P_Large,
if Error is P_Large   and Var_Error is P_Medium   and Pressure is Medium   then Var_Coolmgs is N_Large,
if Error is P_Large   and Var_Error is P_Small    and Pressure is Medium   then Var_Heater is P_Large
if Error is P_Large   and Var_Error is P_Small    and Pressure is Medium   then Var_Coolmgs is N_Large
if Error is P_Large   and Var_Error is P_Large    and Pressure is Small    then Var_Heater is P_Large,
if Error is P_Large   and Var_Error is P_Large    and Pressure is Small    then Var_Coolmgs is N_Large
if Error is P_Large   and Var_Error is P_Medium   and Pressure is Small    then Var_Heater is P_Large,
if Error is P_Large   and Var_Error is P_Medium   and Pressure is Small    then Var_Coolmgs is N_Large
if Error is P_Large   and Var_Error is P_Small    and Pressure is Small    then Var_Heater is P_Large,
if Error is P_Large   and Var_Error is P_Small    and Pressure is Small    then Var_Coolmgs is N_Large
```

FIG. 3. Definition section and rule base section.

We found that for sufficient process control the size of rule base is limited to a bounded number of rules (e g 85 rules only) This is an essential advantage for V&V process

2.4 Defuzzyfication process

Because an actuator needs a discrete value for operation, a certain defuzzyfication strategy has to be applied Usual methods of defuzzyfication are

MAX_HEIGHT
MEAN_OF_MAXIMA
CENTER_OF_GRAVITY

We decided to implement the *center of gravity strategy* because of its efficient control behaviour [2]

3 SAFETY FEATURES OF FUZZY CONTROLLER

In safety technique there exist certain fundamental principles like *dynamization principle, monitoring function, watchdog function, quiescence current principle.*

So, we decided to implement these principles into our design for a safety-critical fuzzy controller After input values have been transformed to fuzzy values by *fuzzyfication process* a certain scanner checks, if one or more rules fire In case of an unplanned stop of the scanner the *dynamic monitoring component*

consisting of a very simple and passive hardware disables a safe gate so that no command telegrams are fed to the technical process (see Fig 4)

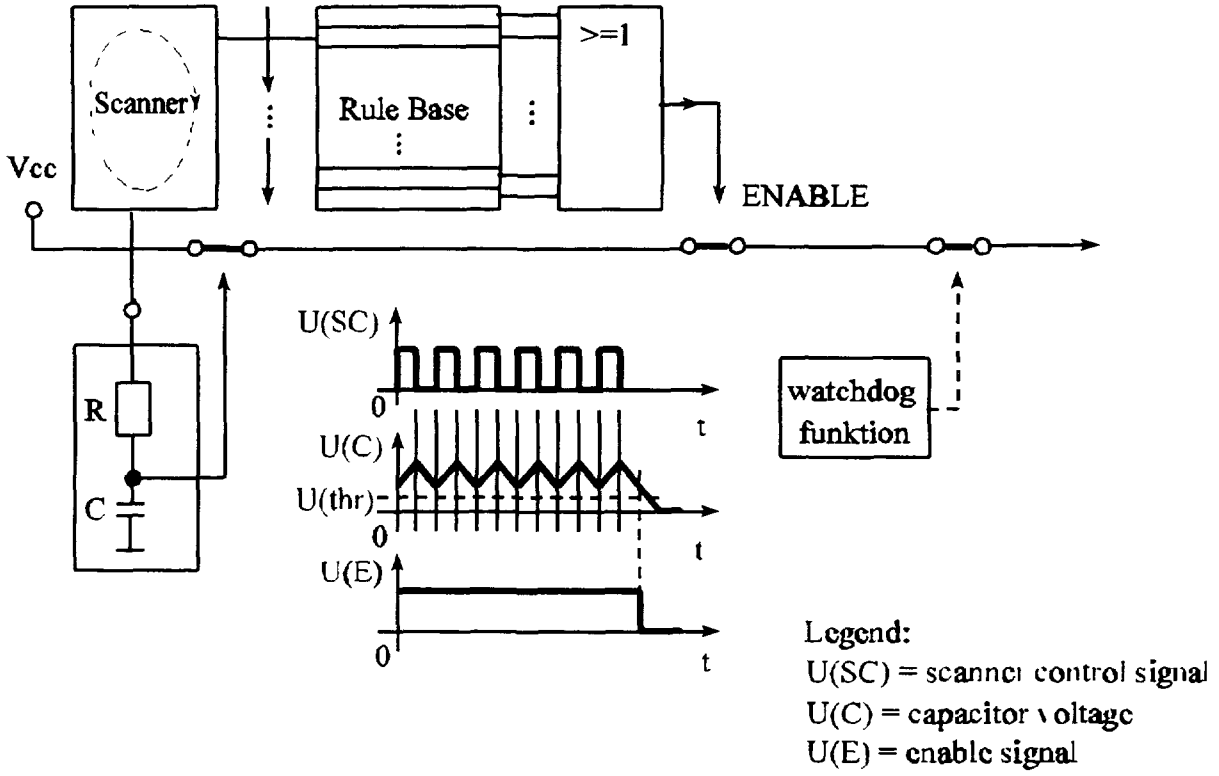


FIG. 4. Safety components for a fuzzy controller.

An additional *watch dog function module* disables a safe gate due to topped scanner or because no rule has fired at all after a well-defined time interval Thus, the technical process changes over to a well-defined safe system state *(shutdown)* As much as possible detailed functions have to be implemented in simple and passive hardware for V&V reasons

4 V & V ASPECTS

Because it is not possible to implement the whole functionality in hardware a one-channeled software remains that has to be validated Fig 5 shows the necessary software structure comprising the *Operating System Software*, the so-called *Standard Fuzzy Software*, and a *Rule Base*. Operating system software and standard fuzzy software have to be validated only once, however for each new application one needs a V&V licensing process for the rule base

5 CONCLUSIONS

A fuzzy controller for safety critical process control has been described We implemented fundamental principles of safety technique like *dynamization principle, monitoring function*, and *watch dog function* into a special fuzzy controller design Hardware and software aspects have been discussed We see not only better chances for V&V process, but also a better real-time behaviour of such a knowledge based system Up to now some theoretical knowledge for *stability proof* is available so that we see a real good chance for applying a fuzzy controller in the field of safety critical process control

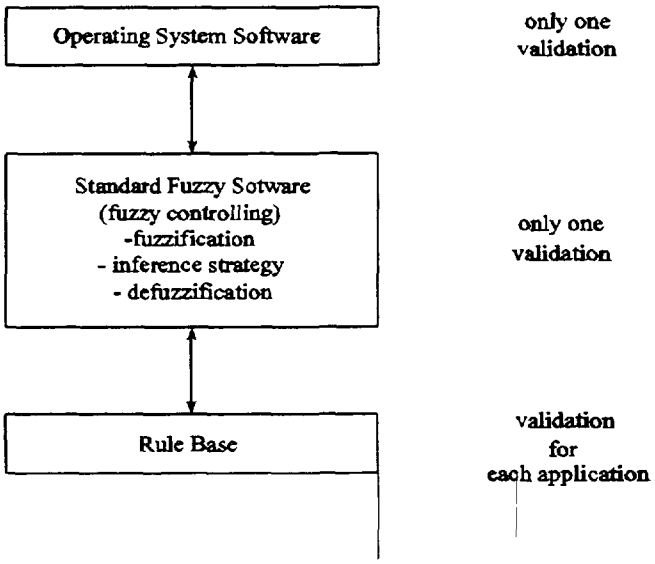


FIG. 5. Software structure of safety critical fuzzy controller.

REFERENCES

[1] Schildt, G H , "On Diverse Programming for Vital Systems"
IFAC, Proceedings on Safety of Computer Control Systems (1989).

[2] Schildt, G.H., "Safety Critical Application of Fuzzy Control",
IFSA 95, Sao Paulo, Brasil, (1995).

[3] APTRONIX INC "FIDE Application Note 006-920914", San Jose, CA, USA (1992)

EXPERIENCE WITH DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS FOR CANDU POWER PLANT MODIFICATIONS

S BASU
Ontario Hydro,
Canada

Abstract

Over the last ten years, Ontario Hydro CANDU power plants have gone through many modifications This includes modification from analog hardwired controls to digital and solid state controls and replacement of the existing digital controls with the latest hardware and software technology Examples of digital modifications at Bruce A and other CANDU power plants are briefly described and categorized. Most of the I&C technology development has been supported by the CANDU Owners Group (COG) a consortium of Canadian nuclear utilities and the Atomic Energy Canada Limited (AECL)

1 INTRODUCTION

Over the last ten years, Ontario Hydro CANDU power plants have gone through many modifications This includes modification from analog hardwired controls to digital and solid state controls and replacement of the existing digital controls with the latest hardware and software technology The digital hardware and software have become major components in the operation of CANDU power plants for control, monitoring, display, alarm, data acquisition and report generation The modification projects involved rigorous efforts in product specification, hardware qualification, software design, configuration management, testing, verification, validation and commissioning checks

Many digital Instrumentation and Control (I&C) systems make use of micro computers with both predeveloped software and custom software All Ontario Hydro's nuclear plants (Bruce A, Pickering A&B and Darlington) use quality engineering procedures and standards in compliance with regulatory requirements, codes and industry standards The quality assurance program for digital I&C modifications has become more stringent, especially for the safety critical applications One major requirement is to have proper software categorization based on the criticality of the functions performed by the software In general, the software category defines the degree of rigour required for the software engineering process as well as the licensing scrutiny by the regulators

2 EXAMPLES OF BRUCE A DIGITAL MODIFICATIONS

2.1. Category I Modifications

- *PHT Pump Automatic Trip (P-Trip)*

P-Trip protects the primary heat transport (PHT) piping and pump supports from pump induced vibration The system consists of two identical Fischer and Porter Microprocessors (Programmable Controllers), process I/O and software within the PHT Auto Trip system The input signals are suction pressure, discharge pressure and reactor power conditionings

2.2. Category II Modifications

- *Digital Computer Control (DCC)*

DCC modification comprised of replacement of the Varian V-72 computer with Second Source Computers Inc (SSCI)-890 hardware and relocation and enhancement of the display and data recording functions on to a new Plant Display System The SSCI-890 computer is the modern equivalent of the V-70 series computer Its speed of execution is twice that of the V-72 and supports 8Mb memory compared to 32Kb for the V-72 computers The software was ported from the V-72 to the SSCI-890 with changes made to the Executive software in order to adopt it to the new hardware features while retaining the structure, function and operational features of the original software

- *Standby Generator Control (SGCS)*

SGCS upgrade consisted of replacing the Governor Control Panel with Bailey Infi 90 control system and upgrade of field instrumentation and Local Control Panel The Bailey Infi 90 is a distributed control system (DCS) comprising hardware from Bailey and Electronics Technology Systems Inc The Multi-Function Processors of Infi-90 are microprocessor based and provide the control logic for fuel control, sequencing, data acquisition and annunciation functions The system is configured using the Bailey Engineering Work Station and then loaded and stored on the industrial hardened computer's hard-drive

- *Fuel Handling Computer*

Software changes were made to the PDP-14 protective computer used for the control of the fuel handling system Changes were also made to the PDP-8 control computer The modifications were made to change the direction of fuelling in the fuel channels, that is, fuelling with flow

2.3. Category III Modifications

- *Plant Display System (PDS)*

The PDS system is a replacement and enhancement of the existing operator interface for the existing Digital Control Computers and Safety Systems Monitoring Computers The PDS is a dual redundant network of Sun SPARC10 Unix Workstations with high resolution colour monitors and colour X window terminals for annunciation Careful selection of components provides a robust system with functionally equivalent components available well into the future and expandability to meet future requirements

- *Safety System Monitoring Computer (SSMC)*

SSMC modifications comprised of replacement of the existing Data Acquisition System (DAS) and Monitor Computer (MC) The DAS supplied by VME Microsystems International is composed of MVE 162-223 Embedded controller with firmware The DAS accepts the input signals from the safety system field instrumentation and sends signals to the Control Room annunciation One DAS exists for each channel of each safety system The monitor computer is based on SPARC-10 computer system manufactured by Microsystems Incorporated The primary function of MC is to exchange data with various DASs, communicate this data to and from the Plant Display System and perform alarm detection

- *Turbine Governor Control (TGC)*

TGC retrofit for Parsons turbines comprised of replacing the original controls supplied by GEC-Elliott with Elsag Bailey Infi-90 distributed control system (DCS) The Infi-90 DCS is a microprocessor based digital control system and provides full redundancy for control modules, communication buses and power supplies The hardware configuration provides three distinct partitions for overspeed, valve control and data logging A portable Engineering Work Station is provided to perform on-line tuning, configuration, graphics modification, and the saving and loading of configurations

- *Active Liquid Waste (ALW) Control*

The ALW system was upgraded to add new equipment consisting of Active Drainage Handling, Filtration, Reverse Osmosis and Evaporation-Solidification subsystems Each of the four subsystems is controlled and monitored by its own Modicon Programmable Logic Controller (PLC) and software The subsystem PLCs are linked by redundant communication links

2.4. Category IV Modifications

- *Water Treatment Plant Control*

The new Water Treatment Plant replaced the old water treatment plant Each of the four subsystems is controlled by its own MODICON 984 PLC with MODICON P190 Programmer The operator interface PanelMate Plus made by Eaton IDT Inc provides control or adjust functions of the PLC operations It replaces the conventional panel-mounted controls The PanelMate Plus is configured with DOS-based configuration software with a family of editors

- *Generator Hydrogen Cooling Temperature Control*

The Bristol Babcock series 624 Pneumatic Temperature Controller was replaced with Fischer & Porter (F&P) series 5000 microprocessor based temperature controller The F&P controller is configured using the floppy disc (F&P software) and a 386 personal computer

- *Mini SLAR*

A computer based tool was developed to locate and reposition garter springs between the pressure tubes and the calandria tubes for the fuel channels

2.5. Not Yet Categorized Modifications

- *Gaseous Fission Products (GFP) Monitor*

GFP system is provided to continuously monitor the concentration of certain fission products in the primary coolant (PHT) for indication of the fuel bundle failure The upgrade consists of replacing the existing PDP-11 computer and associated devices with integrated signal processor and PC based field computer The field computer performs multichannel analysis, data processing and sends the field data to a central computer for processing The system was configured using the pre-developed application software and in-house custom software

- *Unit Stack Effluent Monitor*

The unit stack monitor, supplied by Sorrento Electronics, performs on line monitoring of stack effluents (particulate, Iodine and noble gases) The conversion of electrical energy pulses to activity counts is done by RM-80 microprocessor The RM-80 also processes the flow rate input from the stack to maintain isokinetic sampling process The microprocessor is also equipped with a terminal where a portable readout device can be connected to collect data

- *Core Discharge Monitor (CDM)*

The core discharge monitor provides safeguards accountancy of the fuel bundles as they enter and discharge from the reactor core CDM is a microprocessor based data logger to log output signals from the detector devices and transmit logged data via telephone modem for remote monitoring

3 EXAMPLES OF OTHER CANDU MODIFICATIONS

3.1. Category I modifications

- *Pickering B digital trip meter*

Primary Heat Transport (PHT) temperature trip modification comprised of replacing the current analog type trip meters with digital trip meter jointly developed by Dixon Inc and Ontario Hydro The meters are microprocessor based with A/D converters EPROM stores configuration data, while EEPROM stores trip and alarm setpoints There are 5 discrete LEDs on the panel to indicate status of the trip, alarm, fault and display conditions

3.2. Category II modifications

- *Pickering A digital control computer(DCC)*

The DCC IBM 1800 computers are being replaced with clones But the original software is being retained

4 IMPORTANT ISSUES

During the modification process, the important issues identified for the digital I&C are

- Equipment Qualification for EMI and RFI
- Environmental Qualification
- Hardware Qualification
- Software Categorization
- Software Qualification
- Human Factor Evaluation
- Software Development. Verification and Validation
- Regulatory Acceptance

5 TECHNOLOGY DEVELOPMENT

Most of the I&C technology development has been supported by the CANDU Owners Group (COG) a consortium of Canadian nuclear utilities and the Atomic Energy Canada Limited (AECL) To meet the timely needs of the I&C modifications COG reports were produced to handle many of the issues including guidelines for hardware qualification, software development, software categorisation and qualification of pre-developed software The COG research and development programs are continued at AECL based on the needs identified by the utilities

TOWARDS FUNCTIONAL SPECIFICATION INDEPENDENT OF CONTROL SYSTEM SUPPLIERS

D. GALARA, E. LERET
Electricité de France,
Research and Development Division, Power Plant Control Branch
Chatou, France

Abstract

For the next nuclear power plant generation, REP 2000, the Engineering and construction Division (ED) and the Research and development Division (R&D) of Electricité de France are working together in the field of Instrumentation and Control (I&C) to improve its engineering method and tools. This method and these tools are defined on the basis of the experience feedback from the N4 nuclear power plant generation and the current information technology, to improve engineering competitiveness and quality of control applications. We intend to decouple the I&C processing from the I&C Human Machine Interface (HMI), because methods and tools are different. In this paper, we only focus on method and tools for I&C processing. We define the I&C processing life cycle into three phases. The first phase is the specification of the control application processing, the product of which is called Functional Requirement Diagrams (FRDs). The second phase is the design of the I&C system. This phase is subdivided into two steps. The step 1 is the distribution of the FRDs into an I&C architecture. The step 2 is the allocation of resources of the I&C system, to support the distributed FRDs. The third phase is the implementation of the distributed FRDs into I&C equipment. The aim of the Engineering Division is to achieve formal FRDs, independent of I&C suppliers. This allows a large improvement for the quality of the specification and the dimensioning of the I&C system before calls for tenders. For the specification phase, studies are almost completed. For the design and the implementation phases, studies and experiments are in progress with European I&C system suppliers. As a conclusion, we present the interest of EDF for standards and especially IEC 1131 improvements.

1. LIFE CYCLE OF THE I&C PROCESSING

The I&C processing life cycle should be summarized according to the following Fig. 1.

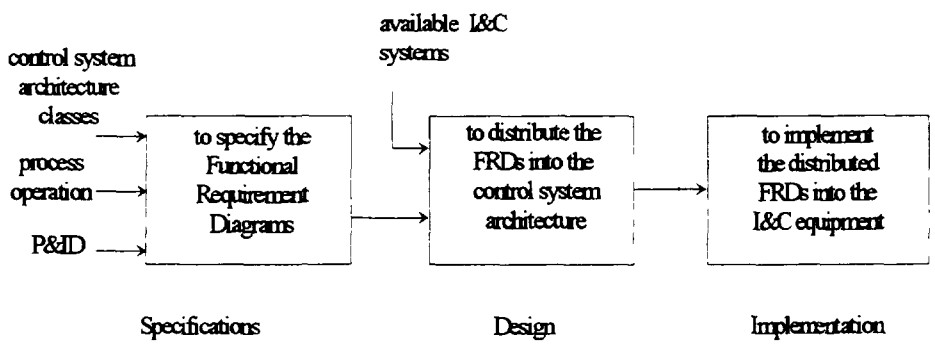


FIG. 1. Control processing life cycle.

In this life cycle, we can distinguish the following major phases:

- The specification of a control processing application the result of which are the FRDs.
- The distribution of the FRDs into a selected I&C architecture.
- The implementation of the distributed FRDs into I&C equipment.

The specification of a control processing application is carried out from the Process and Instrumentation Diagrams (P&ID), describing the process mechanical parts the remote transmitters and actuators, and a textual description of the process operation describing start up, normal and abnormal operation, and shut down The result of the specification of a control processing application are FRDs including performance constraints like time, safety and availability

For the design of the I&C system, we have to complete the formal description of the FRDs Then, the design is made in two steps First, the FRDs are distributed into an overall I&C system architecture Second, the I&C resources are allocated to support the distributed FRDs

The last phase is the implementation of the distributed FRDs into the I&C equipment

2 SPECIFICATION OF A CONTROL PROCESSING APPLICATION, THE FRDS

The FRDs are the specifications of a control processing application FRDs are composed of a set of control functions depending on the process under control, with attached functional performance constraints

2.1. Identification of control functions

There are different types of control functions composing FRDs

- measurement control functions delivering process measurements,
- control functions
  - open loop control functions controlling actuators,
  - closed loop control functions, single or cascade, controlling process phenomenon,
  - sequence control functions, co-ordinating down-stream control functions

For the specification of a control processing application, we have, first, to identify control functions, second, to specify the control functions

Let us take a simple example of a process composed of a tank feeding three pumps From the P&ID and the description of the operation, we can identify two control functions

- *Control function 1*: to maintain the level of water in a tank The level of the tank is delivered from a level measurement A closed loop control actuates a control valve feeding the tank and maintaining the level of water to a setpoint
- *Control function 2:* to feed water a down stream circuit Two among three pumps are feeding a downstream circuit In case of trouble with one of the two operating pumps, the third redundant pump will be switched on to maintain feeding water of the down stream circuit

Once the control functions have been identified, and the operation is described with text, we have to specify these two control functions with a neutral engineering function block language This language is independent of any programming language, to avoid being in favour of any supplier However, the control functions, described with the engineering language, are implementable into I&C systems

2.2. Engineering function block language

The characteristics of the ED neutral engineering function block language are

- it is a process control-driven language, it is not an implementation language,
- it must be built on standard foundations,
- it must be built on standardized blocks, but the standard must also provide construction rules allowing the definition of application blocks (energy, manufacturing, chemical) implementable into I&C equipment,

- the independence of a neutral engineering language allows the Engineering Division to reuse studies for other control systems, whatever the type of control system compliant with the standard is

Describing the FRDs using a neutral engineering language doesn't mean to describe the FRDs without taking into account the capabilities of the control equipment available on the market It means to define an engineering language satisfying Engineering Division needs, being compatible with international standards and implementable into I&C systems

In order to specify control functions with the engineering function block language, we need different types of blocks gathered in two libraries A library of Elementary Function Blocks (EFBs) which are basic logical mathematical operators A library of Application Function Blocks (AFBs) depending on the control application, for example switchover 2/3, measurement and actuation function blocks Each block is defined with an internal and an external view

The external view is a graphic symbol representing a block. The external view is used to describe graphically the specification of any control functions

- An EFB is summarized with a graphical representation on which we have standardized and optional inputs and outputs, and a symbol (graphic or text) to summarize the internal processing
- An AFB is summarized with a graphical representation on which we have standardized and optional inputs and outputs, a graphical symbol summarizing the application, optional symbols (graphic or text) for the different types of operator interfaces with the different types of commands and optional textual characteristics

The internal view is the description of the behaviour of a block:

- An EFB should be a standardized block from a standard As most of these process control EFBs are not in conformity with the IEC 1131, these EFBs have been partially described with the ST language of IEC 1131,
- An AFB should be
  - network of EFBs or should be described with a standardized formal language (an improvement of Structured Text of IEC 1131), if this description does not stick to I&C technological constraints,
  - a textual description, if the description depends on technological constraints

We point out that measurement and actuation AFBs include all the processing from the process interfaces (signals from switches or transmitters and commands to power interfaces) up to operator interfaces (Turn Push Light management for example)

2.3. External view of the FRDs

For the specification of a control function, we have to describe

- The control function inputs
  - the set of observations (from measurement or from other control functions) the control function will process,
  - the set of requests (from operators or from other control functions) the control function will process,
- The control function outputs
  - the set of reports (to the operators or to other control functions) the control function will deliver,
  - the set of actions (to actuation or to other control functions) the control function will deliver,

- The behaviour of the control function, described with EFBs and AFBs using the engineering graphical function block language.
- The performances of the control function:
  - time constraints such as ordering of the function blocks processing, sampling time for measurement or for control loops, response time between operator command and actuator power interface, response time between alarm detection and protection operation;
  - availability constraints such as requiring the implementation of each pump actuation function block into a different control equipment, or to require the implementation of control functions into different control equipment;
  - safety constraints such as requiring the implementation of each pump actuation function block into a different control equipment with separated power supplies.

On the following Fig 2, we have specified the two previous control functions of our example with the engineering function block language, taking advantage of the external views of the AFBs and EFBs.

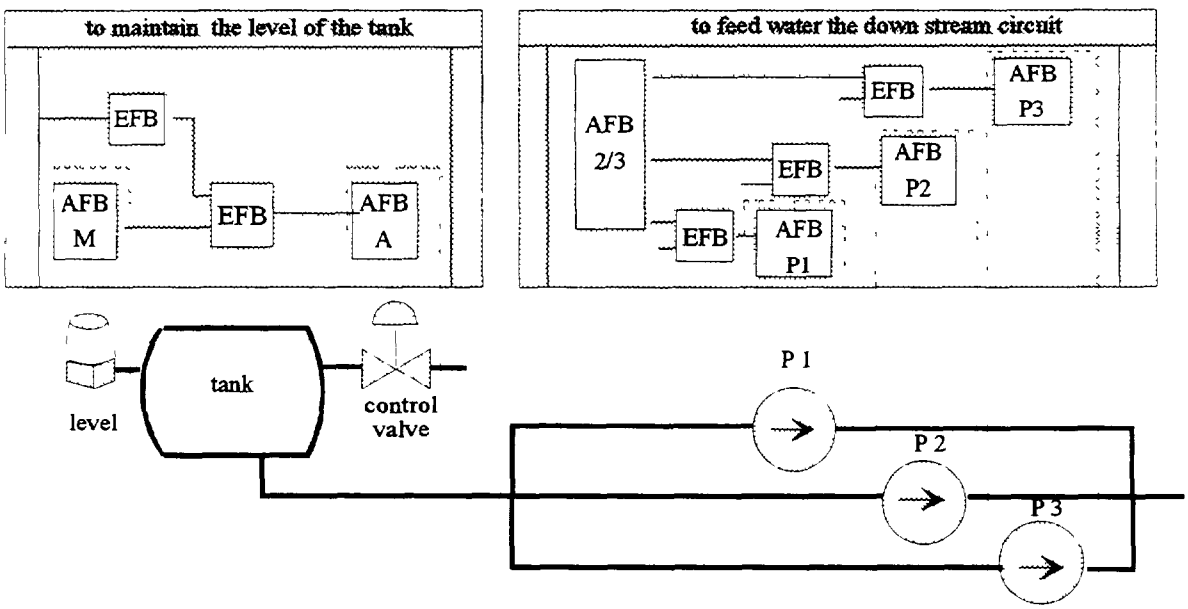


FIG. 2. External view of control functions.

