Safety implications of computerized process control in nuclear power plants

Report of a Technical Committee Meeting
held in Vienna, 13–17 November 1989
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.
Modern nuclear power plants are making increasing use of computerized process control because of the number of potential benefits that accrue. This practice not only applies to new plants but also to those in operation. Here, the replacement of both conventional process control systems and outdated computerized systems is seen to be of benefit. Whilst this contribution is obviously of great importance to the viability of nuclear electricity generation, it must be recognized that there are major safety concerns in taking this route. However, there is the potential for enhancing the safety of nuclear power plants if the full power of microcomputers and the associated electronics is applied correctly through well designed, engineered, installed and maintained systems. It is essential that areas where safety can be improved be identified and that the pitfalls are clearly marked so that they can be avoided.

The deliberations of this Technical Committee Meeting are a step on the road to this goal of improved safety through computerized process control.
EDITORIAL NOTE

In preparing this material for the press, staff of the International Atomic Energy Agency have mounted and paginated the original manuscripts as submitted by the authors and given some attention to the presentation.

The views expressed in the papers, the statements made and the general style adopted are the responsibility of the named authors. The views do not necessarily reflect those of the governments of the Member States or organizations under whose auspices the manuscripts were produced.

The use in this book 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 specific companies or of their products or brand names does not imply any endorsement or recommendation on the part of the IAEA.

Authors are themselves responsible for obtaining the necessary permission to reproduce copyright material from other sources.
CONTENTS

INTRODUCTION .......................................................................................................................... 7

CHAPTER 1. COMPUTERIZATION OF PROCESS CONTROL SYSTEMS
IN NUCLEAR POWER PLANTS ......................................................................................... 11

1.1. Purpose ......................................................................................................................... 11
1.2. Applicability of philosophy/criteria ........................................................................ 11
1.3. Basic requirements for computerization .................................................................. 11
1.4. Safety implications of computerization .................................................................. 12
1.4.1. Direct or indirect improvements to safety ...................................................... 12
1.4.2. Direct or indirect reductions in safety ............................................................. 13
1.5. Nature of computerized control systems (CCS) .................................................. 14
1.6. Human factors ......................................................................................................... 14
1.6.1. Man-machine interface .................................................................................. 14
1.6.2. Extent of human intervention ......................................................................... 14

CHAPTER 2. COMPUTER SYSTEM RELIABILITY .................................................................. 16

2.1. Introduction ................................................................................................................ 16
2.2. Standards .................................................................................................................. 16
2.3. Classification ........................................................................................................... 17
2.4. Assessment ............................................................................................................... 18
2.5. Design ....................................................................................................................... 19
2.6. IAEA support .......................................................................................................... 20

CHAPTER 3. PLANT COMPUTER REPLACEMENT ................................................................ 21

3.1. Introduction ................................................................................................................ 21
3.2. Plant computer replacement management .......................................................... 22
3.2.1. Planning ............................................................................................................. 22
3.2.2. Organization ....................................................................................................... 23
3.2.3. Design phase ....................................................................................................... 23
3.2.4. Testing ................................................................................................................ 23
3.2.5. Implementation ................................................................................................... 24
3.3. Design basis for plant computer systems in NPPs ............................................. 24
3.3.1. Design basis ....................................................................................................... 24
3.3.2. Advance applications ....................................................................................... 26

ANNEX. PAPERS PRESENTED AT THE TECHNICAL COMMITTEE MEETING

Regulatory requirements for improvements in man-machine interface
using computerized display systems ........................................................................... 29
R.E. Touzet

Application of computerized process control in nuclear power plants with WWER 440
reactors in Czechoslovakia ......................................................................................... 35
P. Krs
Reliability and safety features in the distributed control system for the CANDU 3 .................. 43
W.R. Whittall

The third generation CANDU control room ............................................................................. 55
R.A. Olmstead

Ensurance of reliability of reactor operator support system as a factor
to increase nuclear power plant safety .................................................................................. 67
A.I. Gorelov, M.N. Mikhailov, N.A. Sazonov

The safety and operational benefits of the I&C computerized systems of the French
nuclear power plants and their accordance with safety criteria ........................................ 85
J.F. Aschenbrenner

Application of simulators in operating nuclear power plants .................................................. 101
R. Hampel

Application of computers for control and protection functions in research and
power reactors ......................................................................................................................... 113
G. Govindarajan

Planning, design basis and requirement specifications for the plant computer replacement
in Krško nuclear power plant .................................................................................................. 131
D. Mandić

Software quality supervision plan for plant computer replacement in Krško
nuclear power plant ................................................................................................................ 143
M. Smolej

Development of man-machine interface for the NPP process computer system ..................... 149
A. Stritar, B. Mavko