The FRDs are the control functions, they are described using the engineering function block language, with the attached performances. At this stage, we point out that some AFBs are not formally described because they are depending on technological constraints.

To summarize, the FRDs are purely functional, they represent the logic to control a process; the protection loops, the open and closed control loops, the sequences. They also include the logic of alarm processing, the information and the actions under control of operators. Even if the FRDs are depending on the technology support, they are not depending on any I&C supplier.

3. COMPLETION OF THE FRDS: INTERNAL VIEW OF THE FRDs

To complete the formal description of the FRDs means to complete the internal formal description of the AFBs depending on the technological constraints The technological constraints of an AFB are depending on a selected class of application (classes are based on safety or availability goals),

For a nuclear power plant control application, the overall I&C architecture is composed of different I&C systems according to the different classes, for example within the overall I&C architecture we have a safety I&C system, an I&C system important for plant availability and a non classified I&C system Within each I&C system we have different layers For example, the layer 0 is dedicated to the power interfaces, layer 1 to the I&C processing and layer 2 to HMI The content of a layer is depending on the class of application

Within the overall I&C architecture, for each AFB we have to explicit its class and its local I&C architecture, in particular for measurement and actuation AFBs

The distribution of the FRDs is made taking into account

- on one hand, the application classes required in the FRDs But distributing the FRDs does not mean to code the I&C equipment, it means to distribute the control functions into these I&C systems and layers,
- on the other hand, the capabilities and the time performance constraints of the selected I&C equipment (processing, data exchanges, etc)

Each control function is a network of function blocks (EFB, AFB) In consequence, distributing a control function means to distribute each function block of the control function into the selected I&C system and layers, with respect to the class of application

Doing that, the following rules must be respected

- EFBs (which are elementary logic-mathematical operations) are distributed into a single layer,
- AFBs (which are composed of internal blocks) can be distributed into different layers, as summarized on the Fig 4 for the actuation function block example

Let us take the example of an actuation AFB When we select a class of application for an AFB, in fact we select a class of I&C equipment and implicitly we select a local actuation architecture with different layers, the Motor Control Centre (MCC) for layer 0, the actuation control processing for layer 1, the HMI for layer 2

Once the actuation architecture is selected, we have to specify the internal blocks corresponding to each layer, keeping in mind that a block is depending on the dedicated class of I&C equipment

In our example, the actuation AFB is composed of three internal blocks, the MCC, the control and the HMI blocks, depending on the safety class, as summarized on Fig 3

Distributing an AFB into an I&C architecture means to cut the AFB into different AFB subsets and to distribute these AFB subsets into different layers This distribution will provide

- AFB processing subset needs,
- communication needs between the AFB subsets (the data exchanged between the different AFB subsets) and the up and down stream function blocks of the control function

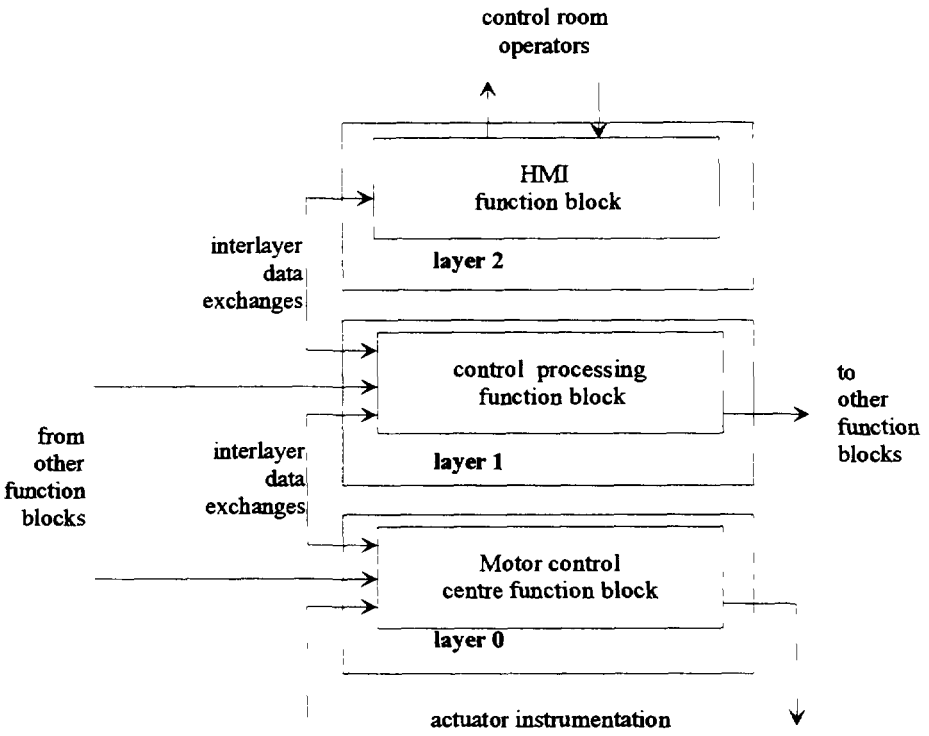


FIG. 3. Internal view of an actuation AFB.

If we don't specify correctly these internal blocks, we may cut internal blocks during the distribution between layers.

Whatever the AFB is, the internal blocks of an AFB are specified with the unique engineering function block language, keeping in mind these blocks are depending on the selected class of application. When the specification of the internal function blocks of the AFB is completed, we have a formal specification of an AFB.

For each AFB of the FRDs we have to select the class, once the class is selected we can formally specify each internal blocks. When all the AFBs of a control function are specified, we have a formal specification of a control function. When all the control functions of the FRDs are specified, we have a formal specification. One can notice that, for a set of FRDs, it is possible to arrange different distributions into the I&C architecture, to optimize the cost and the performance of a distribution. At this stage, we point out that the different layers of the I&C architecture can be supported by equipment from different suppliers.

On the Fig. 4, we have distributed the control function "to feed water the down stream circuit" into three layers of a selected I&C system. All the EFBs and AFBs are distributed into these layers. For this example, all the EFBs and the AFB 2/3 are distributed into the layer 1, the AFB for pump 1, 2 and 3 into three layers. For each layer we have a control function subset.

A point of interest of the formal FRDs is the simulation:

- to validate each application function block;
- to validate each control function, composed of elementary and application function blocks;
- to validate the interworking of the control functions of the FRDs;
- to validate the operation of the FRDs connected to a simulation of the process.

Due to the cost, the validations are carried out taking into account safety, availability, and novelty considerations.

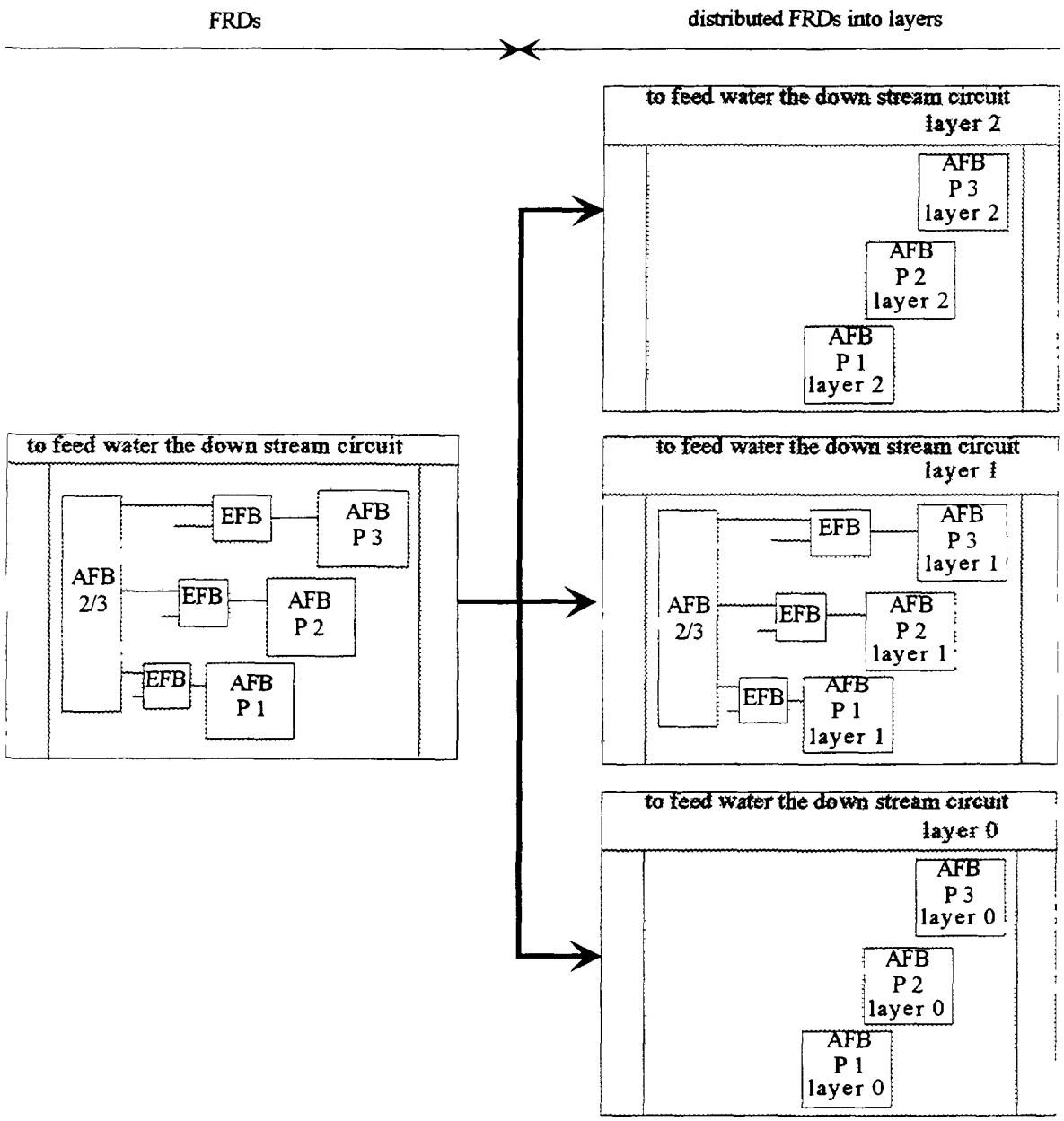


FIG. 4. Distribution of a control function into three layers of an I&C system class.

4 DESIGN OF THE I&C SYSTEM: ALLOCATION OF I&C RESOURCES TO SUPPORT THE DISTRIBUTED FRDs

The allocation of I&C resources to support the FRD subsets is arranged taking advantage of the processing and data exchanges capabilities of the available I&C equipment

For the allocation of the FRD subsets into the I&C equipment, we describe:

- the sizing of the PLCs and the cabinets;
- the system integration of the I&C equipment;
- the impact of the I&C technology on the FRDs.

For the impact of the technology we take into account the mode of operation and the disturbances of the I&C equipment (I/O, CPU and bus hardware failures, different types of reset, processing error recovery, etc) The FRD subsets are completed with additive function blocks depending on the technological constraints. At this stage we point out the difference between FRDs and distributed FRDs

FRDs are purely functional, distributed FRDs are FRDs embedded with technology. For example, we have additive I/O blocks to describe the inputs and outputs hardwired and point to point connected to field devices (digital, analog signals). We have additive serial blocks to describe the digital and analog inputs and outputs exchanged between PLCs through a network. We can also have validation blocks, for example to check congruent switches, to filter switch blinking, to filter analog spike, etc

We also have to take into account the safety and availability constraints. For example, from Fig. 4 we have a control function subset layer 1 with 3 pump actuation under control of a 2/3 switch over. To improve the availability of this control function, we can allocate this control function subset into three PLCs, to avoid a common failure. The 2/3 switchover is also allocated into three PLCs. On the Fig. 5, the control function subset layer 1 is distributed into three I&C equipment.

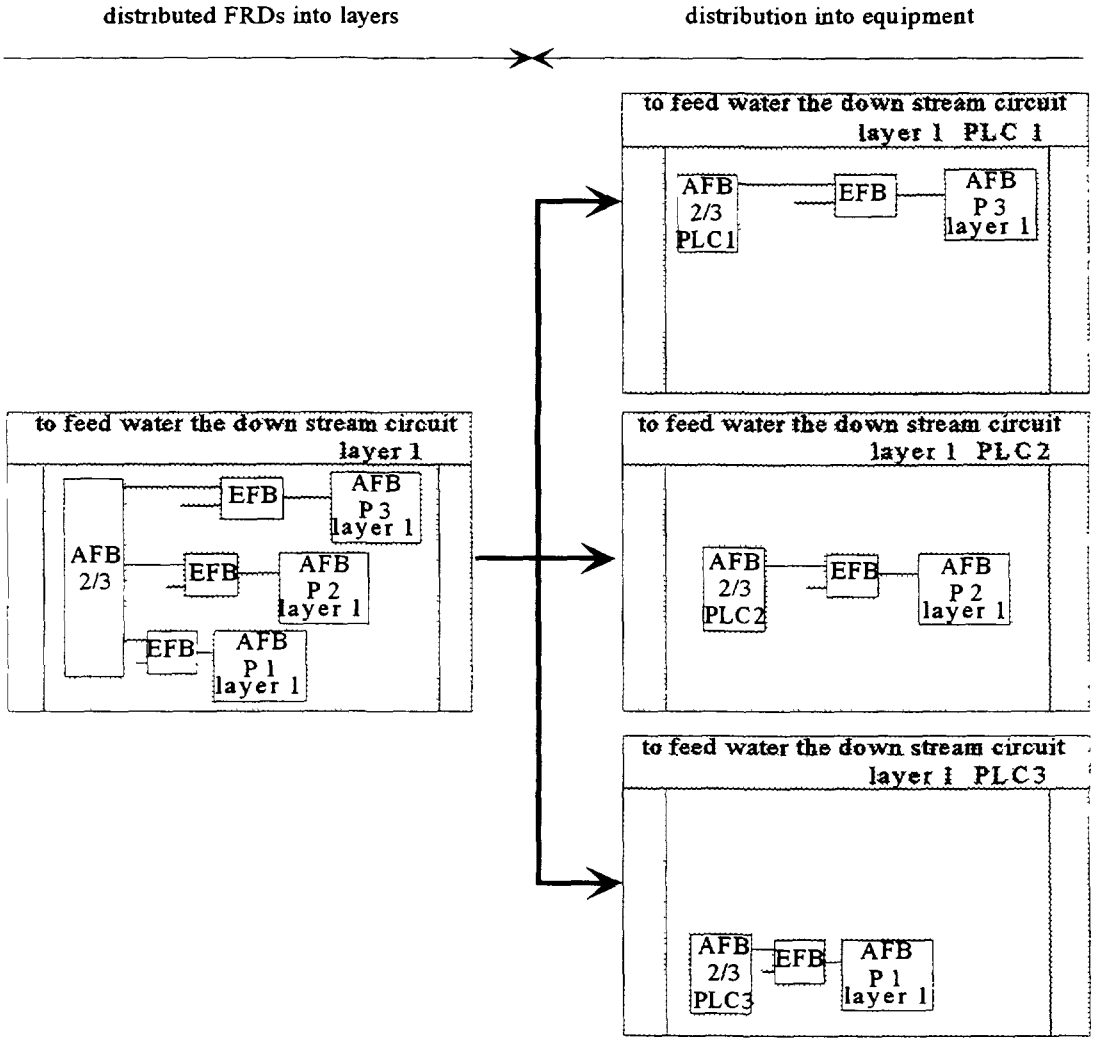


FIG. 5. Allocation of a layer 1 control function subset into PLCs of the layer 1.

Once the allocation is completed, we can size and optimize precisely the PLC's and the cabinets of the I&C system.

To improve the quality of the design, previous hardware qualification tests can be performed on the I&C equipment of the shelves. In addition, previous functional tests allow an evaluation of the processing and data exchanges capabilities the certified I&C equipment

5. IMPLEMENTATION OF THE CONTROL PROCESSING INTO AN I&C SYSTEM

The implementation of the FRD subsets aims at delivering the I&C equipment coded From the distributed FRDs the code generation should be automatic The code is downloaded when the I&C equipment are assembled It means, to fill in the racks of the cabinets with the CPU, I/O, network boards, interconnecting the cabinets and the HMI devices, the power supplies, implementing the distributed FRDs code and commissioning the control application

6 CURRENT EXPERIENCE FEEDBACK

6.1. Specification of FRDs feedback

To achieve formal and non ambiguous description, the EFBs have been described partially with the Structured Text of the IEC 1131 standard The library of the EDF engineering function block is currently composed of 80 EFB These EFB should be part of a standard We need a standard for process control function block in addition to IEC 1131 As this standard doesn't exist, we tried to use the IEC 1131

But, as the IEC 1131 is a programming-driven standard for manufacturing industries, the IEC 1131 standard is not currently adapted for building an EFB library and an engineering function block language Some lacks must be completed

For example, for the EFB variables, we need logical, engineering, percentage and time variables At the specification stage we don't mind about integer, double integer, floating point variables, this is used for programming I&C equipment

For the EFB processing (filters and so on), we don't mind about the algorithms For the specification, we are reasoning in functional terms, it means pure mathematical and physical formulations We need to specify a mathematical formulation, its range of operation and its requested accuracy, whatever the algorithm would be implemented further on

For the AFB processing, we have two cases

- AFB for mathematical processing,
- AFB for standardized applications described as a network of EFBs and mathematical AFBs

For mathematical processing AFBs, we need to specify a direct mathematical formulation instead of a network of mathematical EFBs

For standardized AFBs, we need different levels of "encapsulation" To highlight this need, let's take the example of the actuation AFB described in the previous chapters 3 and 4 Within the FRDs, an actuation AFB is represented as a graphical symbol summarizing all the processing and the inputs and outputs between the actuator instrumentation (for example, the limit and torque switches, the switchgear control) and the operator interfaces (for example, the display and the touch-screen in the control room, on the front panel of the MCC)

When we distribute the AFB into the different layers of an I&C system, we decompose the AFB into three "macroblocks", each "macroblock" is distributed into a specific layer and there are connections between these "macroblocks"

Inside each "macroblock", we have a description of the processing as a network of EFBs

We need a standard for the rules of construction of such a generic mechanism of encapsulation We point out that the AFB can be considered as a specific block, but in fact the AFB is built as a network of standardized EFBs

For the AFB execution, we need standard rules to configure the order of the EFB execution within the "macroblocks" and to configure the order of execution of "macroblocks" execution within AFBs

As control functions are networks of EFBs and AFBs, we also need to configure the order of execution of the blocks within control functions

Last but not the least, as FRDs are networks of control functions, we need to configure the order of execution of the control functions within FRDs

6.2. Distribution of the FRDs feedback

For the distribution of the FRDs into FRD subsets, we need to keep the function blocks execution ordering of the FRD subsets in conformance with the execution ordering specified in the FRDs

For the AFBs, such as actuation and measurement, which are composed of "macroblocks", they are implemented into distributed I&C equipment We need a standard mechanism which maintains the order of execution of the distributed "macroblocks" in accordance with the execution order specified in the AFBs

For the control functions which are composed of networks of EFBs and AFBs, these EFBs and AFBs are implemented into distributed I&C equipment We need a standard mechanism which maintains the order of execution of the distributed EFBs and AFBs in accordance with the execution order specified in the control functions

Last but not the least with the FRDs which are composed of control functions

Within the design, we have to take into account the technological constraints, from the current experimentation, we have currently identified some needs

- definition of a standardized mode of operation for the function blocks initialisation,
- definition of a standardized mode of operation for the function block reset, in particular for time varying function blocks,
- definition of standardized function block error recovery (for example, overflow, underflow, division by zero),
- definition of standardized digital and analog function blocks for inputs and outputs supported by serial multiplexed or hardwired point to point connections

6.3. Neutral files between CAD systems

From the Fig 1, the life cycle is composed of three phases The activities of these phases can be carried out by different companies These companies will exchange application data

From the experimentation feedback, we identified we need neutral file standards to exchange these data between CAD systems In a first case, these data should be exchanged between the specification and the design phase, we need standards

- to export the graphical description of the FRDs (control functions and AFBs),
- to export the internal behaviour of the FRDs (network of EFBs and AFBs for control functions, network of EFBs for AFBs)

In a second case, these data should be exchanged between the design and the implementation phase, we need standards

- to export the graphical description of the distributed FRDs,
- to export the internal behaviour of the distributed FRDs

A standard for the graphical description of the FRDs and the distributed FRDs will allow to achieve a consistent graphical description all along the specification, the design and the implementation phases This is a key point for the quality and the maintenance of the control applications

A standard for the description of the behaviour of FRDs and distributed FRDs will avoid manual translation between the different phases and improve the quality and the maintenance of the control applications

7 CONCLUSION

The needs we have identified are the results of current experimentation still in progress, to prepare the control applications of the future power plants To contribute to the standardization effort, these needs have been delivered and presented to the IEC 65C WG7 "Process Control Function Blocks" It seems that the WG7 is only focusing on the definition of a library of process control EFBs

We point out that applications are becoming more complex, with the introduction of maintenance and technical management needs, delivered for example by intelligent measurements and actuation, in addition to control ones

A standardized library of process control EFBs may be not enough to cope with current application needs In addition to a standard of EFB library, this should force us to standardize rules of construction and representation of AFB and control functions to achieve flexibility and scalability of future control, maintenance and technical management systems, we already need

ADVANCED I&C SYSTEMS FOR NUCLEAR POWER PLANTS

H -W BOCK, A GRAF, H HOFMANN
Siemens AG,
Erlangen, Germany

Abstract

Advanced I&C systems for nuclear power plants have to meet increasing demands for safety and availability Additionally specific requirements arising from nuclear qualification have to be fulfilled To meet both subjects adequately in the future, Siemens has developed advanced I&C technology consisting of the two complementary I&C systems TELEPERM XP and TELEPERM XS The main features of these systems are a clear task related architecture with adaptable redundancy, a consequent application of standards for interfaces and communication, comprehensive tools for easy design and service and a highly ergonomic screen based man-machine-interface The engineering tasks are supported by an integrated engineering system, which has the capacity for design, test and diagnosis of all I&C functions and the related equipment TELEPERM XP is designed to optimally perform all automatic functions, which require no nuclear specific qualification This includes all sequences and closed-loop controls as well as most man-machine-interface functions TELEPERM XS is designed for all control tasks which require a nuclear specific qualification This especially includes all functions to initiate automatic countermeasures to prevent or to cope with accidents By use of the complementary I&C systems TELEPERM XP and TELEPERM XS, advanced and likewise economical plant automation and man-machine-interfaces can be implemented into Nuclear Power Plants, assuring compliance with the relevant international safety standards

1 CONCEPT

A process control system covering all automation tasks in nuclear power plants requires equipment for automation, communication, operator control and monitoring, engineering, diagnosis and maintenance The features of this equipment and the manner in which it interacts characterize the process control system As innovation cycles in software and hardware development become shorter, process control systems will only have any chance on the market in future if they are based on standards because standards usually have a longer life than individual components For this reason the extensive use of standards was determined as fundamental principle of the common concept behind TELEPERM XP and TELEPERM XS

However, because standard components are naturally unable to cover all the requirements specific to power plant I&C, it is necessary to superimpose specific characteristics This is done in a way that is transparent to the user by means of engineering tools which together form an engineering system This allows unrestricted exploitation of the technical and cost advantages associated with the use of standards while enjoying a previously unavailable comfort during engineering, maintenance and diagnosis as well as consistency in documentation

2 ENGINEERING, MAINTENANCE, DIAGNOSIS

The central interface between the equipment for automation, operator control and monitoring, and communication and the personnel responsible for running the I&C system is the engineering system It is an integral part of the I&C system and supports not only engineering tasks but also maintenance and diagnosis of all I&C components, i e both the plant specific software functionality for automation, operator control and monitoring, communication and the hardware functionality of the entire I&C system The most important feature is that all activities - the specification of the control functions as

well at the design of the hardware architecture - can be performed through the same graphic user interface by means of standardized symbols.

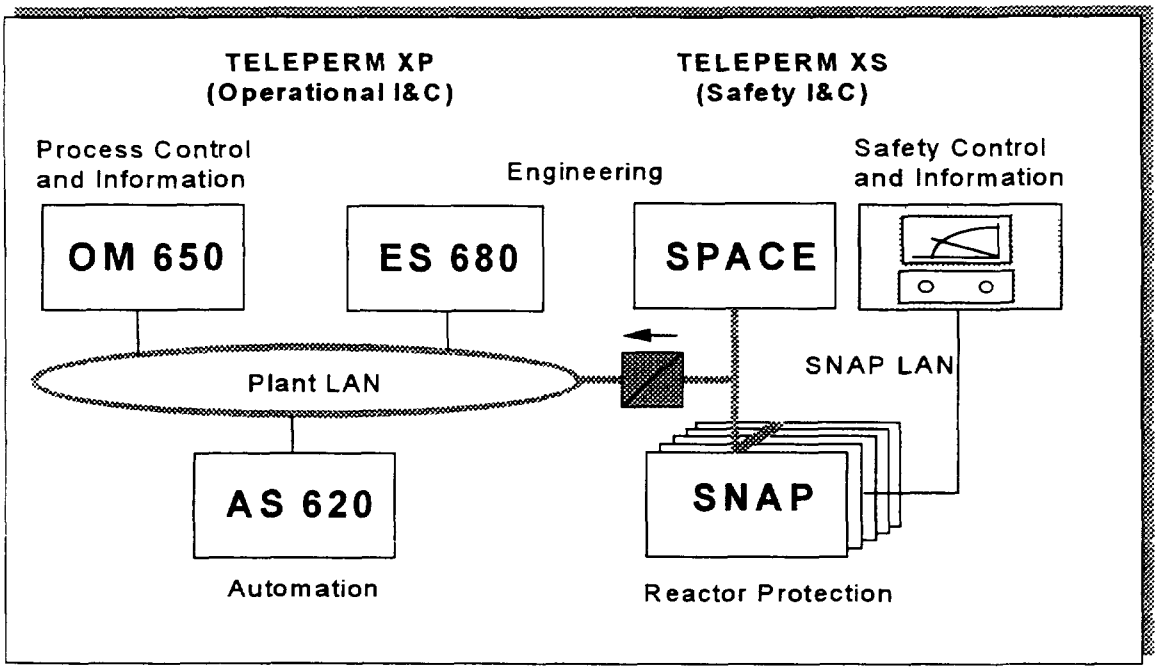


FIG. 1 Advanced I&C systems for nuclear power plants.