An example of plant computer replacement: the new centralized information processing
system (KIT) in the 34 PWR 900 MW French plants .............................................................. 157
M. Moulin, T. Meslin, P. Marcq

Experimental investigations of ex-core power control system parameters at
nuclear power plants with WWER-1000 type reactors .......................................................... 163
V.S. Zhernov, V.B. Zvezdochkina, A.N. Kamishan, A.R. Kostitzin, A.M. Luzhnov,
V.H. Meshkov, V.V. Morozov, Yu.B. Prohorov, S.G. Ztipin

Probabilistic techniques for software verification .................................................................... 179
W.D. Ehrenberger

List of Participants ................................................................................................................... 189
INTRODUCTION

The increasing power of computers and their associated electronics, together with the reduction in their physical size and cost means that conventional systems of control are being replaced by computerized systems. Additionally, in some utilities who have employed earlier generations of computer technology, there is a move to replace these systems with the more powerful devices.

The current generation of VLSI devices and micro electronics enable computing power to be distributed around nuclear power plant with data being transmitted on electronic highways between these centres of intelligence. Modern visual display units enable operators to be presented with information on plant status and, through appropriately designed keyboards, to enter commands and responses which control the nuclear power plant.

There are many financial advantages to be gained from the use of computerized process control which will reduce the costs of nuclear generated electricity. Conventional control systems utilize large amounts of cable linking discrete signals from transducers to indicators and controllers. This represents a significant fraction of the civil engineering, equipment and installation costs of any plant due to the need for cable corridors of sufficient capacity, cable tray and ladder support, the cable itself and the effort needed for installation. When these signals are multiplexed, there is a substantial saving in all of these areas. Savings can also be made in the presentation of information to the operator if long conventional control panels designed to accommodate discrete indicators, controls, lamps etc are replaced by a suitably engineered VDU system of reduced size. This, however, does not represent the only advantage of computerisation, in that larger amounts of data can be collected by the distributed intelligence, transmitted to the control room and displayed in a flexible manner on multiplexed V.D.U.s & keyboards.

Further benefits that accrue from the use of computerized systems are improved efficiency through the ability to employ more sophisticated control algorithms, derive previously hidden state variables and improve the accuracy of instrument readings through local intelligence applied to such tasks as online calibration and
linearization: maintenance effort is also reduced because of self-diagnosis in the system itself and the ability to detect plant failures through on-line monitoring. The fact that the system is programmable is often of great advantage in that late design changes can be accommodated or plant modifications can be undertaken in a shorter time period.

However, in the drive for fiscal goals, the impact of such systems on safety must not be forgotten. The features that produce the financial benefits may act either to improve safety, if correctly implemented or reduce safety, if they are poorly conceived and executed. With this in mind the IAEA convened a Technical Committee Meeting to consider the safety implications of computerized process control in nuclear power plants with the task of producing a TECDOC giving some views on the problem and some direction on how to avoid potential problems.

It should, perhaps, be pointed out at this stage that the safety implications of computerized trip systems were not in the intended scope of the meeting. Nevertheless, it was recognised that many, if not all, of the problems associated with software and micro electronics were present in trip systems as well as process control systems. In addition, computerized process control systems can reduce plant excursions thus lowering trip demands. Also the potential for initiating unspecified events due to software errors or micro computer failures needs to be considered.

Many of the reasons for the financial benefits of computerisation can sometimes contribute to the reduction in safety. The very power of a computer can lead to systems becoming overly complex and prone to the introduction of errors of both omission and commission. The multiplexing and time-sharing features make the system vulnerable to common mode and common cause failures. Their flexibility and ease of programming mean that late design changes may not be given sufficient safety consideration. The large amount of information can swamp the operator and reduce his ability to take correct actions in the event of an incident. Finally, because of the very nature of software it is extremely difficult to establish that it does not contain unsafe errors.
Fortunately, many of the features of computerized process control systems can, if properly designed and engineered, have a positive impact on safety. Calculations can be performed in real time which enable safety margins to be determined more precisely. Plant health monitoring can be integrated into the control structures. Unsolicited changes in plant status can be detected. Many of these safety improvements flow from the increase in information gathering and manipulation. With regard to the human operator, it is possible to automate more of his tedious routine tasks or those tasks that require a rapid response under difficult circumstances. A well structured operator console with properly organised data presentation will have a significant positive effect on safety.

The detrimental safety effects of all of the problem areas discussed earlier can be reduced to tolerable levels provided good practices are followed. The problem of common mode failure is still amenable to the standard redundancy/diversity solution. Ill considered or unauthorised modifications can be guarded against by the use of standard security practices, entry of passwords and the use of the various types of read only memory (ROM) now available.

In developing the views expressed in this document, papers were presented by delegates from ten Member states spread throughout the world. A total of seventeen papers were received in all on topics ranging from general software reliability, computerised protection and process control, intelligent instrumentation and human factors. Also, included in the seventeen papers were four specifically addressing the issue of replacing either an existing conventional control system or a computerised system of an earlier outdated design.

These national presentations provided much food for thought. Alarm hierarchies were mentioned plus the need to keep the operator permanently informed at all times. The utilization of "blackboard" or overall plant status mimics was seen as an important operator aid. The segregation of control/data trains into channels was regarded as important since this reduces the risk of common cause failure. We were also able to hear the Regulators' point of view on software reliability particularly in the context of reactor protection. This was supplemented by an utility presentation on a computer based protection system developed in France.
Intelligent instruments were seen as significant in the drive to improve safety. Software reliability received much attention together with views on software testing, quantification of reliability, fault avoidance, and fault tolerance. The need to separate the two testing functions of fault detection and reliability quantification was highlighted. As mentioned earlier a number of papers dealt with the issue of backfitting computer based systems. Here problems of foreshortened project time scales were raised plus the difficulties of ensuring that an accurate specification of the old system had been defined. Finally the field of human factors was represented where the subject of cognitive engineering was raised plus the need to employ task analysis to properly define the operators role. Expert systems as operator aids with VDU presentation of instructions were seen as contributing to improved safety.

Following the national presentations, working groups were set up to produce views on the issues of computer system reliability, backfitting computer based process control systems and the safety implication of this computerisation. This document represents their collected views.
1.1 Purpose

The purpose of this chapter is to identify the general principles/criteria governing the computerization of Nuclear Power Plant Process Control Systems and to examine the associated advantages and disadvantages of computerization with respect to safety. General guidance on the use of computers in safety systems is to be found in IAEA Safety Guides.

1.2 Applicability of Philosophy/Criteria

The advisability of using computer control in a given system is largely dependent on

a) The nature/structure of the existing system and the degree of automation of the system.

b) The degree of automation that is envisaged

On this basis it is clear that every proposal for computerization must be carefully examined on a case-by-case basis. Such a detailed approach is clearly impossible within the framework of this document, and we have therefore attempted to identify those principles or criteria which are applicable to all computerized systems and which are, as far as possible, independent of specific forms of computer architecture or the degree of computerization.

1.3 Basic Requirements for Computerization

It is considered that any process control functions may be computerized. However, in arriving at the initial decision on whether or not to proceed with computerization, the following basic requirements should be considered:

a) the computerized system must be at least as reliable as the equivalent conventional system,
b) the computerized system, when used for a safety-related function, must comply with all the basic nuclear safety criteria (e.g. Segregation, Redundancy etc.)

c) the sampling rate of the computer should take account of the smallest time constant of the controlled process.

1.4 Safety Implications of Computerization

A computerization of a Process Control System will introduce certain features, some of which will improve system safety, and others which might result in a reduction in safety.

1.4.1 Direct or Indirect Improvements to Safety

A computer system will:

a) process a large volume of complex information.
b) process the data and display information rapidly to the operator in a form which is easily interpretable.
c) allow automatic validation of process information.
d) allow means for the operator to check that the system is complying with Technical Specification requirements.
e) result in a general reduction in the volume of hardware (cables, cabinets etc).
f) provide a convenient method for the transmission of plant status information outside the Control Room for use in emergency situations.
g) provide a convenient means for storing data from previous events, which will form a useful data base for analysis.
h) remove tedious and distracting activities away from the operator.
i) assist the operator during an emergency situation in fulfilling the requirements of the Emergency Operating Procedures.
j) enable easy "upgrading" of the system, and can automatically provide documentation of all changes that have been introduced
k) be provided with a built-in diagnosis unit which will detect failure of the system itself.
l) allow improved verification of functional parameters.
NOTE:
Many of the above safety attributes are intrinsic in the design of any computer (e.g. the ability to process a large volume of complex information). Certain other safety advantages (e.g. diagnostic facility) must be built-in to the design. It is recommended that these additional design features should be included.

1.4.2 Direct or Indirect Reductions in Safety

a) the introduction of extensive computerization will reduce the "on-job" involvement of the operator and will therefore require more intensive and specific retraining. (Note: this item also has a positive aspect as listed under h above)

b) introduction of computerization tends to introduce new problems of "common mode failure".
   In order to reduce the impact of such problems the computer system structure must be made more complex.

c) programmable devices are themselves very complex and subject to modification, and hidden failure paths are possible. It is impractical to fully verify system performance under all possible situations.

d) state of the art techniques for highly reliable software are immature and expensive. Specialized knowledge and considerable resources must be used to ensure that the best professional practices are used, where system criticality demands them.

e) Computers cannot react intelligently to unexpected situations, so greater reliance on the computer, especially in emergency situations, could be dangerous.

f) ease of "upgrading" may lead to inadequately verified changes.
1.5 **Nature of Computerized Control Systems (CCS)**

Provided that nuclear safety criteria are met, the computer system configuration may be adjusted to meet the requirements of the individual user.