This means that the entire plant-specific functionality of the hardware and the software is specified in graphics using the engineering system and stored centrally in a database. To enhance clarity the engineering tool supports hierarchical structures with several levels. The engineering data created as part of the normal plant design serves as a reference for all further activities. It is used not only to derive the construction documents for cabinet fabrication but also to automatically generate the entire plant-specific software code. It also forms the basis of complete function- and location-oriented documentation, thereby ensuring that the documentation of all components of the I&C system is always up to date and complete. The graphic user interface behind which the specific data and mechanisms of the I&C system are concealed is in itself an important step into the future and permits the process engineer to specify the functional requirements on the I&C system without any software knowledge.

Although an integrated engineering support considerably simplifies commissioning, the real advantages of the engineering tool become apparent later when the plant is in operation. The strong consistency of the plant documentation with the I&C functionality actually implemented, which is ensured by the consistent use of strict feedforward documentation, is especially important if frequent modifications and expansions are required during the plant operation time. The engineering system is also used for maintenance and diagnosis during operation of the I&C system. For example, internal states such as fault signals from modules or simply the current values of variables can be scanned and visualized on the graphic user interface of the engineering tool. Furthermore overview pictures describing the I&C structure together with the ergonomic user interface assure quick and direct identification of all module faults, so that specific repair measures can be taken in time and service costs reduced

3. OPERATOR CONTROL AND MONITORING

Operator control and monitoring of the process is performed using the process control and information system. It is characterized by a client-server concept based on international standards that permits distribution and scaling of the functionality in a way that no other architecture can. Clients and servers communicate via a common, open terminal bus so that all information is available everywhere. This permits adapted implementations, ranging from low-cost minimum configurations as they are necessary for example for local control stations up to screen-based complete control rooms with overview displays and one or more control consoles.

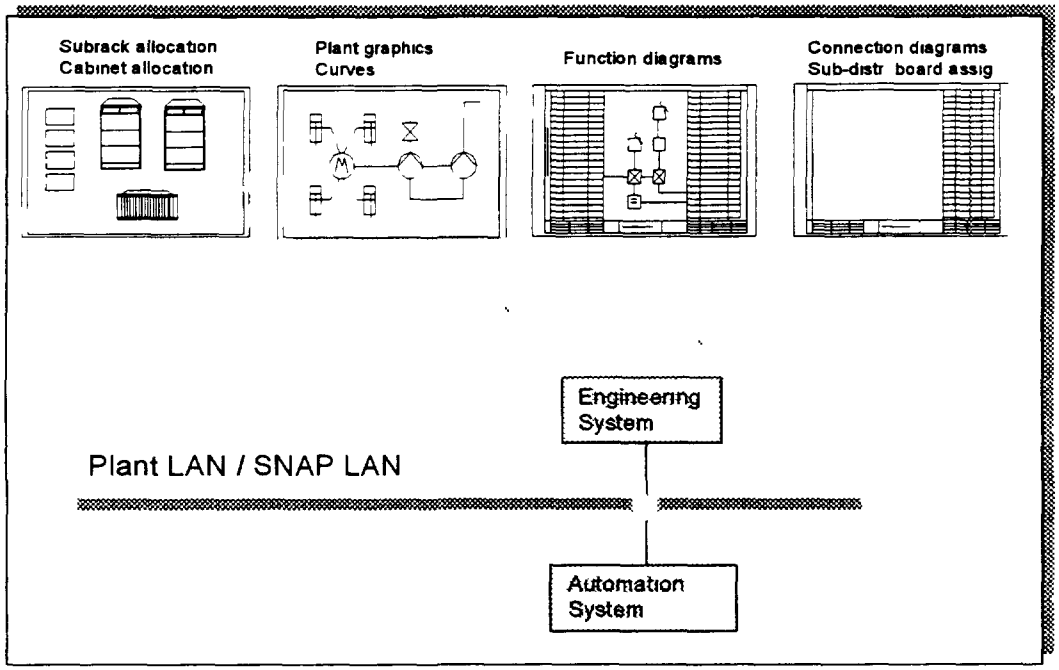


FIG. 2 Tasks of the engineering system.

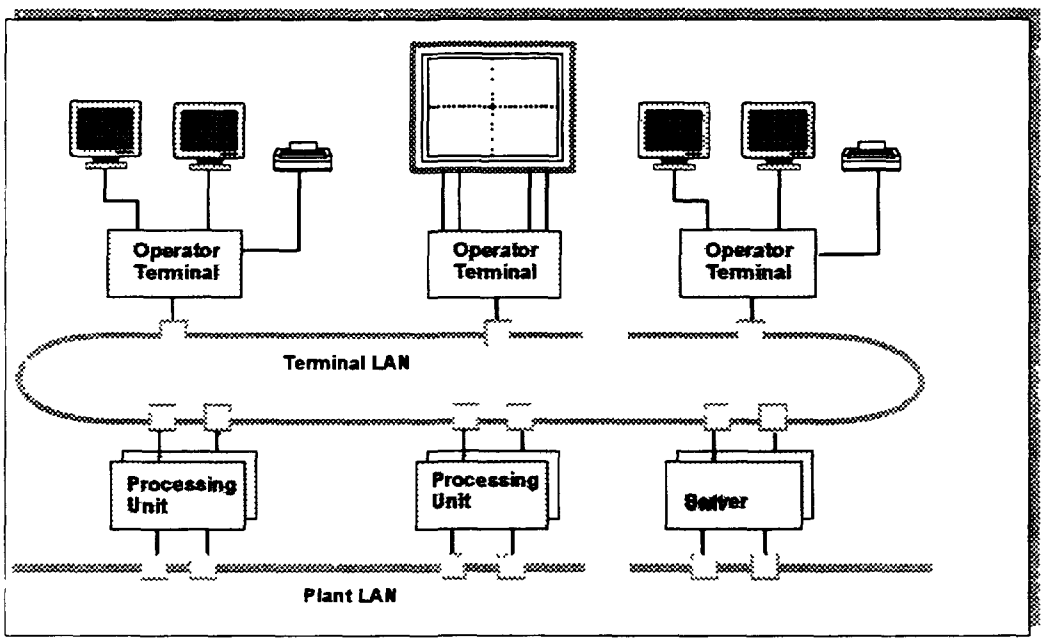


FIG. 3 TELEPERM XP process control and information.

The display devices used are high-quality graphics monitors and large-area displays allowing information about the process, about the plant and about the process control system to be displayed graphically or alphanumerically Operator input is made using an input device that is in wide-spread and successful use in the PC world, the mouse

A screen-based control room necessarily involves a greater information density than a conventional control room For this reason, ergonomic display of information and operator guidance are especially important The visualization of functionally coherent process complexes in conjunction with a hierarchically structured organization of the process display has proven especially advantageous This method of representation is supported by the process control and information system by surrounding each display with an identical frame containing selection fields with which the operator can request

additional information and navigate his way through the displays to request additional information and navigate his way through the displays to obtain the required information Extensive case studies have shown that this concept can provide the operator with all the necessary information even under stressful conditions

In addition to these classic processing functions for process control and information, other future-oriented function modules can be integrated into the server computer One example of this is the "forecasting computer" function module that calculates process behaviour in advance on the basis of the current plant state to provide the operators with information about the profiles of important process variables for a certain time into the future This means that action to remedy faults can be taken in good time, thereby enhancing the availability of the plant

4 COMMUNICATION

Open communication between systems and components of different manufacturers is the aim pursued by international standardization activities in communication technology The most important standard for open networks is the OSI reference model from the International Standardization Organization It provides an abstract description of the network architecture and the associated protocols All other standards are based on the functions defined in this model This also applies to the SINEC (Siemens Network Communication) local area networks used with TELEPERM XP and TELEPERM XS

The relevant requirements for electromagnetic compatibility and decoupling are met by the choice of the transmission medium

- Triaxial cable,
- Optic fibers,

and relevant requirements for transmission performance by the choice of the bus type

- Ethernet (IEEE 802 3),
- Profibus (DIN 19 245)

In applications where insensitivity to electromagnetic interference, galvanic isolation, or bus lengths of up to 4000 meters are required, optic fibers are used as transmission medium

The great significance that communication between the I&C components has for the safety and availability of the power plant demands an extremely high degree of reliability for data transmission In order to meet this demand the buses themselves used must be as a matter of principle of fault tolerant design

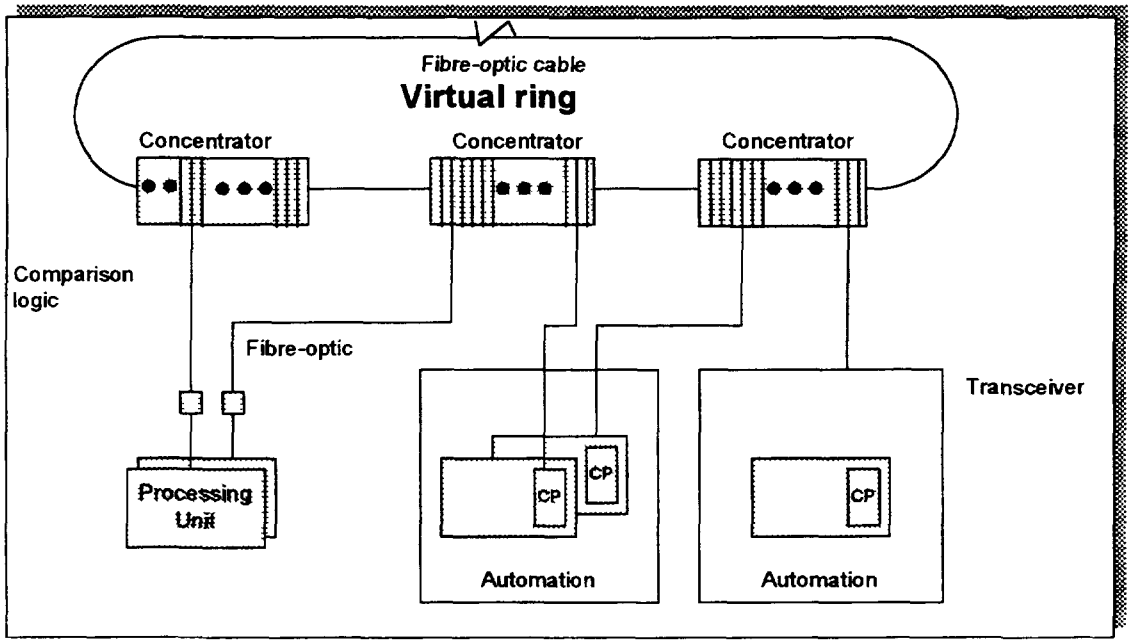


FIG. 4 TELEPERM XP open communication acc. to ISO/OSI.

5. AUTOMATION

In automation, the I&C tasks of closed-loop control, open-loop control, signaling, monitoring and protection are implemented. To achieve this, the automation equipment acquires measurements signals from the process using analog or binary input modules, perform the necessary data processing and output commands to the actuators in the plant (motors, valves, etc.) via analog or binary output modules. In this way, start-up and shut-down sequences are implemented, load changes are made, appropriate action is taken in response to disturbances and, if necessary, protection trips are initiated.

For economic implementation of a process control system it is of paramount importance to be able to adapt the structure of the automation to the requirements of the plant flexibly This means that the automation must be structured in a task-oriented way. TELEPERM XP and TELEPERM XS both provide the freedom to meet all demands economically. The scalability of the systems assures that individual autonomous control loops, medium-sized systems with local control stations, or complete nuclear power plants with a large-scale screen-based control room can all be implemented just as economically. Fail-safe or fault-tolerant systems can also be implemented, thanks to provision made for planned degrees of redundancy throughout the process control system.

All automation equipment can be connected to a common plant LAN so that all available information about the process can be evaluated centrally. This renders possible effectively to monitor the consistency of the information continuously so that only validated information is passed on to the operator.

The concept described forms the basis of both the TELEPERM XP and TELEPERM XS digital I&C systems. Both systems can be used independently or together. TELEPERM XP is intended for all automation tasks for which no specific qualification for nuclear applications is required. This is the case for the control of essential process variables, for almost the entire man-machine interface as well as for the extensive open-loop controls of the auxiliary systems. This delimitation means that TELEPERM XP can be used for all the automation tasks of a fossil-fired power plant as well as for functions not important to safety in nuclear power plants

TELEPERM XS, on the other hand, is intended for the safety I&C of a nuclear power plant. Its typical applications are reactor protection and ESFAS functions The scalability of the system permits automation of other safety-related tasks, such as control of the refuelling machine or the control rod

movement computer To cover all these tasks, TELEPERM XS is qualified for use in the highest safety category.

Teleperm XP

The TELEPERM XP process control system is designed to perform all automation tasks in the power plant for which no specific qualification for nuclear applications is required In order to perform these tasks, TELEPERM XP is scalable in large extents so that economic solutions can be ensured both for very small application and for complete plants.

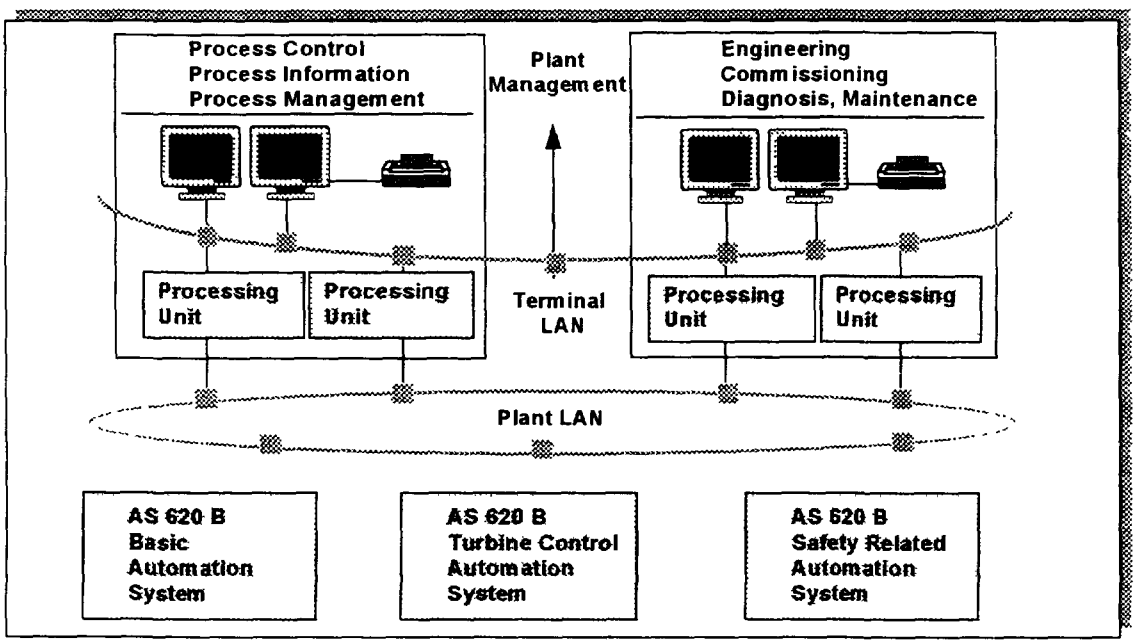


FIG. 5 TELEPERM XP overview.

For engineering, maintenance and diagnosis, TELEPERM XP contains the ES 680 engineering system All components of TELEPERM XP, i.e the equipment for automation, operator control and monitoring, and for communication can be handled in every phase of the engineering process in accordance with the general concept Configuration and documentation of the plant-specific software functionality, of the process I/Os or of communication is possible. After commissioning, the same system is used to make modifications to the software or to locate failures of hardware components

TELEPERM XP includes the OM 680 process control and information system for operator control and monitoring. This system features a user-friendly man-machine interface, the use of modern visualization media, high availability and a modular hardware and software concept OM 680 meets the above mentioned requirements to user friendly and ergonomic information displays and supports manual control Appropriate configuration with just a few basic hardware components such as PC, monitors and local area networks permit compact solutions which can be expanded right up to large-scale man-machine interfaces

The hierarchically structured automation system fulfills the most varied demands in a power plant with its three function-oriented system types:

- Basic functions (AS 620B);
- High availability and fail-safe applications (AS 620S);
- Increased dynamics, e.g for turbine control (AS 620T)

The system types AS 620B and AS 620S can be used at the individual control level with function modules on a parallel, redundant cabinet bus Additionally the AS 620B signal modules can be

connected via the SINEC L2 DP serial peripheral bus. In this way, it is possible to implement future-oriented field bus concepts with TELEPERM XP at the automation level.

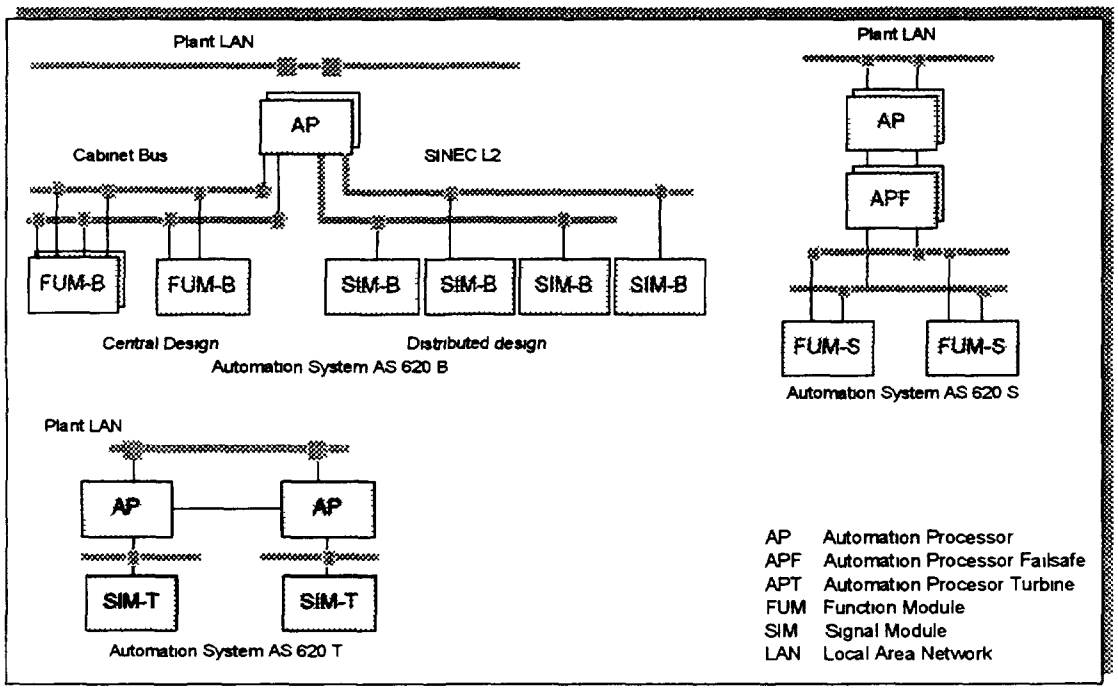


FIG. 6 variants of automation.

To increase availability, all automation processors and the function modules can be implemented redundantly Not only is the use of future field bus technology being prepared - a precondition of this are intelligent and bus capable field devices - but the use of fuzzy logic has also been planned for new closed-loop control tasks

All components of TELEPERM XP intermesh fully and they together form a modern process control system with which the various process control tasks of a power plant can be implemented in a future-oriented and economic way The modular system structure permits adequate solutions for all types and sizes of power plants

Teleperm XS

National and international codes and standards impose special requirements on the safety I/C of a nuclear power plant These concern

- Fault tolerance;
- Robustness;
- Qualification.

In order to be able to meet these requirements to the full without making operational automation tasks unnecessarily expensive by excessive conservatism, the TELEPERM XS I&C system was developed to complement the TELEPERM XP system. It is largely based on standard devices selected for their quality characteristics and adapted by specific design measures. The qualification required by nuclear codes and standards is achieved by supplementary type tests and extended factory tests.

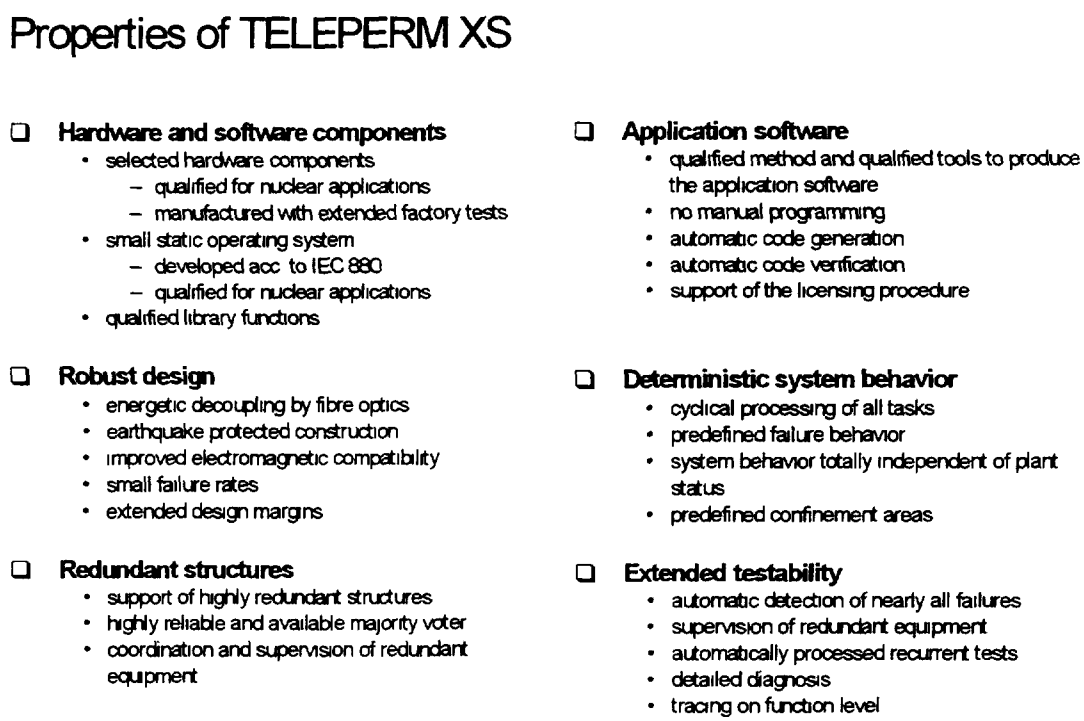


FIG. 7Properties of TELEPERM XS.

6 REACTOR PROTECTION

The most important requirements on safety I&C in nuclear power plants concern the automation equipment for reactor protection The required fault tolerance characteristics demand for a distributed multicomputer system The automation devices used must permit the implementation and supervision of widely distributed topological structures

Superimposing the functional requirement that some protective actions must be initiated very rapidly so as to prevent unsafe states reliably to the above mentioned characteristic, leads to very high performance requirements

TELEPERM XS fulfills these requirements and also has system characteristics that support the implementation and operation of highly redundant, spatially distributed architectures For example, highly reliable and highly available I/C systems consisting of two, three of four redundant trains can be implemented with each required topology within the trains The electrical isolation of automation units is mainly achieved by the use of fiber optics for communication To avoid a reliability bottleneck in the interface between the redundant I&C trains and the individual control level, a highly available architecture has been applied for the associated voting processor

Robustness demands design measures that affect both hardware and software The use of modified packaging hardware allows TELEPERM XS to withstand accelerations such as during an earthquake or in the event of an aircraft crash Appropriate shielding measures for the cabinets ensure that the stringent requirements on electromagnetic compatibility are also met In addition to design measures for the hardware, special design rules are also applied on the software One important rule demands the effective decoupling of the plant process from the behavior of the I&C system because it must be guaranteed that a disturbance or accident in the plant process cannot under any circumstances cause an impact on the safety I&C For this reason, the computers of TELEPERM XS process all tasks cyclically and do not use event-controlled programs This means measurement signals are read in, limit signals formed and control commands output in a never varying sequence regardless of whatever happens in the plant or in other computers

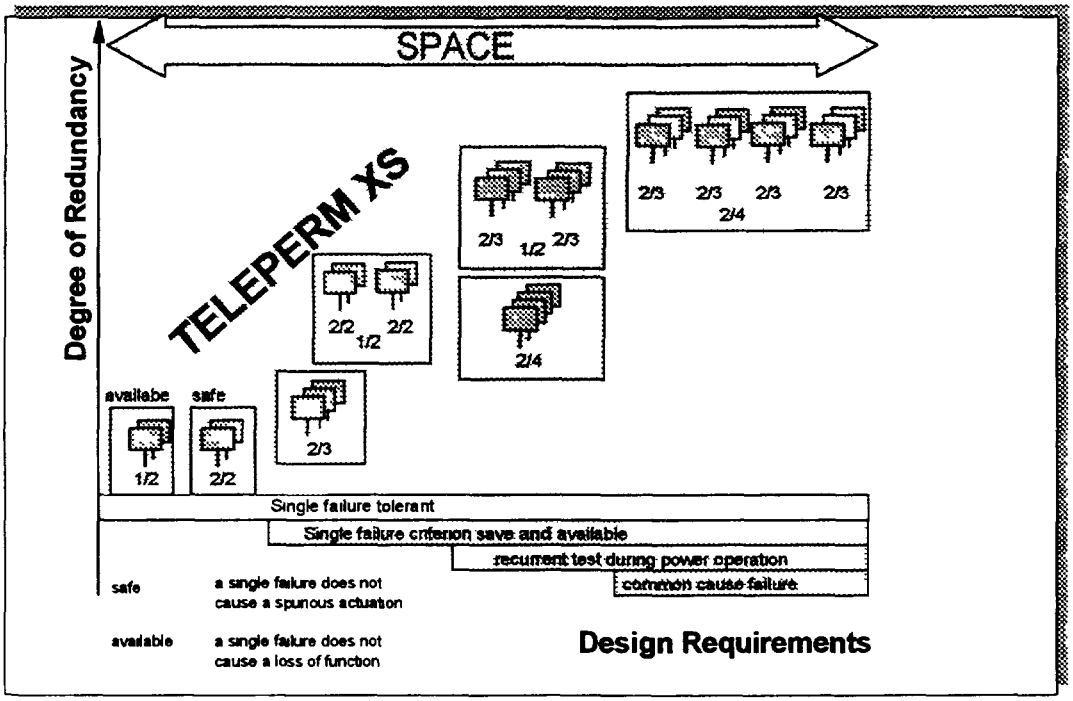


FIG 8 Structure of safety I&C.

7 SAFETY CONTROL AND INFORMATION

Operator control inputs in nuclear power plants mostly involve operational tasks Safety related manual intervention such as manual input to the safety I&C system is very limited in scope Moreover, the low market potential does not justify the development and qualification of a screen-based user interface via which safety-related manual intervention could be implemented TELEPERM XS therefore does not have dedicated equipment for operator control and monitoring Instead, the hardwired control room instrumentation is used for safety-related manual command input However, TELEPERM XP equipment can be used, for example, to display or archive process variables acquired via the safety I&C as part of normal process control For this purpose, the safety I&C system is connected to the plant LAN of the operational I&C via a uni-directional gateway

Local control stations for safety-related equipment are only used operationally as well and can therefore be implemented using TELEPERM XP devices

8 ENGINEERING

The development of plant-specific application software is generally considered the most error-prone activity during the implementation of safety-related I&C systems For this reason, for TELEPERM XS the production of application software is strongly formalized In this way, problems related to individual working methods of the staff members can effectively be avoided Not only the production but also the verification process can be automated to a remarkable high degree In addition to the function described, the tools required for verification and validation have also been integrated into SPACE, the engineering system of TELEPERM XS, so that its function scope is far greater than that of any previously known engineering aid

With SPACE the following process model is used to developed plant-specific application software the task specifications are mainly laid down by mechanical engineers, process engineers and physicists - as always - in prose, diagrams, equations and tables, and are passed on to the I&C specialists in this form These problem definitions are read and understood by I&C specialists - i e control engineers, communications engineers, physicists, computer engineers and mathematicians Queries for better understanding develop into system discussions The I&C specialists then prepare all the data and information in a pre-defined way before using the editor of the engineering system SPACE to specify the I&C functions in the form of function diagrams These function diagrams with well-defined presentation

conventions are readable and understandable for the parties that originated the task specifications for verification purpose and also serve as documentation for the customers. A format recommended by VGB is used which was the result of contracted development of the institute of Prof. Welfonder, Stuttgart

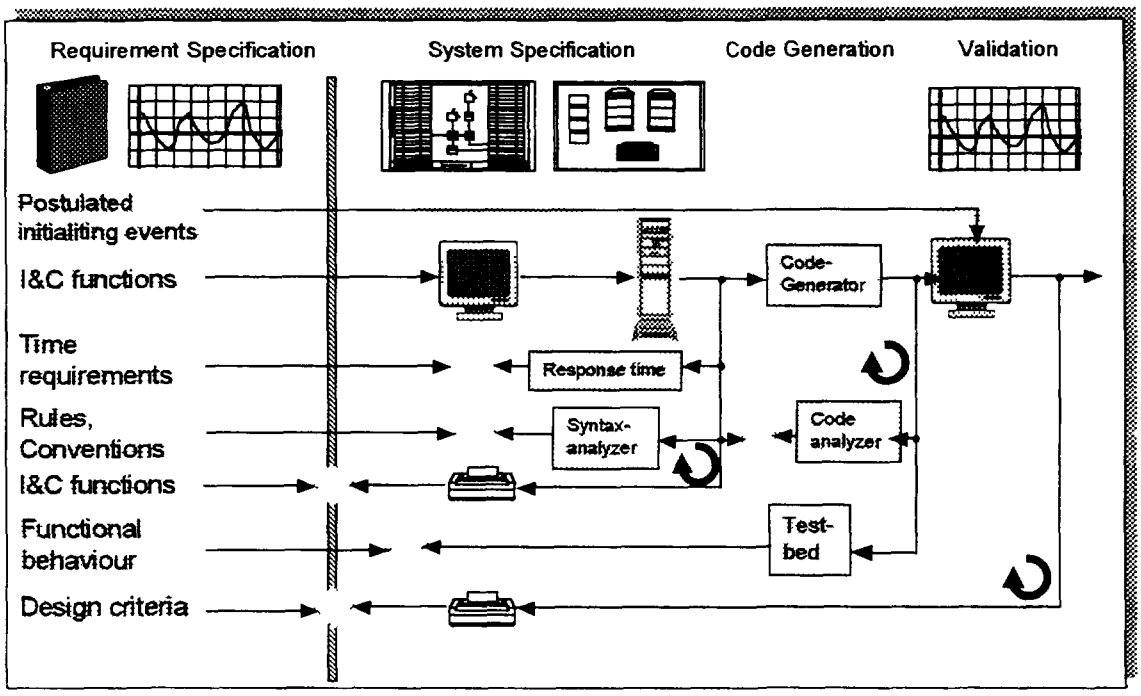


FIG. 9 The system design process.

Once the specification is complete, it can be checked automatically according to various criteria using analysis tools. This analysis includes such important characteristics as completeness and the absence of ambiguity. This has only been made possible by the use of rigorously formal methods The formally correct specification is then passed on for verification by the originators of the requirement specification who are also responsible for its release. For the quality of the application software it is of decisive significance that the application software is automatically derived from the formal specification by qualified generators. Because the software was generated by an automatic tool, it is possible to verify the consistence of the generated code with the formal specification using a second automatic tool. One consequence of this method is that quality verification of the code generator can be kept economically viable.

After this verification step, the code is ready for testing As an option to facilitate testing, a test environment can be generated by the code generator This provides all the aids required for efficient testing. For example, arbitrary signal transients can be generated in order to provoke specific responses and all internal signals and memories can be accessed in order to evaluate the functional behavior.

If realistic feedback from the process is required to evaluate functional behavior, the generated code can be linked to a partial area simulator. In such functional tests the partial area simulator simulates the thermohydraulic power plant process and provides the I&C functions with the required measured data. The I&C function, i.e. the test object, responds to this measured data with commands to the final control elements which in turn affect the thermohydraulic power plant process. If necessary, power transients as well as malfunctions or accidents can be simulated by the partial area simulator.

9 QUALIFICATION

Especially when developing new technology systems which are to perform important safety functions, it is essential to take care of safety requirements from the beginning in order to avoid problems which in

later stages of the development process might lead to costly changes or even redesign Therefore a development accompanying assessment has been decided

Accompanying evaluations and concept assessment of the whole system **by GRS ISTec.** Since 1988, continuous evaluations of the development on behalf of the Bavarian licensing authority (BStMLU) In June 1992, acceptance of the concept to realize I&C systems for safety functions of the highest category

a) Type testing

Type testing has to demonstrate the compliance of the modules with the data specified in the corresponding data sheet It consists of a theoretical and a practical part Essential issues of the theoretical assessment are the failure effect analysis, the critical load analysis and the program for the practical tests, which comprise functional tests and robustness tests (internal and external influences/events) The role of an authorized expert (independent institute) is the assessment of the documents as prepared by the manufacturer, the evaluation of the practical test program, the participation in the practical tests (to the extent considered necessary) and the assessment of the test results Software type testing is performed in analogy to hardware type testing This can be done because as a rule we are facing distributed systems with reusable software modules which can be configured and parameterised according to their envisaged application

b) Type testing of the software modules

Since October 1992, contracted to GRS ISTec, which is supported by TUV-Nord In June 1996, the qualification of the system software and the application modules was finished One new aspect is that all re-usable software is subject to a type test "analogous to the stipulations of KTA 3503" This method is of special advantage to the TELEPERM XS concept because the entire application software is made up of re-usable software modules combined by generators, i e software modules are used in the same way as hardware modules in hardwired systems A software module has a well-defined functionality and a well-defined interface that can both be checked against the pecification Whereas in the hardware type test, greater emphasis is placed on practical testing, in the software type test equal emphasis is placed on theoretical and practical testing

c) Type testing of the hardware modules

Since February 1994, contracted to TUV-Nord to elaborate the module analysis and the test specifications The practical testing was delegated to the test institute of TUV Rheinland (ISEB)
In October 1996, the practical tests of the hardware modules for the qualification were finished

d) Plant Independent System test

proving the main system features with participation of GRS ISTec and TUV Nord as independent assessors These tests are scheduled for November 1996

The main system features to be proven by this tests are checking the specified system performance, e g the strict cyclic processing of the application code and proving the correctness of the recalculation of processor and bus loads as well as of the response time for the specified application code by the engineering tool SPACE, validation of the process of generating the application code, system behaviour independent of the application software and its allocated input data trajectories

Fig 10 gives an overview on the main standards relevant as well for the development as for the qualification

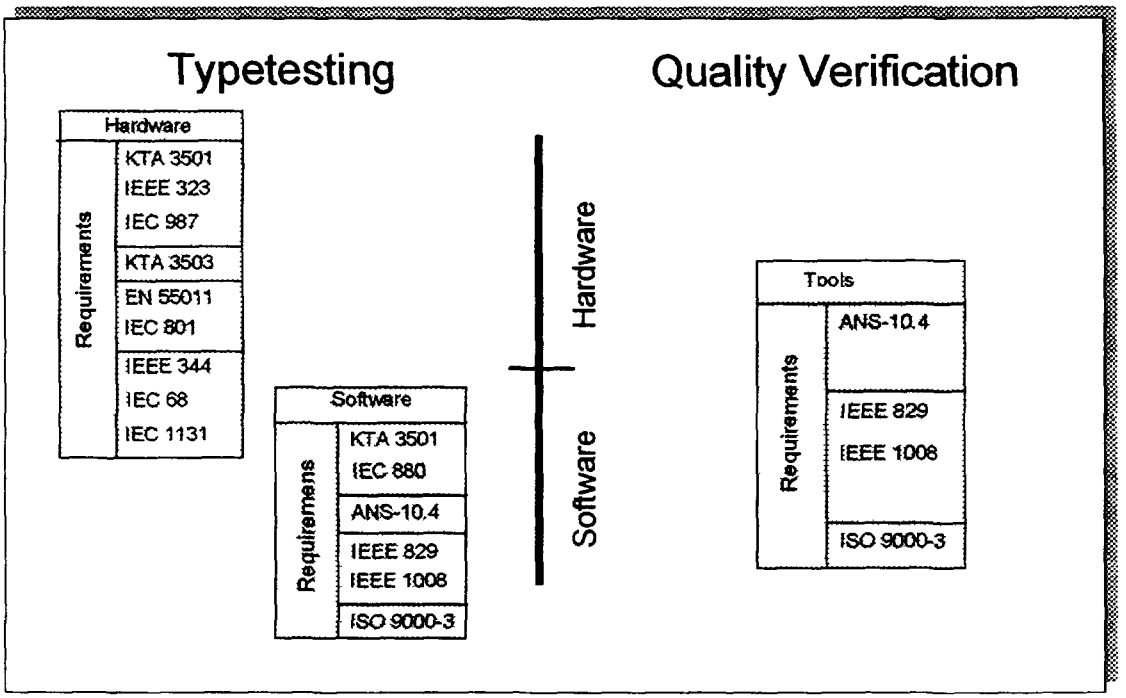


FIG. 10 Basis of qualification.

Abbreviations

ANS	American National Standard
AS	Automation System
CP	Communication Processor
DIN	Deutsche Industrie Norm
EMC	ElectroMagnetic Compatibility
ES	Engineering System
GRS	Gesellschaft für ReaktorSicherheit
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Standardization Organization
ISTec	Institut für SicherheitsTechnologie
KTA	KernTechnischer Ausschuß
LAN	Local Area Network
OM	Operation and Monitoring
OSI	Open System Interconnection
SNAP	Siemens Nuclear Automatic Protection
SPACE	SPecification And Coding Environment
TÜV	Technischer ÜberwachungsVerein
VGB	Verband der GroßkraftwerksBetreiber

AN INTEGRATED APPROACH FOR INTEGRATED INTELLIGENT INSTRUMENTATION AND CONTROL SYSTEM(I^3CS)

C H JUNG, J T KIM, K C KWON
Korea Atomic Energy Research Institute
Yusong, Taejon, Republic of Korea

Abstract

Nuclear power plants to guarantee the safety of public should be designed to reduce the operator intervention resulting in operating human errors, identify the process states in transients, and aid to make a decision of their tasks and guide operator actions For the sake of this purpose, MMIS(Man-Machine Interface System) in NPPs should be the integrated top-down approach tightly focused on the function-based task analysis including an advanced digital technology, an operator support function, and so on The advanced I&C research team in KAERI has embarked on developing an Integrated Intelligent Instrumentation and Control System(I^3CS) for Korea's next generation nuclear power plants I^3CS bases the integrated top-down approach on the function-based task analysis, modern digital technology, standardization and simplification, availability and reliability, and protection of investment

1. INTRODUCTION

All of the nuclear power plants in Korea are operating with analog instrumentation and control(I&C) equipment that are increasingly faced with frequent troubles, obsolescence and high maintenance expense Electronic and computer technology have improved rapidly in recent years and have been applied to other industries The digital technology provides advantages such as processing of numerous data, improvement of system reliability, flexibility of adding new functions, automation of periodic tests, self-diagnostics, and improved operation and maintenance using standardized components So it is strongly recommended that we adopt the modern digital and the computer technology to improve plant safety and availability

The TMI-II accident was primarily caused by a wrong identification of the plant state resulting from human factors deficiencies in the plant information system It is very difficult for the operator to identify abnormalities of process state in transients For the sake of identification of the abnormal conditions, the operator should get sufficient and credible information such that the operator diagnoses and prognoses the process states, and confirm operator's actions It is a good approach that the integrated top-down approach tightly focuses on the function-based task analysis including an advanced digital technology, an operator support function and so on Figure 1 illustrates the strategy for applying the integrated approach into NPPs in Korea

In light of the need to improve MMIS of NPPs, the advanced I&C research team in KAERI has embarked on developing an **Integrated Intelligent Instrumentation and Control System(I^3CS)** for Korea's next generation nuclear power plants I^3CS bases the integrated top-down approach on the function-based task analysis, modern digital technology, standardization and simplification, availability and reliability, and protection of investment The initial effort in this multi-year project focuses on process monitoring, alarming, alarm diagnosis, increasing automation, human-performance evaluation of the developed system and a development of methodology of software verification and validation We are developing Alarm and Diagnosis-Integrated Operator Support System, called ADIOS, to filter or suppress unnecessary or nuisance alarms and diagnose abnormality of the plant process ADIOS has been built in an object-oriented AI environment of G2 To increase automatic level, ASICS is developed to automate low power level from cold shutdown to 5 % reactor power level by using supervisory modular control scheme To evaluate and validate the performance of the developed system, a study is progressed on the field of human-performance evaluation and software verification and validation [1-4]

2 TARGET OF I^{3}CS

To establish the technical goals of I^{3}CS, we have evaluated the technical level of I&C, such as Computerized Compact Workstation, Digital Control, Digital Protection, Operator Support, Network, and Digital Data Acquisition and Nuclear Integrated Monitoring Technique The results of the evaluation were to increase the level of automation applying the advanced control techniques such as supervisory control and automatic startup/shutdown system, to consolidate the function of diagnosis and operator support in process transients, and to integrate these systems properly according to operator's cognitive mental model Fig 2 shows the technical goals of I^{3}CS

We proposed I^{3}CS for beyond the next generation NPPs in Korea I^{3}CS reflects a concept of EPRI Utility Requirement Document such as top-down approach based on the functional task analysis, modern digital technology, standardization and simplification, availability and reliability, and protection of investment, etc To accomplish this purpose, the major targets of I^{3}CS were established with the following major elements

Reduced Human Errors

First of all, to reduce human error, the integrated design methodology should be developed There is a feasible way of the integrated top-down approach to reconstruct the I&C architecture including control room based on a task allocation by the functional-based task analysis Second, a cause bringing about human error should be eliminated Because the automatic start-up/shutdown system reduces the operator intervention in operation of start-up and shutdown mode, a mistake of operator will be significantly reduced Intelligent operation support system aids to identify the plant state in the transient condition, make a decision of the operator tasks, and guide operator actions

Improved Availability and Reliability

The reactor protection system and safety related system will be designed by digital technology with an automatic test function and self-diagnosis features These technologies will significantly decrease the unnecessary reactor trips The use of digital technology in NPPs takes advantages such as processing of numerous data, flexibility of adding a new function, and reduction of operation and maintenance expense However, an application of digital technology may bring about a new problem to ensure safety and reliability as concerns common mode failure and software verification and validation(V&V) Especially because of the characteristics of software, the safety and reliability of software are critical issues in the digital I&C system of NPPs

Standardization and Simplification

I^{3}CS uses the industrial open architecture and off-the-shelf equipment manufactured in the domestic industry Because the off-the-shelf equipment is developed with the design of adapting the industry standard, modularizing and simplifying, repair of I&C equipment will be accomplished by simple modular replacement in the field Operation and maintenance cost may be reduced

Assure License

An application of digital technology, especially digital safety system may bring about the new problems such as common mode failure, software verification and validation(V&V), establishment of quality assurance program and resolution of elecro-magnetic interference A number of method and tool to solve these problems are being studied and developed, but not completely resolved These problems are directly connected with licensing issues For the sake of protection of utility's investment, license should be assured by solving these problems

3 INTEGRATED APPROACH

It is expected that I&C systems, particularly the control room, for future plants will be strongly focused on human factors engineering Therefore, the design of I&C architecture and the control room should be done in terms of operator tasks for human error reduction The design concept that

provides the greatest consideration to the operator is only achieved by the integrated approach to re-construct the whole I&C structure and control room based on the allocation of functional task-centered human operator MMIS of next generation NPPs in Korea integrates the operator support functions, the process operation functions and the monitoring functions according to operator's cognitive mental model

The integrated top-down approach focused on operator tasks and should be performed on the basis of the previously obtained system design technology, the developed research results, and the transferred technology from ABB-CE In the development stage, we will develop a standard design package(I^3CS) of the level If there are some fields of technology lacking in Korea such as diagnosis model, operator response model, supervisory control techniques and performance evaluation, etc, they will be provided by cooperation with foreign suppliers

4 APPROACH FOR I^3CS

The I^3CS consists of three major parts, (1) the advanced compact workstation, (2) the distributed digital control and protection system, including Automatic Startup/shutdown Intelligent Control System(ASICS), and the computer-based alarm processing and operator support system, called Diagnosis, Response, and operator Aid Management System (DREAMS) The advanced compact workstation adapts a control workstation concept by adding the new design features such as supervisory functions, operator support display, and selected mobile overview display, etc The distributed digital control and protection system are designed by using the robust and fault-tolerant control method, the intelligent supervisory control technique, the automatic startup/shutdown system, the data communication network, etc DREAMS provides the operator exact information by using the dynamic alarm processing techniques, the model-based fault detection and the diagnosis functions, etc

4.1. Advanced compact workstation

The advanced control workstation has adapted a computer-based compact workstation concept on the application for next generation NPPs By the first effort to allocate the function of the computer-based compact workstation, the function-based task analysis was performed This advanced compact workstation is upgraded by adding the new design features on the basis of functional-based task allocation The added design features are as follows

- extension of supervisory functions,
- extension of coordinated function between operators,
- consolidation of operator support function,
- Intelligent soft control technique,
- electronic display of normal and emergency procedures,
- Extension of overview display,
  - two detailed system overview mimic displays,
  - a selected movable overview display

4.2. Fully distributed digital control and protection system

Through the function-based task analysis, the control and protection system is also adapted in I^3CS by adding the following design features

- Fully using data communication network
- Supervisory control coordinating primary and secondary system
- Automatic startup/shutdown system with supervisory coordinator
- Robust and fault-tolerant control
- Addition of Macro control functions
- Certain resolution for common-mode failure, software V&V and EMI

The first effort in the control and protection system is to develop the digitized system The digitalization, especially of the protection system, has some problem such as common-mode failure, software verification and validation, and hardware electro-magnetic interference, etc To solve these problems, the control system is duplicated using the different hardware and software, and the protection system adds the system-based hardwired backup system The methodology for resolution of the problems of software V&V and EMI is being studied

The second effort is to increase the level of automation The increase of automation reduces operator intervention that is a cause of human errors The automatic startup/shutdown system is developed for these purposes

4.3. Automatic startup/shutdown intelligent control system (ASICS)

The target of ASICS automates operation from cold shutdown to 5 % of reactor power ASICS uses hierarchical modular control scheme and supervisory control scheme ASCIS divides the control scheme into three hierarchical control level Fig 3 shows ASICS's hierarchical control configuration scheme In the first supervisory control level, supervisory coordinator confirms an action of the lower level controllers, supervises the plant state and coordinates the lower level controllers The control level of the second operating mode divides the four control mode such as heating mode I sequence control, heating mode II sequence control, critical mode sequence control, and 2nd mode sequence control In this control level, the mode sequential controllers controls the needed components of the lower level control system in each control mode according to the sequential procedure As there are the break points between modes, the supervisory coordinator automatically checks and alarms a safe condition of control process and coordinates the lower level controllers The major control in heating mode I is temperature control in the primary system The major control in heating mode II is pressure and temperature control in the primary system The major control in critical mode is reactivity control in Core The major control in 2nd mode is level and pressure control in secondary system The low control level is the same of the conventional control scheme

4.4. Diagnosis, response and operation management system (dreams)

There are the strongly developing areas At present, one of the most important issues in human factors engineering field is to reduce human errors To reduce human errors, there are two ways that eliminate the essential cause of human errors by intervening operator and informing the operator what to precisely identify plant state in emergency condition and by directing the operator actions DREAMS provides the operator an exact information that supports the operator to diagnose abnormalities of plant, to manage the operator response on the application of the following technologies

- Computer-based dynamic alarm processing techniques
  - alarm suppression on operating mode,
  - alarm suppression on direct precursor and cause-consequence relationship,
  - dynamic prioritization dependent on plant state
- Model-based fault detection and diagnosis functions
- Integrated operation support and management system with computer-based guide display of normal and emergency operation, and technical specifications monitoring

The initial effort as a part of developing DREAMS focuses on intelligent process monitoring, alarming and diagnosis, namely Alarm and Diagnosis-Integrated Operator Support System (ADIOS) We are currently focusing on implementing an advanced alarm processing using G2 real-time expert environment ADIOS uses equipment-state dependency, plant mode dependency, alarm generation, and cause-consequence relationship(sometimes called, direct precursor), and multi-setpoint relationship(sometimes called, level precursor), in addition to some unique methods Our unique methods include separation of the process alarms (e g , temperature or pressure alarms of the main

process) from equipment-related alarms (e g , vibration or lubrication alarms of a pump), presentation of status alarms (e g , PORV not closed) on the process mimic, representation of group alarms assimilating information from several related alarms Fig 4 shows how the alarms are processed and presented in ADIOS

Two different scales of ADIOS are under development using G2 real-time expert system shell, (1) a small scale with about 40 alarms to devise a generic architecture for alarm processing and presentation and also to demonstrate the basic concepts of annunciation improvement, and (2) a large scale with hundreds of alarms to show the alarm management in a more practical environment The small-scale system is used as an example to illustrate the major concepts Fig 5 shows the process overview mimic display in ADIOS Once the large-scale ADIOS is developed, it also shall undergo several performance tests including (1) a preliminary test with the CNS, (2) verification and validation (V&V) of the ADIOS knowledge base using an automated V&V tool, called COKEP (Checker Of Knowledge base using Extended Petri net), and (3) a human-factors test using the Simulation Analyzer with a Cognitive Operator Model (SACOM) in the KAERI's Integrated Test Facility (ITF)

The activated alarms are then prioritized using several alarms processing methods, such as plant-mode dependency, equipment-state dependency, multi-setpoint relationship (i e , level precursor), cause-consequence relationship (i e , direct precursor), and so on Each alarm in ADIOS is initially classified into one of two different priority groups (1) the first priority group of priority 1 or 2, and (2) the second priority group of priority 2 or 3 This classification of every alarm is based on its importance as to the promptness of the operators' response needed, or the effect of the alarm on the plant process or equipment The prioritized alarms are displayed on the process overview mimic, and also the chronological list of alarms is givens on another dedicated CRT, with those alarms categorized by systems shown on the third CRT as a spatially dedicated soft alarm panel Priority 1, 2, or 3 alarms are shown differently in red, yellow, or white, respectively The same color coding is applied to the alarm texts in the alarm list, and also to the window tiles on the soft alarm panel

4.5. Safety software verification and validation (SSVV)

The use of computers in safety-critical, real-time, instrumentation and control applications requires that the issues of system performance, software verification and validation (V&V), software safety, and software related common mode failures be addressed Resolution of these issues as they pertain to nuclear facility applications is an emerging technology Nevertheless, for commercial nuclear applications, these issues must be adequately addressed during licensing process The modern and KNGR designs in Korea will utilize computers in safety-critical, real-time I&C applications

SSVV team is responsible for developing an indigenous technical capability for verifying and validating the software safety of computer-based I&C systems for safety-critical applications in nuclear facilities The missions of SSVV team in KAERI are (1) to evaluate the worldwide issues of digital safety system in nuclear power plant, (2) to construct the high-assurance software development environment, (3) to develop the methodology to design and to V&V software important to safety, (4) to study the basic technologies on safety-critical software We are conducting these missions successfully through the cooperative R&D with industry and universities, the globalization of R&D, and the collaboration with the regulatory body and the international standards organizations Fig 6 depicts the technological tree of SSVV and the relations

5 CONCLUSIONS

In light of the need to improve MMIS of NPPs, KAERI has embarked on developing an Integrated Intelligent Instrumentation and Control System(I^3CS) for Korea's next generation nuclear power plants I^3CS bases the integrated top-down approach on the function-based task analysis, modern digital technology, standardization and simplification, availability and reliability, and protection of investment

The initial effort in this multi-year project focuses on process monitoring, alarming, alarm diagnosis, increasing automation, human-performance evaluation of the developed system and a development of

methodology of software verification and validation We are developing Alarm and Diagnosis-Integrated Operator Support System, called ADIOS, to filter or suppress unnecessary or nuisance alarms and diagnose abnormality of the plant process ADIOS has been built in an object-oriented AI environment of G2 To increase automatic level, ASICS is developed to automate low power level from cold shutdown to 5 % reactor power level by using supervisory modular control scheme To evaluate and validate the performance of the developed system, a study is progressed on the field of human-performance evaluation and software verification and validation

REFERENCES

[1] KIM, J T , HAM, C S , KWON, K C , LEE, D Y , "The Strategy for the Advanced I&C System (I^3CS) Development", Proceedings of a Specialists' Meeting Organized by the IAEA in Co-operation with ISTec and held in Garching, Germany, 4-7 July (1995)

[2] KIM, I S , HWANG, I K , LEE, D Y , PARK, J C , HAM, C S , "An Integrated Approach to Alarm processing", The 2nd American Nuclear Society Topical Meeting on Nuclear Power Plant on Nuclear Power Plant Instrumentation, Control, and Human-Machine Interface Technology, University Park, Pennsylvania, USA, May 6-9 (1996)

[3] Na, N J , Kim, I S , Kim, J T , Hwang, I K , Lee, D Y , and Ham, C S , "AI-Based Alarm Processing for a Nuclear Power Plant," FLINS'96, The 2nd International FLINS Workshop on Intelligent Systems and Soft Computing for Nuclear Science and Industry, Mol, Belgium, September 25-27 (1996)

[4] JUNG, C H , " A Development of Automatic Control Modes for the Startup Operation of NPP," Proceeding of the Korean Nuclear Society Autumn Meeting, Vol 1, Seoul, Korea (1995)

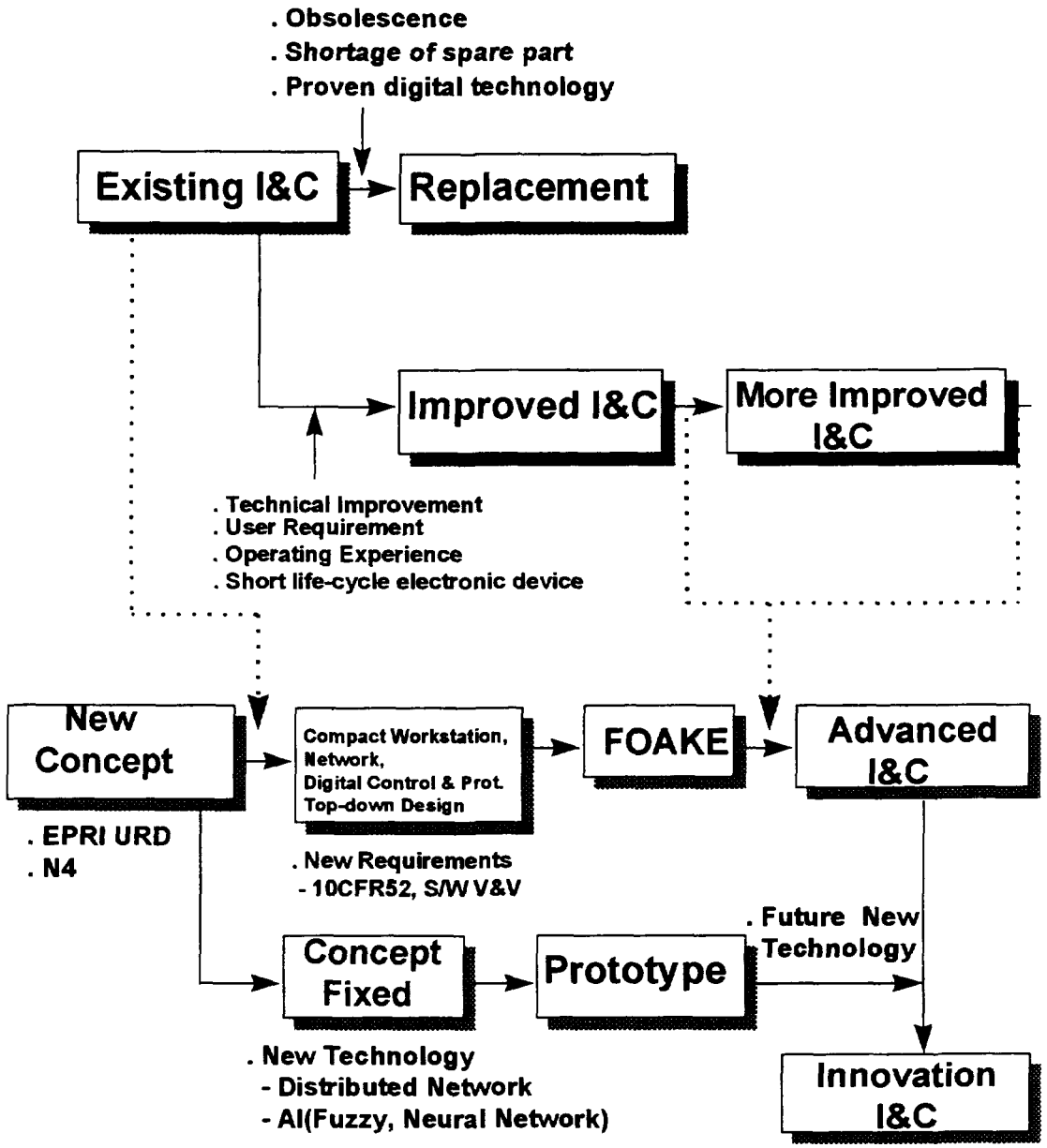


FIG. 1. The strategy for applying the integrated approach.

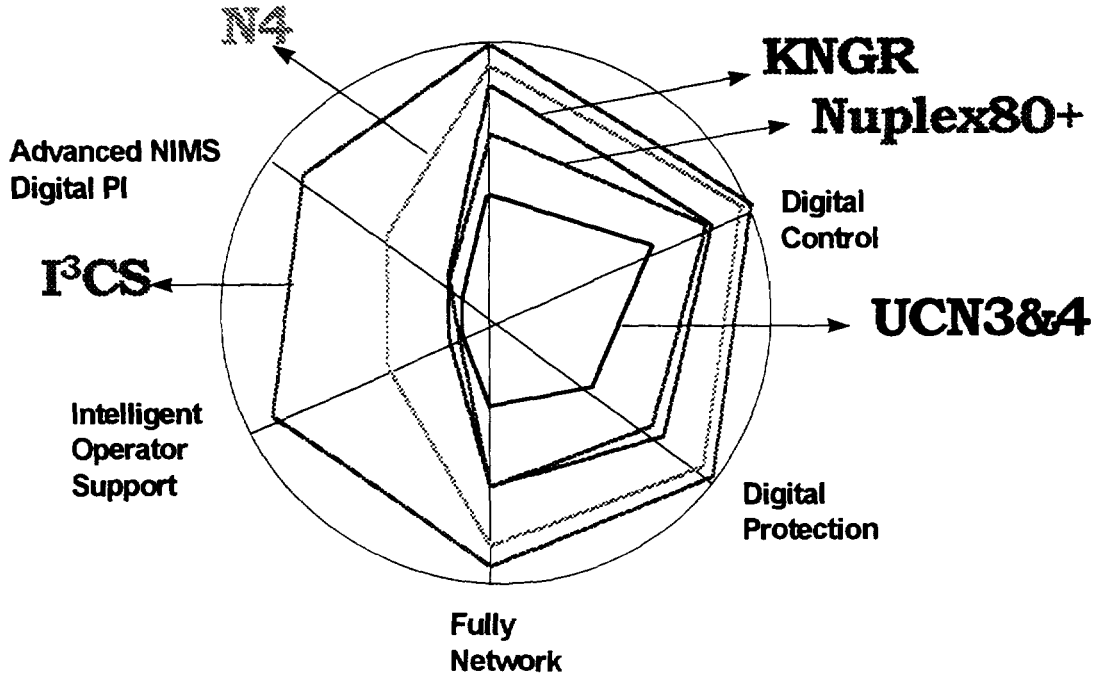


FIG. 2. The technical goals of I³CS.

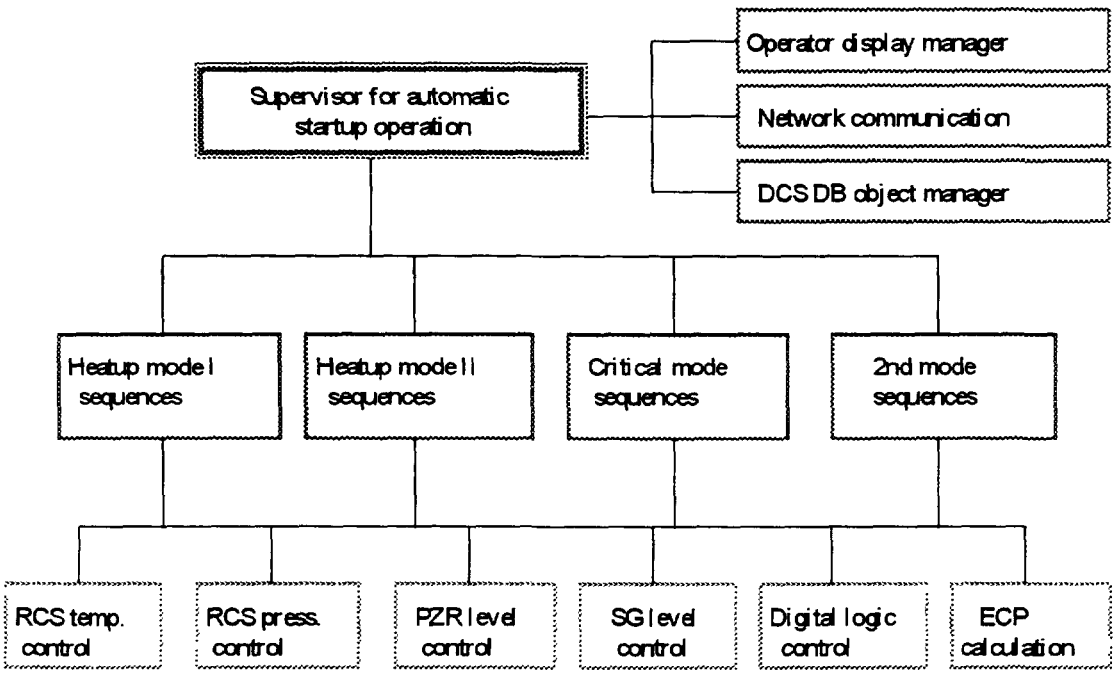


FIG. 3. ASICS's hierarchical control scheme.

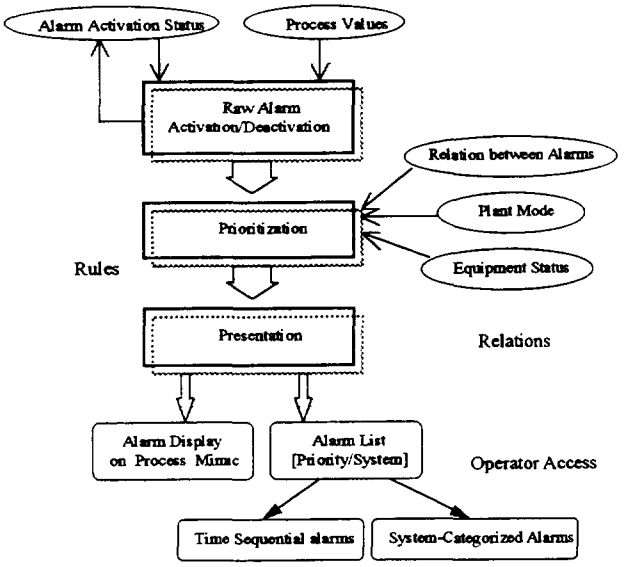


FIG. 4. Alarm processing flow in ADIOS.

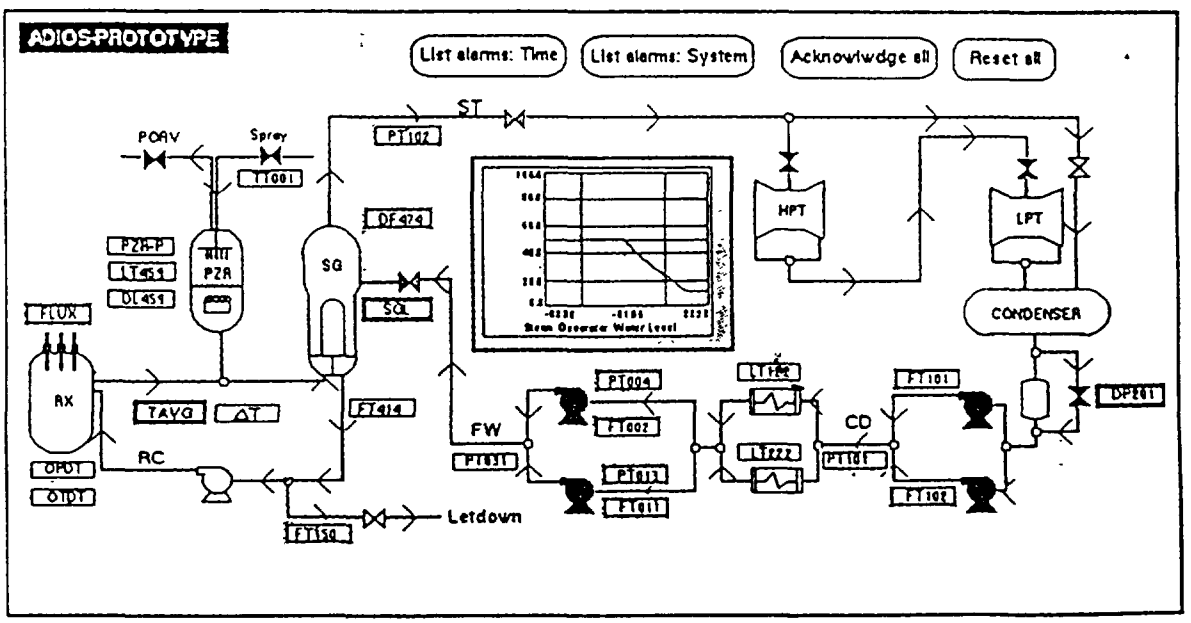


FIG. 5. Process overview mimic display in ADIOS.

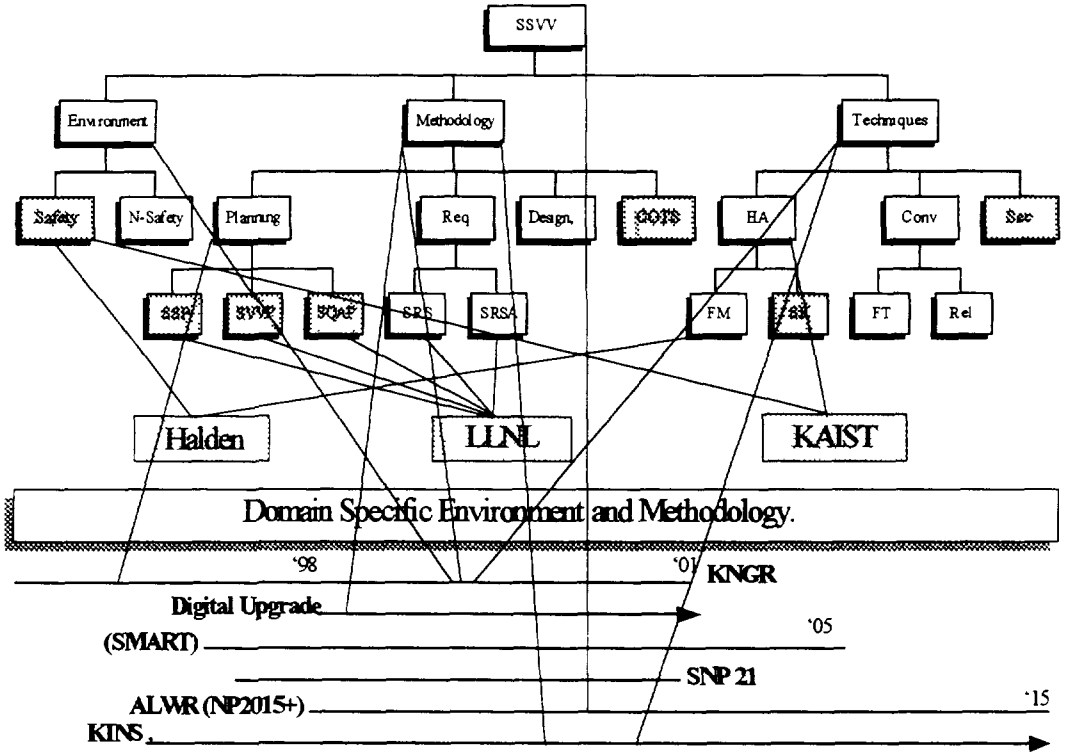


FIG. 6. Technology tree of SSVV and relations with others.

HUMAN-MACHINE INTERFACE ASPECTS AND USE OF COMPUTER-BASED OPERATOR SUPPORT SYSTEMS IN CONTROL ROOM UPGRADES AND NEW CONTROL ROOM DESIGNS FOR NUCLEAR POWER PLANTS

Ø BERG
Institutt for energiteknikk
OECD Halden Reactor Project

Abstract

Computer-based solutions for instrumentation and control systems replace old analogue equipment in nuclear power plant control rooms and CRT-based human-computer interfaces replace conventional control and instrument panels At the same time designs for tomorrow's reactors are developed characterized by fully digital instrumentation and control systems, and advanced, computer-based control rooms These trends open possibilities for improving the support functions assisting operators in their cognitive tasks At the Halden Project efforts are made to explore these possibilities through design, development and validation of Computer-based Operator Support Systems (COSSes) which can assist the operators in different operational situations, ranging from normal operation to disturbance and accident conditions The programme comprises four main activities 1) verification and validation of safety critical software systems, 2) man-machine interaction research emphasizing improvements in man-machine interfaces on the basis of human factors studies, 3) computerized operator support systems assisting the operator in fault detection/diagnosis and planning of control actions, and 4) control room development providing a basis for retrofitting of existing control rooms and for the design of advanced concepts The paper presents the status of this development programme, including descriptions of specific operator support functions implemented in the simulator-based, experimental control room at Halden (HAMMLAB, HAlden Man-Machine LABoratory) These operator aids comprise advanced alarms systems, diagnostic support functions, electronic procedures, critical safety function surveillance and accident management support systems The different operator support systems developed at the Halden Project are tested and evaluated in HAMMLAB with operators from the Halden Reactor, and occasionally from commercial NPPs, as test subjects These evaluations provide data on the merits of different operator support systems in an advanced control room setting, as well as on how such systems should be integrated to enhance operator performance The paper discusses these aspects and the role of computerized operator support systems in plant operation based on the experience from this work at the Halden Project

1 INTRODUCTION

Even if nuclear power plants have a very good safety record, there is a strong motivation in all countries for further improvements Control room improvement is given high priority, and modern computer technology, used in the correct manner, has the potential of greatly improving operational safety

A number of weaknesses in old control rooms have been identified relevant information may be missing due to limited instrumentation, too much information (alarms) may make it difficult for the operator to diagnose the process state, wrong or inconsistent information may mislead the operator In addition, the operator could benefit from assistance in both diagnosis of problems, in action planning and in implementation of control actions

Techniques are available to improve on all points given above dynamic process models may supply relevant process information, alarms may be filtered and presented more clearly and well structured, consistency check of process data before presentation helps identify wrong measurements Knowledge-based or model-based operator support systems may diagnose the cause of plant disturbance and identify which procedures are relevant Finally, computerized procedures may prevent the introduction of errors that often are experienced

At the Halden Project efforts are made to explore these possibilities through design, development and validation of Computer-based Operator Support Systems (COSSes) which can assist the operators

in different operational situations, ranging from normal operation to disturbance and accident conditions

These systems are implemented in the simulator-based, experimental control room at Halden (HAMMLAB), where they are tested and evaluated with operators from the Halden Reactor, and in some cases also with operators from the Loviisa NPP in Finland, as test subjects Through these experiments data on the merits of different operator support systems in an advanced control room setting are obtained Further, studies of how the systems should be integrated in the existing control room to provide efficient operator support are carried out Adding new COSSes may increase the information in the control room, resulting in increased danger of information overflow, if information structuring and presentation are not properly designed The man-machine interface of the COSSes should be standardized, and care must be taken to avoid that the operator is so involved in the use of one particular COSS that he overlooks more important tasks to be performed

This paper gives an overview of the man-machine systems research and a brief description of a number of the COSSes developed at the Halden Project, and discusses aspects of system evaluation and integration before such systems are taken into use in plant operation

2 MAN-MACHINE SYSTEMS RESEARCH AT THE HALDEN PROJECT

The research programme at the Halden Project addresses the research needs of the nuclear industry in connection with introduction of digital I&C systems in NPPs The programme provides information supporting design and licensing of upgraded, computer-based control room systems, and demonstrates the benefits of such systems through validation experiments in Halden's experimental research facility, HAMMLAB and pilot installations in NPPs

The programme includes four main areas 1) verification and validation, 2) man-machine interaction research, 3) computerised operator support systems, and 4) control room development Fig 1 illustrates how these areas are interconnected and also shows the type of deliverables from the different areas

The activity on *verification and validation* addresses software safety and reliability aspects The work comprises investigations of methods and tools which can be used to improve the reliability and verify the safe use of computerised control and supervision systems for nuclear power plants The results provide a basis for establishing guidelines for design and licensing of safety related software

The work in the *man-machine interaction* area aims at enhancing safe and efficient operation of nuclear power plants through improving the man-machine interfaces of the control room systems based on human factors considerations To this end experimental evaluation of the systems is performed in HAMMLAB using operators from the Halden Reactor as test subjects In addition to improving the man-machine interface of the specific operator support systems being developed at Halden, the analyses of these validation experiments provide a more general understanding of factors influencing operator behaviour This knowledge is utilised to establish technical bases for guidelines for design and evaluation of man-machine interfaces

The work on *computerised operator support systems* addresses development of systems assisting the operator in functions like fault detection, diagnosis and prognosis, and advisory systems aiding him in action planning and implementation The work in this area is primarily aimed at developing systems for backfitting in current control rooms, but the resulting systems are also applicable as modules within more integrated surveillance and control systems in advanced control rooms

The activity in *control room development* addresses the potentials and possible problems of completely computer-based control rooms including several operator support systems The work comprises integration of these systems focusing on co-ordination and prioritisation of information, man-machine interfaces and underlying hardware/software structures A demonstration version of a fully digital control room is established in HAMMLAB This demonstration control room is utilised to gather information of relevance for the introduction of digital control room solutions in nuclear power plants

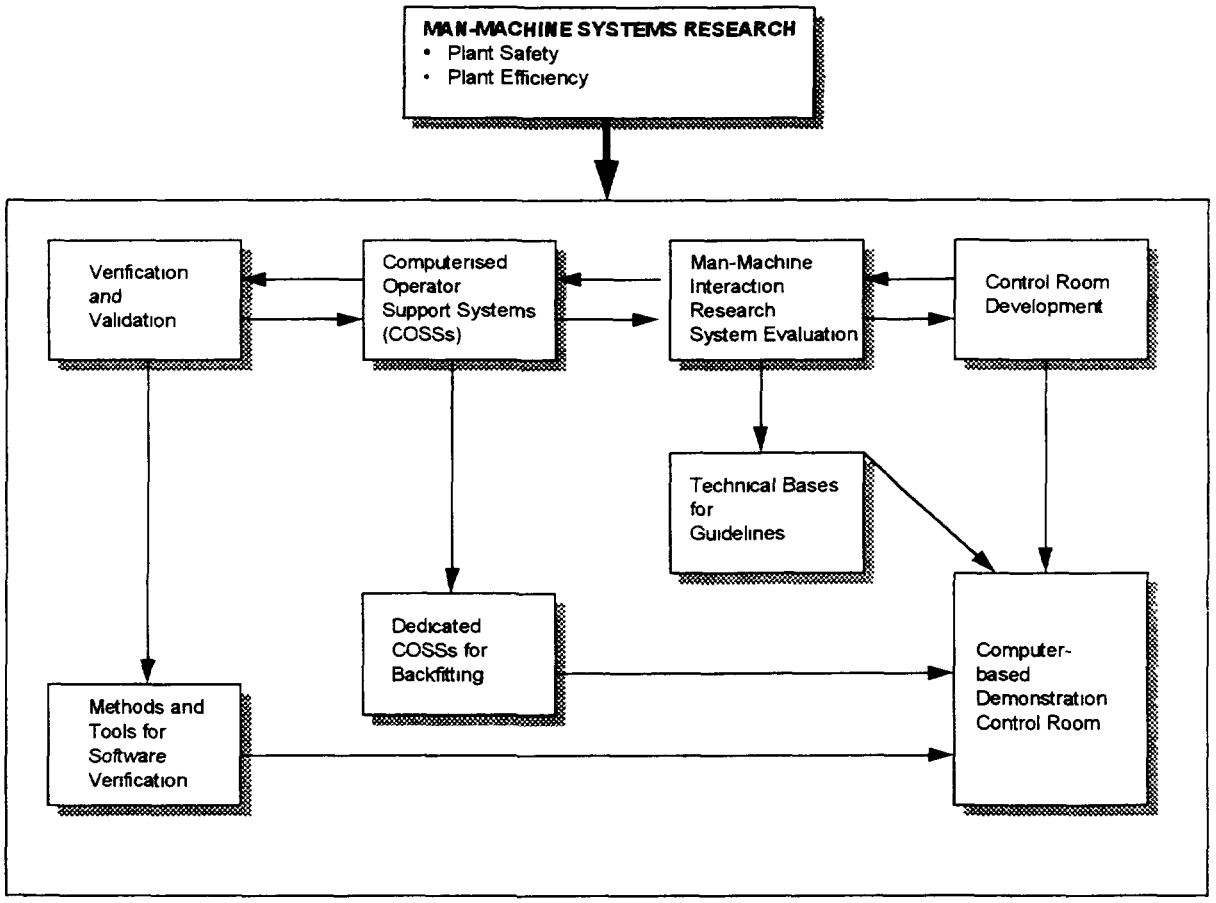


FIG. 1. Man-Machine Systems Research Programme. Upper four boxes show the four main programme items, lower four shows the main products from the research programme at Halden.

3 COMPUTER-BASED OPERATOR SUPPORT SYSTEMS DEVELOPED AT THE HALDEN PROJECT

5.1. Model-based early fault detection

Early detection of faults and plant disturbances in nuclear power plants reduces the risk of disturbances developing into severe plant conditions (shutdown or accidents) since the operators have more time for diagnosis and counteractions. Further, early detection of the disturbance usually means better localisation 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 limit 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. Therefore, the operator is confronted with a large number of alarms within a short period of time which makes the diagnostic task difficult Alarm filtering techniques may reduce this problem to some extent by focusing on essential alarms [1].

An alternative method for fault detection is illustrated in Fig. 2. The method is based on mathematical reference models describing the dynamic behaviour of the process in normal operating conditions (no disturbances or faults in the process). By comparing measured process variables with corresponding calculated variables from the reference models in real-time, the time to detect disturbances can be reduced compared to traditional alarm systems. By splitting the reference models into a number of submodels where the input variables to each individual submodel are measured output variables from the preceding subprocess (Fig. 2), a good localisation of the problem area in the plant is obtained. By this technique, propagation of faults in the detection algorithms outside the particular subsystem containing the fault, is avoided thus reducing the diagnostic task [2]. However, also this method requires additional rules for detailed diagnosis in order to discriminate among various possible failures within a subsystem which may cause an observed deviation between reference models and

measurements For instance, errors in the control system or instrumentation may turn out to be the real problem, but this type of failure should also be detected as early as possible

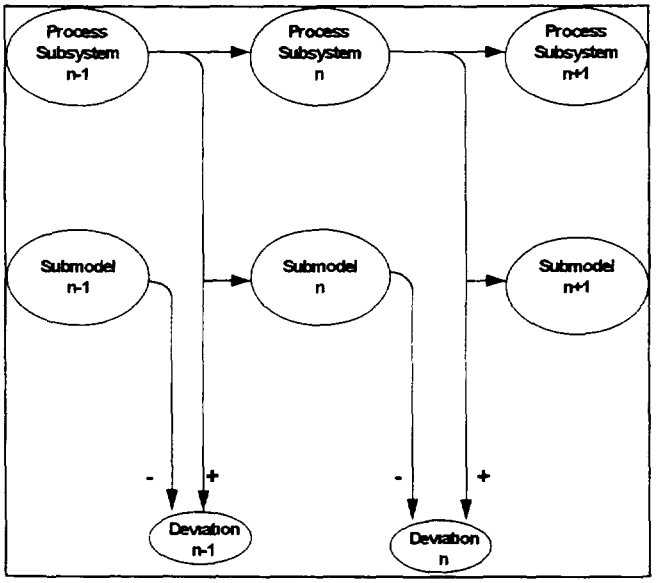


FIG. 2. The principle of model-based early fault detection.

At the Halden Project Early Fault Detection (EFD) systems based on the method described above have been developed Two pilot installations have been made at the Loviisa nuclear power plants in Finland, one for leakage detection and one for signal validation of flow sensors The systems have proved successful through detecting internal leakages in preheaters in the feedwater system and degradation of feedwater flow instruments [3,4]

5.2. Surveillance of critical safety functions

In case of major disturbances in nuclear power plants 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 kind 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 amount of alarm messages even in situations where you have a moderate plant disturbance The presentation of unimportant information mixed with important information may in fact be misleading to the operator Further, an event-oriented alarm system tends to draw the operator's attention to problems with individual components while his attention in accident situations rather should be directed towards the performance of critical plant functions

These problems have resulted in a function-oriented approach to nuclear power plant monitoring for disturbances which potentially may develop into accidents From systematic studies 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 of the disturbance, like staff injuries and plant damage

This function-oriented approach to plant monitoring has lead to development of so-called Safety Parameter Display Systems (SPDSs, also denoted Critical Function Monitoring Systems) which alarm the operators when critical safety functions are threatened The emergency operating procedures (EOPs) have been restructured accordingly, the EOPs of nuclear power plants are now all symptom-based (i e function oriented) and aim at checking the status and maintaining the integrity of the critical safety functions

The Halden Project has explored the concept of critical safety function monitoring through development and evaluation of different SPDS-types of systems Together with Combustion Engineering the Halden Project evaluated the Critical Function Monitoring System (CFMS)(and the Success Path Monitoring System (SPMS) in HAMMLAB [5] The SPMS system augments the monitoring of the critical safety functions through presenting to the operator the status of alternative success paths for maintaining a particular critical function in case it is threatened or lost The experiments in

HAMMLAB showed clear advantageous effects of supporting the operator with success path monitoring with respect to his performance during simulated accident scenarios .

5.3. Intelligent alarm handling

One of the main tasks for operators in nuclear power plants is to identify the status of the process when unexpected or unplanned situations occur. The alarm system is the main information source to detect disturbances in the process, and alarm handling has received much attention after the TMI accident in 1979. It was realized that conventional alarm systems created cognitive overload for the operators during heavy transients.

Over the years the Halden Project has explored different approaches to alarm handling, like alarm filtering techniques, model-based early fault detection and function oriented approaches like critical safety function monitoring.

The experience gained from the work with these different alarm systems has shown that there is a need for a generic tool for configuring more intelligent alarm systems where different alarm handling techniques can be integrated. Therefore, the Halden Project has developed an alarm system toolbox, called COAST, which makes it possible to build integrated alarm systems through mechanisms for addressing different principles for alarm generation, structuring and presentation [6].

COAST contains facilities for building specific alarm systems as well as facilities for alarm system execution. It is an integral part of the final alarm system, and is not only a tool for building dedicated systems. COAST is shown in its final environment in Fig. 3.

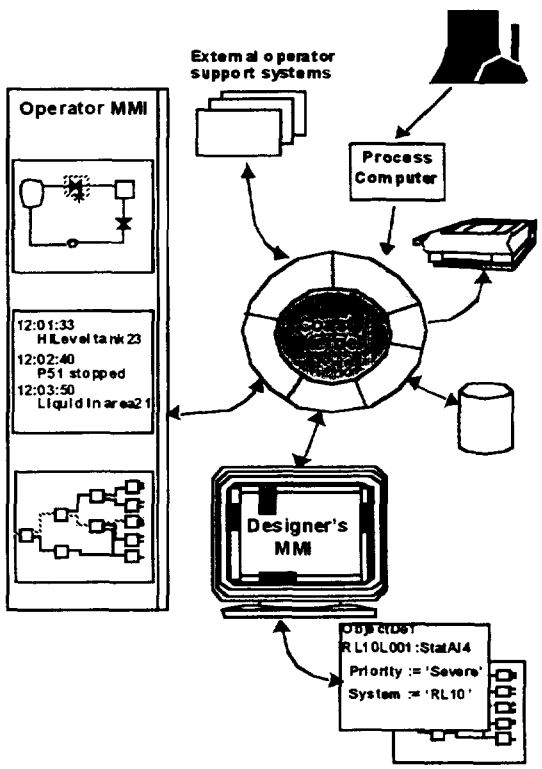


FIG. 3 The COmputerised Alarm System Toolbox, COAST, with interfaces to external systems

COAST is meant to be an add-on possibility to conventional process control systems. As shown in Fig. 3, it receives process measurements from the process computer, updates all necessary statuses, and sends updated alarm information to the display system in the control room. COAST itself does not possess graphic capabilities, but can easily be coupled to different graphical systems. It has been coupled to the Picasso-3 user interface management system developed in Halden [7]. Coupling to all external systems is done through an application programmer's interface, which includes simple functions to get data in and out of COAST, e.g., process data must be provided as input to the alarm objects. It is also easy to couple COAST to an existing alarm system. Existing alarms will then be structured or

filtered by COAST before presentation The designer's MMI is designed as an alarm editor, but it is also possible to operate COAST through text-files

An advanced alarm system called CASH (Computerized Alarm System for HAMMLAB) [8] has been developed using the COAST alarm system toolbox and installed and tested in the PWR simulator-based experimental control room at Halden New methods for alarm structuring and presentation are introduced, which together with established ones provide a high degree of suppression of non-important alarms CASH introduces an innovative overview display which combines advantages of space-distributed tile alarm systems and CRT based systems with chronological alarm list No information is removed from the system, only suppressed from the overview display according to well-defined criteria However, all alarms and additional information are available upon request in so-called selective displays Alarm information is also integrated into process mimics displays used for process control and surveillance

5.4. Diagnosis systems

At the Halden Project prototypes of diagnostic systems have been developed to investigate their merits for NPP operation DISKET is a rule-based expert system where information on patterns of the actual alarms and other process variables are matched with precalculated patterns from known disturbances to arrive at hypotheses for the cause of the alarms The system was originally developed by JAERI (Japan) and further developed at Halden DISKET has been validated in HAMMLAB, and the results show improved operator performance when the operators have access to DISKET during disturbances [9]

Detailed Diagnosis (DD) has been developed to perform diagnosis of alarms originating from the Early Fault Detection (EFD) system The diagnosis is based on knowledge based techniques Typically the results will be identification of failed components, control system failure or instrument malfunctions

Currently the Halden Project is working on an Integrated Diagnosis System aiming at utilisation of the experience from already developed diagnosis systems to make a general framework for diagnostic systems, incorporating important qualities of the previously developed systems In this way, more robust systems will be obtainable due to the diversity in diagnostic methods and knowledge [10]

5.5. Computerized procedure system

A number of observed and potential problems in the nuclear industry is related to the quality of operating procedures Especially when it comes to EOPs, much work has been done in recent years for improving their quality This applies to most aspects related to procedure production, procedure structure and contents, procedure implementation and procedure maintenance

Many of the problems identified can be directly addressed by developing COmputerised procedure handling tools Thus, there is a growing interest in taking modern computer technology into use for improving today's practice in procedure preparation, implementation and maintenance

COPMA-II is a computerized procedure system developed at the Halden Project [11] The system has two main components *the procedure editor, PED-II*, is a tool designed to be used by the procedure writers during procedure preparation and procedure maintenance Procedures to be used with COPMA-II must be expressed in a formal, general purpose procedure language, PROLA, developed by the Halden Project *The COPMA-II On-line procedure following system* is the tool developed for supporting the process operators during retrieval and execution of procedures The term *on-line* reflects that the system is designed to work with a live data communication link to the process computer, simulator, or any other external software component Fig 4 illustrates the relationship between PED-II, COPMA-II On-line and the plant computer or simulator

COPMA-II is intended to *replace* the traditional system of paper-based procedures Existing hard-copy procedures must be transferred to COPMA-II by using the procedure editor A more or less thorough rewriting of the procedure using the PROLA procedure language is necessary There are *no* elements of automatic procedure generation or procedure synthesis during on-line operation

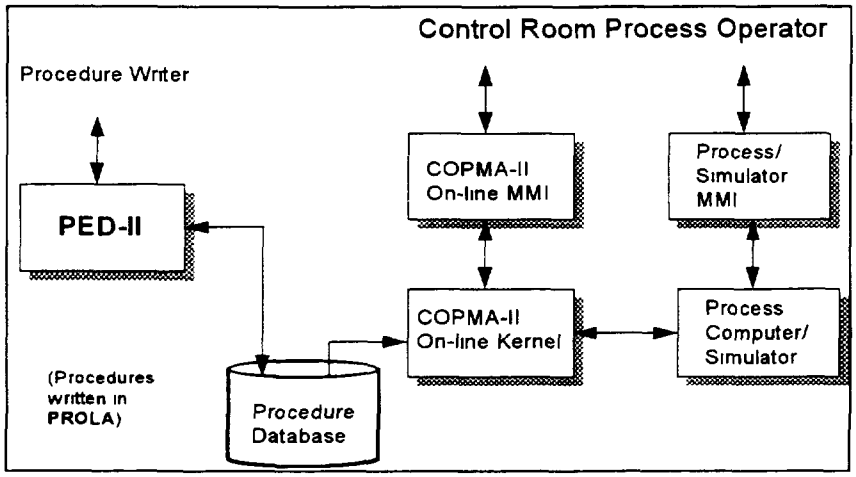


FIG. 4 COPMA-II system components

COPMA-II acts as a *shell* for storing procedural information, for access and implementation by the operating crew As designed, COPMA-II is not supposed to automate the actual execution of procedures Normally, the operator drives the execution by acknowledging individual instructions within the procedure, making his personal judgments as much as he did when using hard-copy procedures COPMA-II may also, if permitted to do so, act as a partial control interface to the process, because certain actions specified in the procedures can be carried out directly through the COPMA-II On-line user interface The integrated information available in COPMA-II combined with the support functions offered by the system, is intended to improve operator performance when implementing operating procedures compared to when doing the same job with paper procedures

COPMA has been subjected to human factors evaluation experiments in HAMMLAB using Halden Reactor operators as test subjects and at the Scaled Pressurized Water Reactor Facility at North Carolina State University where 16 licensed NPP operators were test subjects These studies have shown that operators can increase their performance and reduce their error rates when using COPMA, compared to using paper-based procedures

5.6. Computerized accident management support

The Halden Project is carrying out a research programme on Computerized Accident Management Support (CAMS) The aim is to establish a prototype of a system which can provide support to the control room operators and the staff in the Technical Support Centre during accident situations The CAMS prototype utilises available simulator codes and the capabilities of computer-based tools to assist in identification of plant state, prediction of future development of the accident, and planning of accident mitigation strategies [12,13]

The CAMS prototype consists of a signal validation module, a tracking-mode simulator, a state identification module, a predictive simulator, a strategy generator, a PSA risk monitor, and a man-machine interface system, see Fig 5

The signal validation module utilises neural networks techniques The tracking-mode simulator will be used to support signal validation and for state estimation There are a lot of physical quantities that cannot be measured If there is enough data available, they can still be calculated The tracking-mode simulator is supposed to take care of that

The predictive simulator predicts what will happen in the plant in the future The future will depend not only of the present state, but also of the planned control actions Many situations with different control actions can be tested, as well as the proposals from the strategy generator and from the users

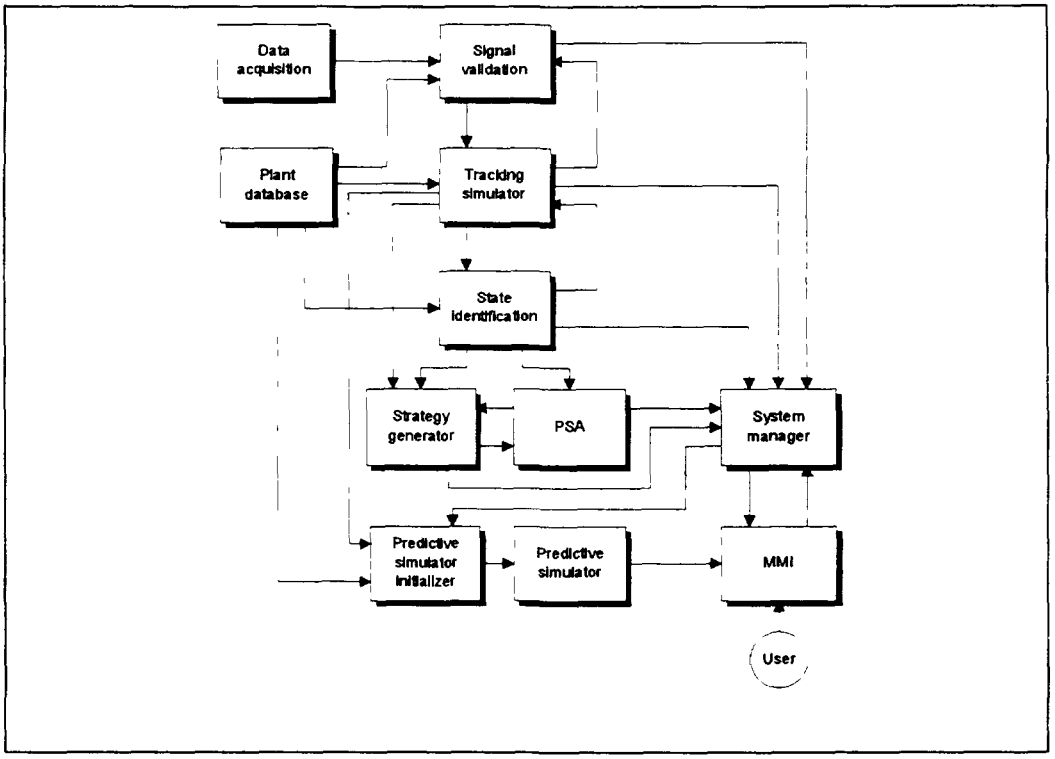


FIG. 5. Block diagram of the CAMS system.

The strategy generator shall provide control proposals and accident mitigation strategies to operators, shift leaders and to the staff of the technical control centre. A PSA module is used for risk monitoring taking into account the current state of the plant.

The users interact with the system through the man-machine interface. Much work is devoted to finding what information to display in different situations and how this information shall be represented.

A first prototype of CAMS comprising the predictive capabilities has been developed, and was tested in a safety exercise in Sweden in co-operation with the Swedish Nuclear Inspectorate (SKI). The test illustrated the potentials of a system like CAMS for accident management training.

5.7. User interface management systems

User Interface Management Systems (UIMSs) are tools to realise graphic user interfaces (GUIs), i.e., presentation of dynamic process information and handling of operator dialogues. The Picasso system is a UIMS tool developed at the Halden Project which is used in development of the GUIs of most of the COSSs described in this paper.

The latest version, Picasso-3, supports object-oriented definitions of GUIs in a distributed computing environment. The system comprises an interactive graphic editor for drawing pictures, generating class libraries and dialogues, and a C++ inspired programming language for defining advanced picture dynamics [7].

4. EVALUATION OF COMPUTER-BASED OPERATOR SUPPORT SYSTEMS

The development of COSSes at the Halden Project has clearly shown the potentials for improved plant operation through taking more advanced operator aids into use. However, introduction of these systems in a NPP control room requires that the systems are thoroughly evaluated with respect to the impact on operator role and performance. The essential role of the operator is to maintain the safety of the plant. Since COSSes obviously have the capability to effectively change some aspects of the role of the operator, we must carefully consider whether such changes are desirable. Further, as improvements in overall performance of the operator crew is the objective of developing and introducing COSSes in the control room, a continuous evaluation must be performed during design and implementation of these systems to assure that this objective is met.

The Halden Project is engaged in defining measurable objectives for operator support systems to enable experimental validation of specific operator aids Although an ideal way to validate systems might be to measure real operator performance in the actual control room situation, this is not feasible because appropriate incidents for system testing are fortunately rare (or not occurring) in real plants The most realistic way to validate the COSSes are thus evaluation in a full-scale simulator, where real conditions should be simulated as accurately as possible All COSSes developed at Halden is validated in this way through experiments in HAMMLAB where operators from the Halden Reactor or occasionally from the Loviisa NPP in Finland are taking part as test subjects In some cases experiments in HAMMLAB are supplemented with experiments in training simulators of member organizations of the Halden Project, to provide additional data, e g , comparisons between conventional and more advanced control room settings Over the years a broad spectrum of evaluation methods has been developed and enhanced to observe and validate human factors characteristics of the COSSes in a best possible way Important factors which must be considered are system user (operator, shift supervisor, technical support centre), workload, automation degree (allocation of task to system or operator), operators' situation awareness, information load, information separation (separate events clearly distinguishable), etc

In addition to providing design feedback on a specific COSS, the evaluations also provide more generic data of importance for formulation of guidelines for man-machine systems design In order to facilitate this work the experience from the system evaluations at Halden has been collected and summarized in lessons-learned reports [14]

In advanced, fully-digital control rooms the possibility exists for integration of a number of different operator support functions This poses a special challenge, namely that of proper co-ordination of the different functions One must avoid that the operator is so involved in the use of one COSS that he overlooks more pressing problems when they occur The control room must be conceived as a balanced entity, not as a collection of COSSes

A set of requirements follow from this a top-down design taking care of the co-ordination and prioritization of different tasks and functions must be followed Further, a unified, standardized man-machine interface including all COSS functions must be designed At the Halden Project a prototype of such an integrated solution to an advanced control room comprising eight different COSSes has been developed and thoroughly evaluated in operator experiments [15], providing useful information for design and implementation of this kind of control rooms

5 CONCLUSIONS

The upgrading of NPP control rooms with introduction of new plant computers and digital I&C systems opens possibilities for assisting the operator through developing computer-based operator support systems (COSSes) At the Halden Project a number of such operator aids have been developed and evaluated through experiments in the experimental control room HAMMLAB with operators from the Halden Reactor or commercial NPPs as test subjects

These evaluation studies as well as feedback from installations of COSSes in NPPs and other process industries have shown that benefits with respect to both plant safety and economy can be obtained through introducing COSSes in the control rooms

It is, however, absolutely necessary to perform a careful evaluation and validation of the systems with respect to their usefulness in a control room setting before introducing such operator aids in a NPP control room This requires utilisation of different methods for man-machine systems evaluation both in the design and implementation phases A final validation in realistic full-scale simulators with competent operators as test subjects is highly recommended to assure that the introduction of the COSS(es) really facilitates the operators' tasks, without endangering his essential role of maintaining plant safety

REFERENCES

[1] MARSHALL, E C , REIERSEN, C S , ØWRE F , "Operator Performance with HALO-II Advanced Alarm System for Nuclear Power Plants - A Comparative Study" ANS Topical

Meeting on Artificial Intelligence and Other Innovative Computer Applications in the Nuclear Industry, Snowbird, Utah (1987)

[2] BJØRLO, T J , BERG, Ø , GRINI, R E , YOKOBAYASHI, M , "Early Detection and Diagnosis of Disturbances in Nuclear Power Plants" ANS Topical Meeting on Artificial Intelligence and Other Innovative Computer Applications in the Nuclear Industry, Snowbird, Utah (1987)

[3] JOKKINEVA, H , LILJA, M , SØRENSSEN, A , "Early Fault Detection in a Real Nuclear Power Plant by Simulation Methods" ENC'90, Lyon, France (1990)

[4] BERG, Ø , BYE, A , SØRENSSEN, A , JOKKINEVA, H , "Early Fault Detection and Signal Validation at the Loviisa Nuclear Power Plant" ANS Topical Meeting AI'91-Frontiers in Innovative Computing for the Nuclear Industry, Jackson, Wyoming (1991)

[5] MARSHALL, E C , BAKER, S M , REIERSEN, C S , ØWRE, F , GAUDIO JR , P J , "The Experimental Evaluation of the Success Path Monitoring System" IEEE Fourth Conference on Human Factors and Power Plants, Monterey, California (1988)

[6] BYE, A , STORBERGET, T W , HANDELSBY, F , NILSEN, S , "COAST, a System for Advanced Alarm Handling and Interactive Alarm Analysis" Paper presented at the ANS-meeting, Philadelphia, Pennsylvania (1995)

[7] BARMSNES, K A , JAKOBSEN, Ø , JOHNSEN, T , RANDEM, H O , "Developing Graphics Applications in an Interactive Environment" 1994 SCS Simulation Multiconference, San Diego, California (1994)

[8] FØRDESTRØMMEN, N T , MOUM, B R , TORRALBA, B , DECURNEX, C , "CASH An Advanced Computerised Alarm System" Paper presented at ANS-meeting, Philadelphia, Pennsylvania (1995)

[9] HOLMSTROM, C B O , VOLDEN, F S , ENDESTAD, T , "Continued Experimental Evaluations of a Diagnostic Rule-based Expert System for the Nuclear Industry" ANP'92 International Conference on Design and Safety of Advanced Nuclear Power Plants, Tokyo (1992)

[10] GRINI, R E , KÅRSTAD, T , "Integration of Diagnosis Techniques" Meeting on Expert Systems and Computer Simuation in Energy Engineering, Erlangen, Germany (1992)

[11] TEIGEN, J , NESS, E , "Computerised Support in the Preparation, Implementation and Maintenance of Operating Procedures" 2nd IFAC Workshop on Computer Software Structures Integrating AI/KBS Systems in Process Control, Lund, Sweden (1994)

[12] SØRENSSEN, A , "Status and Plans for the CAMS Project (Computerised Accident Management Support) at the Halden Project" IAEA meeting on the Role of PSA and PSC in NPP Safety, Vienna (1995)

[13] BJØRLO, T J , SØRENSSEN, A , BERG, Ø , SCOT JØRGENSEN, U , SIROLA, M , ØWRE, F , ÅDLANDSVIK, K A , "Combining Simulation and Improved Presentation Techniques to Support Accident Management Decisions" ANS Topical Meeting on Nuclear Plant Instrumentation and Man-Machine Interface Technologies, Oak Ridge, Tennessee (1993)

[14] HALLBERT, B P , MEYER, P , "Summary of Lessons Learned at the OECD Halden Reactor Project for the Design and Evaluation of Human-Machine Systems" ANS-meeting, Philadephia, Pennsylvania (1995)

[15] FOLLESØ, K , FØRDESTRØMMEN, N T , HAUGSET, K , HOLMSTROM, C B , "ISACS-1, a Limited Prototype of an Advanced Control Room" IAEA Specialist Meeting on Advanced Information Methods and Artificial Intelligence in Nuclear Power Plant Control Rooms, Halden, Norway, (1994)

APPLICATION OF MODERN INFORMATION TECHNOLOGIES FOR MONITORING OF 600 RP KEY COMPONENT PERFORMANCE AND LIFETIME ASSESSMENT

S N KARPENKO, YU G KOROTKIH,
A A LEVIN, E I SANKOV
Research Institute of Mechanics of Lobachevski State University
Nizhny Novgorod, Russia

A B POBEDONOSTZEV, S L SHASHKIN
OKB Mechanical Engineering
Nizhny Novgorod, Russia

Abstract

Safety and reliability of NPP operation in the first turn depend on reliability and quality of the main technological equipment Diagnostics systems are envisaged for the equipment state inspection to determine its serviceability in NPP designs An assessment of the equipment residual lifetime at operating plants is calculated as a difference between specified (according to the operation model accepted in the design phase) lifetime and actual time in operation Real influence of operating modes on the main equipment lifetime, in this case, is not taken into account Within a design of NPP with VPBER-600 passive safety RP a system for lifetime assessment of RP key component is provided as a part of a process control system Specialists from OKBM and Scientific Research Institute of Mechanics participate in development of this system Now the first stage of the work on creation of this system is completed This paper describes the purpose, the basic configuration principles of the system, its position among other NPP systems, organization of user-system interaction

1 INTRODUCTION

In the process of implementation of new NPP projects a great attention is paid to safety, reliability and economical efficiency issues Safety and reliability of NPP operation in the first turn depend on reliability and quality of the main technological equipment Diagnostics systems are envisaged for the equipment state inspection to determine its serviceability in NPP designs

Diagnostics is subdivided into operational and a periodic one Operational diagnostics is performed in real time of the technological process and the results are used (can be used) for NPP preventive maintenance A periodic diagnostics is performed, as a rule, not in the real time, but often during the reactor shutdown In this case specific diagnostic methods can be applied, such as vibration-acoustic, acoustic emission, etc

The most wide-spread method for operational diagnostics is a parametric diagnostics The essence of the method is the following In the process of NPP operation such technological parameters as pressure, temperature, flow rate, etc are continuously monitored The information obtained is processed with the application of specific methods of analysis As a result, malfunctions in NPP equipment can be detected The results obtained are, as a rule, of a probabilistic nature

One of the most important aspects of a technical diagnostics is the assessment of the main technological equipment lifetime Being aware of the equipment residual lifetime the utility may plan preventive maintenance and repair works, including the equipment replacement

An assessment of the equipment residual lifetime at operating plants is calculated as a difference between specified (according to the operation model accepted in the design phase) lifetime and actual

time in operation Real influence of operating modes on the main equipment lifetime, in this case, is not taken into account

Within a design of NPP with VPBER-600 passive safety RP a system for lifetime assessment of RP key component is provided as a part of a process control system Specialists from OKBM and Scientific Research Institute of Mechanics participate in development of this system Now the first stage of the work on creation of this system is completed

This paper describes the purpose, the basic configuration principles of the system, its position among other NPP systems, organization of user-system interaction

2 PURPOSE OF THE SYSTEM

The purpose of the structural components lifetime assessment is to enhance safety and increase economical efficiency of the power unit operation by

1) Calculation of the exhausted lifetime for power unit equipment's structural units using actual operational history and residual life prognosis for anticipated operation programs
2) Analysis of calculated and predicted lifetime accuracy and the validity assessment
3) Identification of provisions for the increase of accuracy and reliability of the obtained estimates

The equipment lifetime assessment system is intended for

- Acquisition and accumulation of information about
  - effect of VPBER-600 operating modes on the process of accumulated damages in RP equipment,
  - history of VPBER-600 RP operation,
  - processes of materials degradation
- An assessment of the exhausted lifetime and prognosis of residual lifetime of the equipment in the process of operation
- Assistance in the analysis of the RP structural materials damage in order to make a decision on repair or extension of operating time

3 GENERAL APPROACHES TO LIFETIME ASSESSMENT

The methodology of the system lifetime assessment is based on a simulation of the equipment material damage accumulation processes on the basis of

- Selection of RP typical operating modes
- Experimental and numerical studies of the impact of these modes on the damage accumulation process in RP individual equipment units
- Simulation of a damage accumulation processes on the basis of
  - actual operating process analysis of the reactor plant equipment presented in the form of typical modes,
  - consideration of individual peculiarities of the RP equipment

The following tasks are solved sequentially and subsequently in accordance with general methodology defining the system construction strategy

1) In equipment, lifetime of which is subjected to an assessment, "critical points" are defined, i e those parts of the equipment which are mostly loaded in different operating modes The procedure for selection of "critical points" is an intellectual task and is based on strength calculations and generalization of the equipment operation experience, laboratory and full-scale studies and tests The scientific premise for selection of "critical points" is a theory of non-linear summing up of damage [1,2,3,4]

2) Various operating modes may effect similarly destruction process in an individual critical point In this case, basic technological parameters (pressure, temperature) influencing lifetime in the selected critical point, in various operating modes may have the same value and nature That is why typical modes are selected among operating modes specified by operating schedule from the viewpoint of their effect on the "critical points" state
3) Then, using numerical methods, effect of typical operating modes on the process of damage accumulation in "critical points" is calculated
4) Numerical model for lifetime calculations is objectively incomplete The following factors may be referred to as not taken into account
   - geometrical characteristics of actual units and technological features of their fabrication,
   - environmental effects,
   - basic assumptions accepted in description of the system (idealization of the equipment operation description, idealization of operating mode calculation scheme),
   - basic assumptions in a mathematical model (validity of state equations, etc),
   - statistical characteristics, etc
5) Effect of these factors may be sufficiently significant and an expert subsystem is envisaged for their assessment in the system design

Development and application of this expert subsystem have the following characteristic features [3]

1) Each expert knowledge base includes a set of generalized dependencies and parameters Their nature and values are specified on the basis of experience, known theoretical points, results of numerical simulation on large computers
2) Applicability conditions and reliability level are indicated for each dependence and parameter
3) qualitative analysis results for factors not taken into account in the operation calculation model of the system are reduced to the integral index of calculated lifetime deviation from the actual one
4) Assessment of deviation reliability is also derived as an integral reliability assessment of dependencies and parameters of database used to derive this deviation

Application of this expert subsystem provides qualitative assessment of influence of factors not taken into account in numerical simulation

In the process of the reactor plant operation, information on the current operating mode is sent to the process control system in the form of an attribute of control mode and its parameters Actual influence of operating mode on the equipment lifetime, if it does not conform to the specified one, is taken into account by the system by calculating with actual parameter values and applying expert knowledge base Total operational assessment of the main equipment exhausted lifetime is defined as an integral index of damage accumulation (with account of accumulation rate) in the equipment "critical points"

4 SYSTEM STRUCTURE

Lifetime assessment system comprises

1) A package of lifetime calculation codes including a set of modules (Mi) for lifetime calculations using different models of material life exhaustion
2) Expert subsystem for qualitative analysis of factors not taken into account in calculation models Expert subsystem includes a knowledge base comprising expert models from different fields of knowledge
3) Database to save information of two types
   - the object description - pre-prepared calculated and experimental information,
   - *the process description and calculation - information calculated in the process of the system* operation
4) Support means of dialogue interface with the user
5) System control means

A structure of lifetime assessment system for structural units of VPBER-600 RP equipment is shown in Fig 1

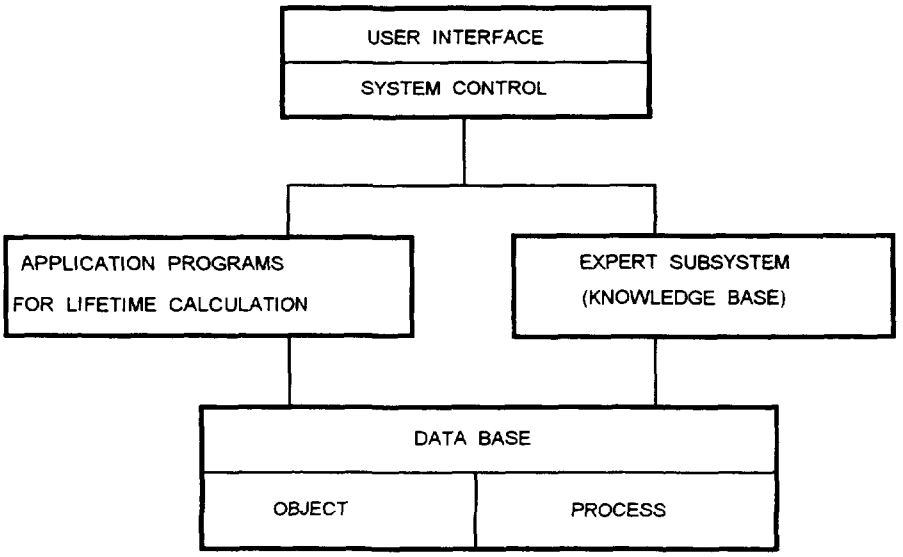


FIG. 1. Operational lifetime assessment system structure

Information about technological parameters and operating modes coming to the system is formed as a database comprising two large sections "OBJECT" and PROCESS" The "OBJECT" description contains

- description of the controlled equipment up to the level of "critical points".
- description of "critical points" properties,
- description (list) of operating modes,
- description of operating mode influence on the damage accumulation in "critical points"

The object description is obtained as a result of a study, during development phase, of VPBER-600 RP operating modes influence on the processes of damage accumulation in structural materials of its units and is introduced into the system prior to its operation onset at the object

The object description may be changed (supplemented, corrected, specified) in the process of the system operation Operation process description enters the system during its direct operation at the object (name of the operating mode, its parameters) The system output information is

- assessment of current damage (life) in "critical points" of the VPBER-600 RP controlled equipment for all previous operating modes,
- prognosis of damage assessment for a specified interval of time with account of possible operating modes,
- statistical characteristics of individual modes' influence on damage accumulation,
- various reference information stored in the system

5 INTEGRATION OF LIFETIME ASSESSMENT SYSTEM IN PCS

Main factors defining a position of lifetime operational assessment system of structural equipment components in PCS are

- correspondence of goals of the life assessment system to PCS goals,
- structure of system users,
- degree of the system output information effectiveness,

- nature of interaction between the system and other components of power unit CPS

From the point of view of relation to diagnostics system the lifetime assessment system is referred to means of local diagnostics The system may be referred to means of operational diagnostics taking into account a method of information acquisition The system is a means of periodic diagnostics from the point of view of the system application Thus, the system should be considered as an element of local periodic diagnostics because the system output information is not used by operator for power unit control

Input data for the life assessment system is a description of operation process Data about parameters of a technological process and operating modes used is kept in information-computing system (ICS) of the power unit Number of technological parameters values requested by the system may be excessive for PCS (i e , this information is not used anywhere) Data excess may result in groundless overflow to ICS data base and increased load for communication channels So, it is advisable to receive from ICS only values of parameters controlled by PCS The missing values should be calculated by lifetime assessment system In this case data base of lifetime assessment system according to RP equipment operation history is arranged an autonomous part of the system Potential users of lifetime assessment system are

1) Diagnostics engineer controls onset of ultimate (according to strength lifetime) state in RP equipment controlled units
2) Power unit shift head may use prognosis of the equipment life expansion to select its operating modes
3) Specialists of intellectual support group (managers, designers, mechanical engineers) carrying out
   - studies for increase of power unit operating efficiency,
   - analysis of situation when achieving operational limits of the controlled equipment and elaboration of recommendations
4) Systems designers participate in supervision and refinement of the system

Basing on analysis of system tasks and functions, its operating mode, potential system users, system links with PCS it was noted that

- the system of lifetime assessment carries out only information functions,
- it is a part of ICS being a part of diagnostics system,
- system input information has abundance with regard to information tasks of ICS,
- system operation results are of passive (with regard to RP control) nature,
- system operation results are a consequence of intellectual information processing,
- there is a necessity for continuous development of the system

In connection with the above

1) The system is located in one of automated workstations (AWS) of the technical support centre
2) Main user of the system is a diagnostics engineer
3) The system is considered as autonomous PCS component designed for intellectual support for staff and operators Fig 2 shows the diagram with the location of lifetime assessment system in entire ICS structure

6 ORGANIZATION OF USER-SYSTEM INTERFACE

The main task of the system is to acquire information about occurring (accumulated) damage in structural components of RP equipment, about the effect of operating modes on damage accumulation process in the equipment, and assessment (prognosis) of a possibility and conditions for further operation of the equipment When implementing these tasks, diagnostics engineer interacts with information source in accordance with the user's needs

The information model of the controlled object and the information model of the operating process have been developed to facilitate user's work

The object information model incorporates

- RP information model
- Information model of the operating mode
- Information model of computation kernel

The RP information model reflects structural RP layout and is constructed using a hierarchical principle (it is converted in accordance with detail levels of structural layout) The RP information model incorporates a list of RP structural components and RP structural layout's graphic display structured in accordance with hierarchy levels List of controlled equipment has four levels of details

- Aggregate - structurally complex equipment component consisting of one or several units
- Unit - structurally simple component of an aggregate
- "Hazardous zone" - unit part most exposed to destruction process
- "Critical point" - place in the "hazardous zone" where destruction process originates

The operating mode information model consists of a list of technological operating modes and mode parameters The computation kernel information model is a set of parameters providing calculation of changes of material damage characteristic in one critical point for one operating mode The computation kernel information model is specified on the level "critical point - operation mode" Parameters are classified by type (number, function, etc) and kind (determined by physical nature) Specific content of the computation kernel information model is defined by used models of lifetime operational calculation

Description of operation process is divided into descriptions of operation intervals corresponding to sequential time periods Description of operation interval incorporates

- Interval period
- Operation model
- State of the controlled object (critical point) in the beginning of operating period,
- Final state of the controlled object in the end of operating period

Model of operation is formed as a sequence of descriptions of operating modes performed during this interval Description of operating mode contains mode number (code) and parameters User-system interface has provisions for

1) Representation on a display screen of
   - control object,
   - operation process,
   - lifetime calculation results,
   - lifetime calculation process,
2) Forecasting of lifetime exhaustion
3) Work with object operating history

Organization principles of user interface are unified within the framework of VPBER-600 RP[5] User interaction with the system is based on a hierarchical (text and graphic) menu providing an access to all information models of the system and a navigation through them in compliance with model structure Control of information presentation on a display screen is done by typical alphanumeric keyboard and/or sensor information input device of "mouse"-type

7 CONCLUSION

1 Application of technical diagnostics system at NPP makes provisions for personnel to acquire more accurate information about the equipment state and running technological process, in this way enhancing safety and increasing operation economical effectiveness
2 A system for lifetime operational assessment of RP equipment provides timely assessment of the equipment residual lifetime Application of expert knowledge base as a part of lifetime assessment system allows to increase accuracy of the system operation The information obtained allows to increase NPP operation effectiveness by timely repair and replacement of equipment with exhausted lifetime, making valid decision on extension of equipment operation schedule basing on its actual operation history
3 Information, obtained during operation of lifetime assessment system, allows to evaluate actual influence of operating modes on equipment structural materials loading, allowing to take this into account during design of new NPPs

Acknowledgment

Authors thank Academician F M Mitenkov, whose experience and results of activities in the field of theoretical basis for equipment lifetime assessment were used in development of operational lifetime assessment system

REFERENCES

[1] ZENKEVICH O S Finite element method in engineering, Moscow, Mir (1975) (In Russian)
[2] MITENKOV F M , KOROTKIN YU G , GORODOV G F , KARPENKO S N , Methodology for operational assessment of exhausted lifetime for engineering industry objects simulation of damage accumulation processes with application of new information technologies, DRAN, v 324, No 4 (1992) 765-768 (in Russian)
[3] GORODOV G F , KOROTKIH YU G , KARPENKO S N , "An integrated intelligent system for routine estimating the spent and residual life of NPP equipment Materials science problems by production and operation of NPP facilities" Trans of the second Int Conf 14-21 June 1992, St Petersburg, Russia (1992) 42-52
[4] MITENKOV F M , KOROTKIH YU G , SANKOV E I , KAZAKOV D A , KARPENKO S N et al "Determination and validation of residual life for mechanical engineering products during long term operation" Problems of mechanical engineering and reliability of machines No 1, (1995) 5-13 (in Russian)
[5] NOVIKOV V V , POBEDONOSTSEV A B , SHASHKIN S L "Basic principles of providing operator information support for control of VPBER-600 reactor plant" IAEA/IWG/ATWR&NPPCI Technical Committee Meeting Espoo/Helsinki, Finland (1994)

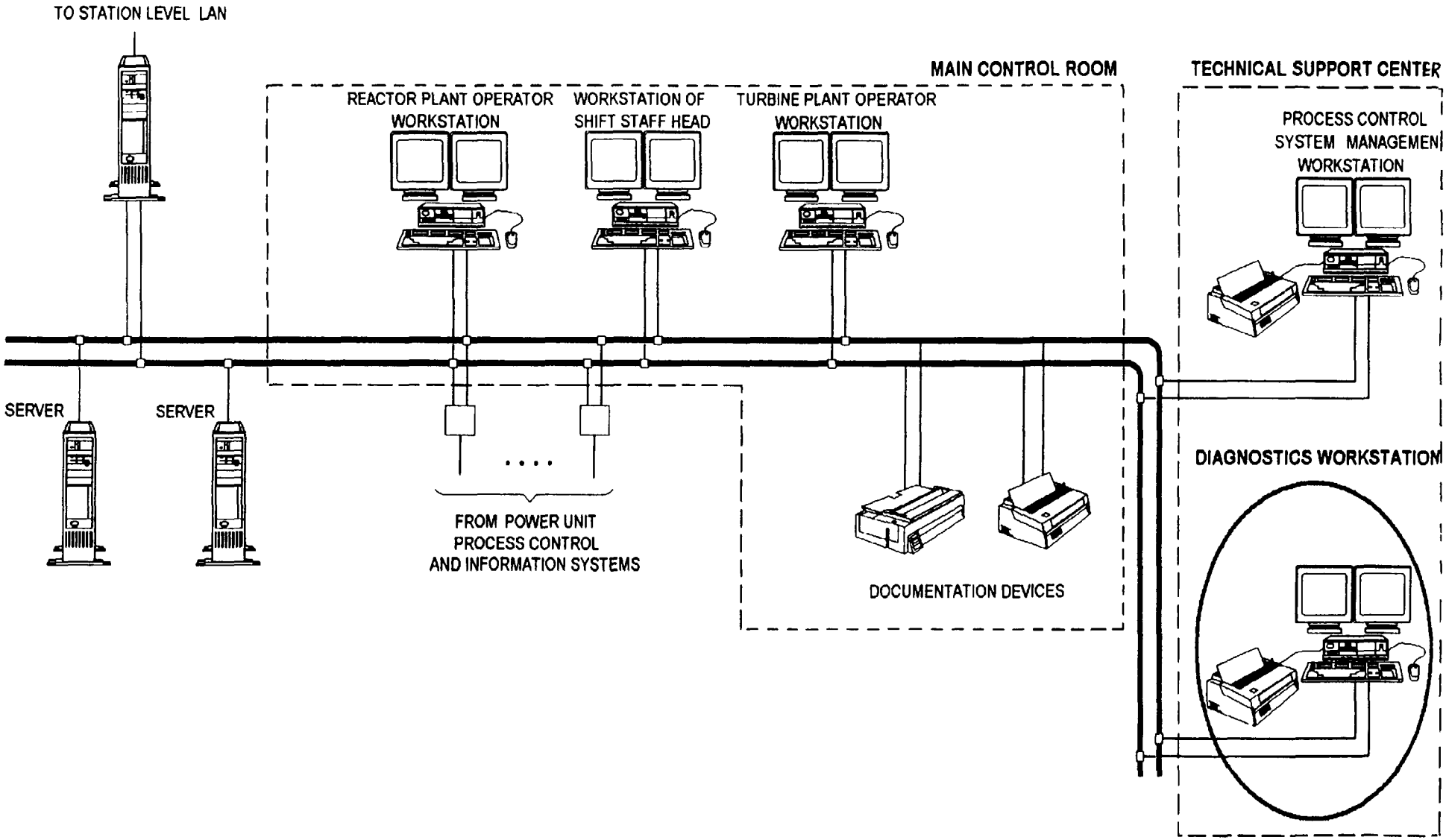


FIG. 2. Information and computation system of VPBER-600 power unit structure

CONTROL AND DATA PROCESSING SYSTEMS IN UK NUCLEAR POWER PLANT AND NUCLEAR FACILITIES

J A BALDWIN, D N WALL
AEA Technology
Winfrith, Dorchester
United Kingdom

Abstract

This note identifies some of the data processing and control systems in UK nuclear power plant, with emphasis on direct digital control systems and sequence control A brief indication is also given of some of the associated research activities on control systems and software

The plant in the UK use an extensive array of control systems, some functions are still performed manually e g power control at Calder Hall, others are supervised by quite complex analogue controllers The latest Advanced Gas cooled Reactors, AGR, make extensive use of direct digital control, while the Sizewell B PWR has one of the most advanced control rooms and control systems in the world

The first reactors at Calder Hall and Chapelcross were relatively simple plants Although they used a number of open and closed loop controllers, the reactor power and thus the coolant gas outlet temperature was under manual control The gas temperature was measured and, on the basis of the value, the operator moved the bank of four control rods to trim the power and maintain the temperature at the desired value Automatic power control was introduced on the Chapelcross reactors in the early 70's in order to reduce the number of operating staff The system was a fail-safe dynamic system implemented using Diode Transistor Logic This system is now approaching the end of life It is proposed to replace the equipment with a modern digital controller The same upgrade exercise is to be performed at Calder Hall which still retains the original manual control The plant have been subject to a number of other upgrades the most obvious of which is the appearance of Cathode Ray Tube, CRT, displays in the main control room These appeared when a computerized data collection and display system was introduced for the plant activity monitors

As the series of Magnox reactors were developed so the sophistication of the control, data collection and data display systems increased One aspect that appeared was the use of direct digital control and CRT displays These aspects were slow to be introduced however a major step forward came with the AGR reactors This was due in part to the effective use made of the Ferranti ARGOS computer hardware Initially the systems were installed on an individual basis with early use of the computers for alarm recording, alarm handling and display This was followed by direct digital control of the heating and ventilation plant When Hartlepool and Heysham I were completed, the whole of the start up sequence of the plant was performed under direct digital control This trend was continued in the design and construction of the latest AGR's at Torness in Scotland and Heysham II in England

The control systems at Torness and Heysham II contain over 1000 control variables and cover four main reactor plant areas These are as follows

- Control of core power generation by motion of the gray absorber rods assigned for automatic control
- Control of the coolant gas flow rate by regulation of the speed/guide vane position on the gas circulators
- Control of the feedwater flow This is performed on a total flow and an individual boiler basis The latter is to correct for asymmetries in the coolant gas temperature distribution

- Control of the turbine speed via regulation of the steam pressure and flow

There are a number of other control systems on the plant e g sequence control for the refuelling machine, control of feedwater temperature, start up and load sequencing for emergency power supplies, heating and ventilation system control

There are a number of options for control of the AGR as base load units The core heat generation rate is under closed-loop control which is achieved by dividing the core into a number of zones, each associated with a control rod The heat generation control parameter is the coolant gas temperature measured at the exit of the fuel channels in the zone There are two further key control loops The first control loop is for heat removal from the core and steam production The second control loop is for steam pressure and turbine control The steam production can be controlled by either forcing the flow rate of the coolant gas or forcing the flow rate of the feedwater In either case, the other parameter is under closed loop control

There is more difficulty with the second control loop as it is very sensitive as the once through steam generators contain little effective inertia There are two effective strategies First the setpoint of the turbine speed governor can be controlled control the steam pressure The unit load is then determined by forcing the rate of steam generation as load variations from the governor are eliminated The second option is to determine the steam pressure by controlling the feedwater pressure The unit load is then determined by the setpoint of the speed governor

The difficult of controlling the turbine boiler loop posses a major problem for the control system and for maintaining the plant in the event of a control system or a plant failure The direct digital control systems have allowed the latest AGR's to survive major transient including rod drop, loss of feedwater flow that normally result in loss of generation and plant trip

The development of the control systems by the two companies, Nuclear Electric and Scottish Nuclear, that operates the latest AGRs differ significantly, although both had identified the problems associated with generating and interpreting the specifications Nuclear Electric, formerly the Central Electricity Generating Board have long used a specially developed language CUTLASS for the development of control systems In contrast, the systems for Torness were developed using close control of the Quality Assurance and software development arrangements with an implementation in the CORAL language

It is interesting to comment on the operational performance of the automated control systems it is understood that it had at times been the practice of the operators to try to outperform the automatic systems by anticipating transients The plant performance has been found to have improved since this practice stopped

The data display systems have been developed with the evolution of the technology and kept pace with the control systems The design of the systems has required careful planning to ensure that the response time of the system is sufficient This has led to the need to look carefully at processor load and distribution of functions around the processors and displays The production of the displays and agreement of the displays with the plant operators form an important part of the system development and system acceptance Considerable care is required with the human factors and logic of the layout of the displays

The older plants have been backfitted with digital control systems and more are being introduced The turbine control of the Hinkley Point AGR is to be replaced with a digital system to improve plant performance While the improvement is expected to be small it is still sufficient to make the investment worthwhile

The direct digital control systems at Hartlepool and Heysham I have been improved with a digital controller installed for power raising The controller raises the power to 30% handling grid connection

and synchronization before control is passed to the direct digital control system This system is now used on a regular basis to take the reactors to power

The most significant digital backfit on an AGR is probably the installation of a computer based protection system on the Dungeness B plant The single channel trip system enables plant output to be increased from just over 400 to over 600 MWe per unit Part of the upgrade was the installation of a computer based monitor of the equipment performance that could also be used to monitor the thermocouple signals and to capture all the thermocouple data in the event of a plant trip

The monitor system running under DOS operating system was supplemented by a dedicated thermocouple health monitor that was used to investigate thermocouple performance The success of this system in investigating plant behaviour has resulted in a new health monitor being installed The new monitor runs under OS/2 operating system and captures and stores all thermocouple data on dual redundant optical discs The system can perform complex analysis functions e g using commercial spreadsheet and statistical packages and also output data to the station network for processing as required by the station SUN computers Some other plants have connected the power plant data collection system to the station network to allow data to be transferred and be used as input to physics calculations for fuel performance and reactivity

One area of digital control which was initially unsuccessfully employed was for fuel route control There were intrinsic problems with the safety case for on load refuelling of the AGR These arose from excessive vibration of the stringer as it was removed from placed into the channel There were further issues associated with potential failure of the control system that could result in the refuelling machine becoming stuck on the pile cap with an assemble part inserted into the core The problems arose in part because of concerns over the quality of the software and difficulty in substantiating the reliability claims This experience in this case of sequence control indicates that great care must be taken in developing control systems and particularly computer based systems It is necessary as part of the process of technology selection and system implementation to consider the needs of the operator and the regulatory requirements

Computer based control systems have been applied extensively in other nuclear facilities in the UK, these include nuclear chemical plant and fuel and transport flask handling facilities These application have extensive use of commercial Programmable Logic Controllers, PLC's Although simple to program using application specific programming languages including ladder logic and employing graphical programming interfaces their deployment has not been without difficulty The systems were implicated in a recent incident at British Nuclear Fuels, BNF, that occurred during non-active commissioning of plant Problems were also encountered in an incident during the commissioning of PLC controlled cranes in a waste handling plant Although neither case resulted in harm, the commissioning exercise revealed undesirable behaviour These examples clearly show the hazards associated with the development and deployment of computer based control systems

It is anticipated that future developments will see the introduction of more complex systems including

- tighter digital control to improve plant performance,
- improved displays and support systems for operators including alarm handling and plant fault diagnostics,
- more extensive distribution and use of historical and on-line plant data,
- the use of plant monitoring to track sensor and instrument performance to reduce the amount of calibration and maintenance required These developments are expected to lead to the introduction of preventive maintenance planned on the basis of the output from the monitoring systems

Considerable activity has been undertaken on the topics of direct digital control, operator aids and human-machine interaction Some has been through association with the Halden and Ispra laboratories, other work at simulators in the UK The latter is possible as the UK has always provided access to

plant simulators for training plant operators This provision includes simulators for prototype reactors such as Prototype Fast Reactor, PFR, and the Steam Generating Heavy Water Reactor, SGHWR, as well as for the Magnox AGR and PWR plant

Following difficulties with sequence control, a self-checking sequence controller was developed using digital, but not programmable technology The system works on the basis of pattern recognition looking at the pattern of the current inputs to check them against the reference pattern expected for the demanded state If the pattern compares correctly, then the controller can pass to the next state on demand In the event that a change is required the new sequence of controller outputs is established and checked via the pattern recognition logic If the match is found the commands are issued and the controller moves to the next state Once the state is reached, an immediate check is done of all inputs to ensure that the required state has been reached This check is again performed using pattern recognition

Fuzzy logic control has also been investigated One concern has been the state of some of the sensors and instrumentation particularly as they age or suffer from calibration drift between outages The latter is becoming more of an issue as the AGR reactors move to a three year outage cycle and there is less opportunity to perform calibration checks One of the approaches investigated was to used three value fuzzy logic to represent the state of an instrument as good, uncertain, and bad and assign a time dependent function to the probabilities These probabilities were reasoned with control algorithm and a weighting of the certainty that the proposed action would be correct In the case where the uncertainties were large, the possible alternative control action are identified The confidence in the predicted action and the sensitivity to prediction of an alternative control action due to sensor and instrument state could be used to determine if and what calibration action would be necessary The system would be appropriate for complex algorithms and would require historic data of sensor and instrument performance i e failure and drift if it were to be integrated into plant maintenance procedures

It was noted during the development work that a number of the complex control algorithms could accommodate the total loss of some inputs without having a significant effect on the control algorithm While such lack of sensitivity would be known from the control equations, it cannot easily be allowed for in a conventional control algorithm It was proposed that it could be accommodated within a rule based or a fuzzy logic based controller

One particular aspect of digital control when applied to safety systems i e class A of the IEC-1226 classification is that of software production The major nuclear control systems have been produced using CUTLASS a bespoke language developed and supported by CEGB (now Nuclear Electric) Other application specific languages e g CORAL, have also been used very successfully e g at Torness Should the control systems perform functions that cause the system to be placed in class A then it is expected to be much more difficult to deploy For example it is expected that the software would have to be subject to static analysis e g with MALPAS, source code comparison and extensive dynamic testing

Nuclear Electric have produced a comprehensive guide for computer based systems as an internal standard This document was re-issued following a period of trial use within Nuclear Electric, Scottish Nuclear Limited and AEA Technology This, along with IEC-880, remain the essential references for computer based protection and control systems in the UK although much is expected of IEC-1508 which is currently issued in draft form

Software research in the UK has been quite extensive Two nuclear related projects, the DARTS and the PODS experiments, have shown that much of the difficulties arise at the specification stage These problems would appear difficult to detect and expensive to repair The DARTS project also showed, on the basis of the four channels produced, that there was no significant difference in the ability of the different methods to identify specification problems and errors made during the development The use of mathematically formal methods did however appear to result in the detection problems and potential problems earlier than the conventional methods

CONTROL AND AUTOMATION TECHNOLOGY IN UNITED STATES NUCLEAR POWER PLANTS

BILL K H SUN
Sunutech, Inc
Los Altos, California, USA

Abstract

The need to use computers for nuclear power plant design, engineering, operation and maintenance has been growing since the inception of commercial nuclear power electricity generation in the 1960s The needs have intensified in recent years as the demands of safety and reliability, as well as economic competition, have become stronger The rapid advance of computer hardware and software technology in the last two decades has greatly enlarged the potential of computer applications to plant instrumentation and control of future plants, as well as those needed for operation of existing plants The traditional role of computers for mathematical calculations and data manipulation has been expanded to automate plant control functions and to enhance human performance and productivity The major goals of using computers for instrumentation and control of nuclear power plants are (1) to improve safety, (2) to reduce challenges to the power plant, (3) to reduce the cost of operations and maintenance, (4) to enhance power production, and (5) to increase productivity of people Many functions in nuclear power plants are achieved by a combination of human action and automation Increasingly, computer-based systems are used to support operations and maintenance personnel in the performance of their tasks There are many benefits which can accrue from the use of computers but it is important to ensure that the design and implementation of the support system and the human task places the human in the correct role in relation to the machine, that is, in an management position, with the computer serving the human In addition, consideration must be given to computer system integrity, software validation and verification, consequences of error, etc , to ensure its reliability for nuclear power plant applications

1 INTRODUCTION

1.1. Technology

Many nuclear power plants, which have been operating since the 1970s, are designed and manufactured based on technology from the 1960s Because of obsolescence, lack of original equipment manufacturer support, challenges to availability due to unnecessary plant trips, component reliability due to aging, and high maintenance and testing costs, analog-based instrumentation and control (I&C) equipment and systems are being replaced with digital systems in current nuclear power plants Furthermore, the technology for I&C hardware and software design and development are changing rapidly due to advancement in state-of-the-art technologies [1]

Computer technology has been playing an essential role in design, construction, operation and maintenance of nuclear power plants Digital technology has been increasingly recognized as a viable tool for fast and accurate processing of large quantities of data and information to support and enhance the human capability for monitoring, diagnosis, control, surveillance, and communications In light of the recent revolutionary growth of digital technology in the computer and electronics industries, there is promise for nuclear power plants to continue to apply that technology, not only to upgrade and prolong the life of existing power stations, but also to broaden its role in the system of future generations of power plants [2-9]

1.2. Important roles of human

Human activities and involvement are of critical importance in the operation and maintenance of nuclear power plants The issue of human reliability impact to safety has been widely recognized by the

world in the response to the nuclear accidents at the Three Mile Island Station in 1979 and at Chernobyl Station in 1986 Major lessons learned from these two accidents indicate that human error is a significant contributor to the overall plant risk

It is important to understand the role of humans in operation safety, and the relationship between human and computers Recent advances in human engineering and computer techniques in the fields of control, protection, testing, surveillance, communication and human-machine interface have offered tremendous opportunities to improve various aspects of the safety operations of nuclear power stations

Many functions in nuclear power plants are achieved by a combination of human action and automation Increasingly, computer-based systems are used to support operations and maintenance personnel in the performance of their tasks It is important to ensure that the design and implementation of the computer-based support systems place the human in an intellectually superior position with the computer serving the human In addition, consideration must be given to computer system integrity, software validation and verification, consequences of error, etc

2 HUMAN-MACHINE RELATIONSHIP

To achieve a balance between computer and human actions, the process of system design must consider each operational function in regard to either computer, human operation or a combination of human and computer The process is usually known in ergonomics literature as "allocation of functions" [10-11]

2.1. Functions which must be automated

The first consideration must be to examine any function for which a computer is mandatory The designer must identify all the functions which exceed the capabilities of human performance and can only be achieved using a computer The design must consider the long-term demands of the task, the required performance under the worst possible conditions, and the variability of the human operator Performance factors which will need to be addressed include required task rate, accuracy, repeatability and, in particular, the consequence of error Functions which exceed the capabilities of humans include

- Processing large quantities of data
- Tasks requiring high accuracy
- Tasks requiring high repeatability
- Tasks requiring rapid performance
- Situations in which the consequences of error are severe
- Situations in which errors cannot readily be retrieved or corrected

Typical applications in a nuclear power plant for which the use of computers will be necessary include data recording, analysis and archives Depending on the particular task performance requirements, in all such cases it will be easy to demonstrate that human capabilities would be exceeded if the resulting task were performed manually

When the decision has been made to use computers for a function, consideration must be given to supplementary tasks, such as maintenance and testing activities, which are required to allow the computer to perform its role [12] It is important that the benefit of using computers is not lost by assigning supporting functions to human actions where the performance of the computer system would be degraded owing to poor maintenance, or where human operators may have difficulties coping with the psychological impact of automation [13]

2.2. Functions which are better automated

Certain functions may be identified which, although lying within the capability of human performance, may be better assigned to a computer These include those functions which are lengthy,

require high consistency, high accuracy or involve a degree of risk to an operator Tasks which might result in boredom or monotony for an operator also fall into this category

Practical examples of computers being introduced to replace tedious or arduous human activities include the use of machines to carry out maintenance or surveillance activities, for example, steam generator examination Computers are also being used increasingly to carry out lengthy, repetitive testing, such as those required for the safety and protection systems Not only does this improve the role of the operator, but it also brings improvements in the consistency of testing and may allow it to be carried out more frequently

2.3 functions which should be allocated to humans

Functions which require heuristic or inferential knowledge, flexibility, etc , will need to be assigned to humans A function may be assigned to a human simply for lack of a precise specification, or some difficulty in producing one

A particular set of functions which must currently be assigned with the human operator is accident situations where human flexibility and high level skills are essential and the unexpected nature of the task makes specifying appropriate computer functions difficult or impossible

2.4. Control process of human operators

The philosophical framework of operator activities in a nuclear power plant control room, with respect to human engineering, may be described using Rasmussen's information model of the control process The control process of a human operator is generally categorized into three stages, (1) skill-based automatic response, (2) rule-based guided responses and (3) knowledge-based problem solving

There are many variables in a nuclear power plant that can lead to abnormal situations and incidents, such as, component failures, errors associated with design, maintenance, testing, etc These incidents can lead to initiation of events in various parts of a nuclear plant The control room crew rely primarily on the sensor readings and alarms to provide the status of the plant in order to control the events

In most transients or events, operators can detect the abnormal situation and execute control functions to stabilize the plant through automatic responses For handling complex transients or multiple events, the operator functions include validation of instrument readings, identification of equipment status, and following operation procedures to execute control actions through rule-based guided response However, in some low-probability complex events which fall outside the scope of routine operator skill-based training and rule-based operating procedures, the operators need to use knowledge-based problem solving techniques to evaluate and predict the next possible plant state and to define tasks for control of the plant The TMI-2 accident showed a situation where complex multiple events went beyond the skill-based and rule-based controls, degenerating into a severe accident when the operating crew was inadequately informed to recognize and control the accident correctly

3 APPLICATIONS OF CONTROL AND AUTOMATION TECHNOLOGY

Since the 1970s, computer application to operation of nuclear power plants has gained broad recognition The advance of digital systems application in broad areas of control and instrumentation has continued around the world Digital technology has been increasingly recognized as a valuable tool for support and enhancement of human capability in the areas of monitoring, diagnosis, control, protection, maintenance, surveillance and communication [14-24]

3.1. Plant process computer system

The plant process computer system provides the plant operators with critical operating parameters in normal and emergency situations This is a system of computer hardware and software that are

integrated together to acquire large amounts of plant data on a real time basis for the purpose of performing calculations and other functions like scan, log, and alarm, data archival and retrieval on a Central Processing Unit, and displaying data processing results through the system's Human Machine Interface (HMI) The real time data is gathered from field sensors located throughout the plant [23]

The applications software can be categorized broadly into the scan, log, and alarm, plant monitoring and performance, and man-machine interface functions The scan, log and alarm function serves to sample the plant instrumentation inputs and log each current value into the database This process includes converting the incoming signal to an appropriate engineering unit and then checking this value against various alarm limits to determine if the signal is valid and if it warrants further attention In addition, data are selectively archived for subsequent retrieval to support engineering analysis of historical events The plant monitoring and performance functions then process the database information to support operational monitoring and performance requirements The HMI provides the interface to the system for controlling these functions as well as to access information from them

3 2 INFORMATION SYSTEMS AND OPERATOR AIDS

In regard to operator aids, it is common practice for information features to be introduced as additional sources to those already available in the control room [15,16] They date back to the TMI-2 accident, where serious information deficiencies were observed The information system to comply with this situation was the Safety Parameter Display System (SPDS) [2] Its purpose was to indicate deviation of the defined Safety Parameters and to provide the subsets of important measurement values in order to assist the operator in reaching the safety goals The impact of the TMI-2 accident has resulted in the widespread adoption of similar SPDS functions in other countries The installation of computers and color graphic workstations is matched by the development of sophisticated application software modules, such as signal validation software [24], to be used as a preprocessor for the SPDS, and emergency procedure monitoring, to integrate the rule-based control functions with the SPDS [2]

The use of on-line computer systems, such as SPDS, in control rooms has two main goals to support human operators, information presentation and information generation [14-16] Video display units are normally used for information presentation The information can be shown in the form of system diagrams with inserted parameter values and plant states, trend curves showing the history of important physical parameters, and as listings of plant alarms in groups or according to their priority

In the course of development, such functions have often been implemented as stand-alone systems or operator aids, driven by the operational needs of a specific plant or by licensing requirements Typical examples are core power mapping systems, load following advisors and safety parameter display systems Today, these systems are normally integrated into the total station data processing and display system of current process computers as well as advanced control rooms

3.3. Control and automation

As the nuclear plants in recent years began to face problems due to technology obsolescence and the resulting unavailability of parts, the existing analog control systems have been gradually replaced by digital controllers, among which the design and implementation of fault-tolerant digital feedwater controllers were accomplished for both BWRs [20,21] and PWRs [22,25]

The fault-tolerant digital control systems offer unique capabilities including dual redundancy, signal validation for sensor inputs, man-machine interface, and control algorithms that handle bumpless transfer from low power to high power and plant dynamics The operating experience of these digital control systems demonstrated that they have not only improved operation reliability and availability by avoiding reactor scrams, but also reduced maintenance expenses

This use has grown, and more complex, non-linear control functions have been progressively included in nuclear power stations A wide range of standard firmware modules are now available for such

applications Computers have been used for distributed digital control (DDC) with great success in some countries since the 1970s The advantages of using DDCs are flexibility of control strategy and integration of control parameter schedules, giving wide control ranges The extensive, non-linearity behavior of the plant can be covered in this way For example, the transfer from startup feedwater control to the main feedwater control mode at a power of about 10%

The control functions needed to maintain station conditions of coolant temperature, steam generator level, feedwater flow, etc , are recognized as having a role in safety since they maintain the reference conditions used by all safety analysis studies and they have a post trip function in control of heat removal The use of computers for such control functions, therefore, may involve justification of their performance as suitable for a safety-related function

4 FUTURE PLANT CONTROL AND AUTOMATION SYSTEMS

Advanced control and automation technology will be an intrinsic part of future nuclear power stations A major program in progress which is sponsored by EPRI, U S utilities, several international utility companies, and the U S Department of Energy is the Advanced Light Water Reactor (ALWR) program [29,30]

4.1. Man-machine interface requirement

The ALWR program has placed significant emphasis on the appropriate use of modern technology for the Human-Machine Interface System Considerable experience has been accumulated regarding operation and maintenance of existing designs This experience provides opportunities to fundamentally improve the safety and operability characteristics of LWRs Breakthroughs in information and communication technology provide a real opportunity and challenge to exploit these capabilities in a manner that will provide benefits to the operator

A top level requirement for the human-machine interface system design is the coordination and complete integration of human-machine interface functions in a consistent manner for all conditions These key requirements call for the use of workstations with multiple computer devices for displays, controls and alarms where an operator may conveniently interact with all necessary control and monitoring features using electronically displayed procedures and other aids

The control room is conceptually designed to contain two redundant operator workstations, each incorporating multiple display, alarm and control devices, and a third identical supervisor workstation for monitoring only In addition, a large board that integrates display, alarm and mimic will be incorporated to complement the workstations

4.2. Displays and indication

Plant operational parameters and engineering data will be presented in graphical and diagrammatic format by means of multiple displays, showing present values, their trends, acceptable ranges, set points, etc These information will be presented in a coordinated manner consistent with the operators' decision-making approach to minimize selection and access time

Operators spend appreciable effort monitoring maintenance status and its impact on plant operations as well as performing configuration control tasks for plant equipment To support these tasks, electronically displayed piping and instrument drawings generated from computer-aided design software will be provided These diagrams will be logically organized for easy access and dynamically updated with equipment status information

4.3. Controls

One of the objectives of control room design is to reduce the size of the control panels to enable the operators to interface the plant through workstations This objective leads to the use of multifunctional controls that can be integrated into the workstation concept

The controls will be coordinated with the displays, alarms and procedures etc , to facilitate operators need for decision making and control executions The control system shall be designed with fault-tolerance features to promote efficient and reliable actuation and preclude inadvertent misactuation

4.4. Alarm systems

The ALWR human-machine interface system design process incorporates alarm input from component designers and additionally employs function and task analysis to develop an integrated alarm system which considers operator needs and capabilities within the context of the overall control room design

Alarm processing criteria provide methods and features to minimize nuisance alarms, reduce the number of alarms during upsets and provide a reflash capability for all multiple-input alarms Alarm presentation criteria are provided for location, grouping, type, display characterization, prioritization, and time sequence of alarms etc In addition, the alarm system will provide suggested cause and response information The information will include suggested procedures that the operator may wish to display and utilize to recover from the alarm conditions

5 CURRENT STATUS OF IMPLEMENTATION ISSUES AND CONCERNS

Today, the increasing obsolescence of nuclear power plant instrumentation and control systems threatens to weaken the nuclear industry's competitive position with other forms of electric power generation, which are rapidly converting their aging analog instrumentation and control systems to more powerful modern digital systems State-of-the-art digital control systems have demonstrated several advantages, including

- Increased system reliability and reduced maintenance costs through fault-tolerance, self-diagnostics, input signal selection, on-line replacement, and no onsite repair
- Improved control characteristics through adaptive tuning, drift-free operation, self-tuning, and nonlinear compensation
- Reduced operator burden through increased automation, improved human-machine interfaces, and expert systems
- Decreased future modification costs as changes are made in software rather than hardware

However, in spite of these distinct advantages, many nuclear utilities have been reluctant to upgrade their aging analog control systems to digital technology The risks perceived include

- Lengthy installation outage
- Possibility of increased trips during initial startup
- Resistance to change
- Desire for short payback period
- Impetus to drastically reduce capital spending

These factors have been intensified by the increase in the economic competitiveness of the power generation environment [31]

The implementation of technological improvements requires continual attention to human factors and cost effectiveness The users of computers must be brought into the developmental processes by review of plans and goals, by being part of the trials on simulators and related laboratory testing and by active participation in designing, executing, evaluating field trials and verification and validation of the system to ensure its quality for applications

A major challenge of integrated I&C upgrade in existing plants lies with implementing and documenting solutions developed for general applications to operating nuclear power plants, developing guidelines to stabilize the licensing process for I&C analog-to-digital upgrades and designing strategies to avoid excessive downtime for large upgrades at plant sites

The increased use of computers in nuclear power plants brings with it concerns about the reliability of the associated software Difficulties arising from software problems affect plant safety, reliability and availability Methodologies and tools on verification and validation are not only important to assure the quality of software, but also enhance the acceptance of computers by plant users and regulators through increased confidence in the software Lessons learned from implementation of safety-related software in the United States, Canada, and France point out the importance of the development of cost-effective methods for verification and validation

6 CONCLUSIONS

Applications of computer systems for display of the plant's state to the operators is now a common human-machine interface technology Operator aid systems with improved human performance in monitoring and diagnosis are being implemented in nuclear power plants world wide

Fault tolerant digital systems have been demonstrated to be effective automation and control technology for nuclear plant applications These controllers use redundant microprocessors and signal validation methods, and provide wide range algorithms with more optimized performance and higher reliability than the previous analog controllers They have been shown to reduce plant outages and trips, and reduce safety challenges to the plant

Computer-based systems for safety protection have been implemented successfully in several countries The extensive verification and validation required for assurance of software accuracy and integrity has been found to be very costly The need to address obsolescence of existing protection equipment and the attraction of better protection algorithms will increase digital protection applications

Large-scale application of computer technology will be intrinsic in future advanced nuclear plants Successful demonstrations of digital systems in existing plants and breakthroughs in telecommunication technology provide a real opportunity to exploit capabilities to the benefit of plant economics, reliability and safety

REFERENCES

[1] ELECTRIC POWER RESEARCH INSTITUTE, Integrated Instrumentation and Control Upgrade Plan, EPRI report NP-7343, Revision 3, December (1992)

[2] ELECTRIC POWER RESEARCH INSTITUTE, Proceedings 1986 Seminar on Emergency Responses Facilities and Implementation of Safety Parameter Display System, EPRI Report NP-5510-SR, November (1987)

[3] ELECTRIC POWER RESEARCH INSTITUTE, Proceedings 1986 Integrated Power Plant Computer Communications Seminar, EPRI Report NP-5641-SR, February (1988)

[4] ELECTRIC POWER RESEARCH INSTITUTE, Proceedings 1987 Conference on Expert System Applications in Power Plants, EPRI Report CS-6080, December (1988)

[5] ELECTRIC POWER RESEARCH INSTITUTE, EPRI Seminar on Data Acquisition, Control, and Communications in Power Plants, EPRI Report NP-6078-SR, November (1988)

[6] BERNARD, J A , WASHIO, T, "Expert Systems Applications Within the Nuclear Industry", American Nuclear Society, ISBN 0-89448-034-0 (1989)

[7] TAYLOR, J J , SUN, B K H , "Applications of Computers to Nuclear Power Plant Operations", *Nuclear News*, October (1990) 38-40

[8] ELECTRIC POWER RESEARCH INSTITUTE, Proceedings 1985 Seminar on Power Plant Digital Control & Fault-Tolerance Microcomputers, EPRI Report NP-4769-SR, September (1986)

[9] SUN, B H K , NASER, J A , "EPRI Development of Expert Systems Technology for Nuclear Power Plant Applications", Nuclear Plant Journal, Vol 7, No 6, November-December (1989)

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Balancing Automation and Human Action in Nuclear Power Plants, Proceedings of a Symposium, Munich, July 9-13, 1990, Jointly organized by IAEA, NEA (OECD) and IAEA, Vienna, STI/PUB/843, (1991)

[11] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Design for Control Rooms of Nuclear Power Plants, International Standards, IEC 964 (1989)

[12] FORDESTROMMEN, N T , HAUGSET, K , Integrating Surveillance and Control Without Overwhelming the Operator, *Nuclear Engineering International*, September (1991) 41

[13] SUZUKI, K et al, Coping with the Psychological Impact of Automated Systems, *Nuclear Engineering International*, September (1991) 43

[14] "Advances in Human Factors in Nuclear Power Systems", Proceedings of the International Topical Meeting, Knoxville, Tennessee, April 21-24 (1986)

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

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer-Based Aids for Operator Support in Nuclear Power Plants, IAEA-TECDOC-549, IAEA, Vienna (1990)

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Implications of Computerized Process Control in Nuclear Power Plants, IAEA-TECDOC-581, IAEA, Vienna (1991)

[18] U S NUCLEAR REGULATORY COMMISSION, A Defense-In-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System, USNRC Report NUREG-0493, March (1979)

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection System and Related Features in Nuclear Power Plants, A Safety Guide, IAEA-50-SG-D3, IAEA, Vienna (1983)

[20] ELECTRIC POWER RESEARCH INSTITUTE, Testing and Installations of a BWR Digital Feedwater Control System, EPRI Report NP-5524, December (1987)

[21] ELECTRIC POWER RESEARCH INSTITUTE, Implementation of a Digital Feedwater Control System at Dresden Nuclear Power Plant Units 2 and 3, EPRI Report NP-6143, December (1988)

[22] ELECTRIC POWER RESEARCH INSTITUTE, Design and Operation of a Digital Low-Power Feedwater Control System for PWRs, EPRI Report NP-6149, January (1989)

[23] ELECTRIC POWER RESEARCH INSTITUTE, Guidelines for Plant Process Computer Replacement, EPRI NP Report TR-101566, Vol 1,2, and 3, December (1992)

[24] DIVAKARUNI, S M , SUN, B K H , and DEUTSCH, O L , Signal Validation Techniques and Power Plant Applications, *Progress in Nuclear Energy*, Vol 22, No 3 (1989) 181-213

[25] ELECTRIC POWER RESEARCH INSTITUTE, Implementation of an Advanced Digital Feedwater Control System at the Prairie Island Nuclear Generating Station, EPRI Report NP-6758, May (1990)

[26] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Software for Computers in the Safety Systems of Nuclear Power Stations, International Standards, IEC 880 (1986)

[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety-Related Instrumentation and Control Systems for Nuclear Power Plants, A Safety Guide, IAEA-50-SG-D8, IAEA, Vienna (1984)

[28] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Programmed Digital Computers Important to Safety for Nuclear Power Stations, International Standards, IEC 987 (1989)

[29] RUMBLE, E , VINE, G , GHIRE, M , "Human Factors Considerations for the ALWR", Proceedings of the ANS Topical Meeting on Advances in Human Factors Research on Man/Computer Interaction Nuclear and Beyond, PP 178-181, Nashville, TN, June (1990)

[30] ELECTRIC POWER RESEARCH INSTITUTE, Advanced Light Water Reactor Requirement Document Volume II, Utility Requirements for Evolutionary Plants, Chapter 10 Man Machine Interface Systems, EPRI Report NP-6780-L, V 2, Ch 10, August (1990)

[31] LORD, M D , "Simulator Testing of Digital Control Systems", *Nuclear News*, September (1994) 35-38

CONTRIBUTORS TO DRAFTING AND REVIEW

Baldwin, J A	AEA Technology, United Kingdom	(2,3)
Bastl, W	ISTec, Germany	(2,3)
Basu, S	Ontario Hydro, Bruce A Nuclear Generating Station, Canada	(1,2,3)
Berg, O	OECD Halden Reactor Project, Institutt for energiteknikk, Norway	(1,2,3,4)
Bock, H W	Siemens/KWU, Germany	(1,2,3,4)
Jung, C H	Korea Atomic Energy Research Institute, Republic of Korea	(3)
Juslin, K	VTT Automation, Finland	(1,2,3)
Kim, B R	Korea Institute of Nuclear Safety, Republic of Korea	(1)
Kossilov, A *(Scientific Secretary)*	International Atomic Energy Agency	(1,2,3)
Leret, E	EdF/Research Division, France	(2,3,4)
Neboyan, V *(Scientific Secretary)*	International Atomic Energy Agency	(4)
Pobedonostsev, A B	OKB Mechanical Engineering, Russian Federation	(1,2,3)
Schuldt, G H	Institut fur Automation, Technische Universitat Wien, Austria	(1,2,3,4)
Sun, B K H *(Chairman)*	Sunutech Inc , United States of America	(1,2,3,4)
Wall, D N	Nuclear Installations Inspectorate, United Kingdom	(1,2,3)

Advisory Group Meetings

(1) Vienna, Austria 13-17 March 1995
(3) Garching, Germany 17-21 June 1996

Consultants Meetings

(2) Erlangen, Germany 4-8 December 1995
(4) Vienna, Austria 11-15 November 1996