However, given the current "state of the art" it is considered that a de-centralised system will more readily meet the safety requirements.

As a further consideration of "state of the art" we also consider that only certain control sub-systems of the plant should be equipped with a closed-loop CCS. However, the overall control of the NPP should remain as an open loop with the operator as the most important link.

1.6 **Human Factors**

To fully assess the safety implications of computerized process control we must take human behaviour into consideration.

Under this heading must be considered:

a) The man-machine interface
b) The extent of human intervention in the automatic process
c) Human reliability

1.6.1 **Man-Machine Interface**

This must be made as "user-friendly" as possible. By this we mean that the operator should have easy and fast access to plant data and that this data is presented in such a form as to permit the operator to take the correct action. In order to achieve this goal there should be an easily understandable and unambiguous form of communication between the operator and the C.C.S.

1.6.2 **Extent of Human Intervention**

It is generally agreed that certain "creative" actions (i.e. those intelligent actions that require a thorough understanding of the physical process and which are beyond the scope of standard procedures), should be left to the operator. Such actions will generally occur during abnormal or accident situations.
In general we consider that the computer can be of great assistance to the operator under stress situations in terms of the presentation of information. However under any situation requiring human intervention the computer may complicate the manual operation. In some cases it would be simpler and faster to act via conventional control devices in the control room.
Chapter 2
COMPUTER SYSTEM RELIABILITY

Programmable electronic systems whether they be general purpose computers, microprocessors, or programmable controllers are playing an increasing role in Nuclear Power Plants. Computers have been and continue to be installed to supplement information systems, provide process control and to control protective systems. While it is the software that causes the greatest uncertainty in reliability predictions it is the reliability at the total system that is of concern. Carefully thought out designs considering the interaction of software and hardware can lead to increased reliability. This chapter provides recommendations on a) reliability assessment of existing systems and b) design approaches for systems to improve reliability.

2.1 Introduction

a) Objective
Objective of this chapter is to provide recommendations on:
a) techniques by which the reliability assessment of existing systems can be carried out
b) design approaches to improve the reliability of future systems.

b) Scope
Recommendations of this report are general enough to be aimed at all computer based systems within a Nuclear Power Plant including information systems, programmable instruments, microprocessors and process computers. The recommendations are primarily in the area of software reliability, but the importance of hardware design on software reliability is stressed.

2.2 Standards

Many standards exist on software quality. Some provide general guidance on overall quality assurance applicable to any engineering endeavour, others provide specific guidance to design and configuration control practices. Nevertheless the majority of these standards lack substance - i.e. the specific guidance normally provided within the standards of other engineering disciplines is not provided.
There is a need to review these standards, consolidate and interpret the advice contained within these standards, and expand the technical content. In general the standard IEC 880 is perceived to be the most applicable to safety related systems. It is suggested that this document be the basic building block for engineering standards in software. As a first step a detailed commentary providing the basis for the rules given in this standard should be written. Further there is a need to provide guidance on the interpretation of these standards.

2.3 Classification

Different levels of reliability requirements should be used for different categories of systems and types of software. It is not necessary that all software be designed or maintained to the same level of rigour.

A classification system should recognize

a) application specific software
That is software designed for a unique application within a Nuclear Power Plant. This category can be sub-divided further into programs that are rarely called upon to fulfill a safety function, such as protective shutdown systems, and process systems that are continuously on-line. Even within process systems, however, there may be sections, such as step-back control, that are also rarely used. Application specific software is characterized by the fact that it will take time, under diverse operating conditions, until the actual in-service reliability of the product is known.

b) mature, on-line software - this is software such as operating systems that have a known history of operation. This software has been in operation under a past operating environment that can be reasonably expected to occur in the future. Included in this category are complex operating systems for station process control as well as smaller operating systems such as proprietary stand-alone products (e.g. process and programmable controllers, and instruments operated by firmware).
Great care must be taken in accepting reliability of complex operating systems in safety related software as obscure errors can exist for many years, and frequent revisions may introduce new errors. Complex operating systems would normally be unacceptable in a protection system.

c) mature, off-line - this category would include such software support tools as assemblers, compilers, loaders, linkers. These tools are usually supplied and maintained by the vendor. In general, these products are characterized by extensive use in a variety of applications. However, care must be taken as these tools are periodically revised and such revision may invalidate the usage history.

2.4 Assessment

The reality of the present situation is that confidence in a computer product by the operator of a Nuclear Power Plant has to be obtained by assessment of the finished product. Quite often fundamental design decisions were made years in advance. The assessment can take the form of analysis of the source code, testing, and analysis of the quality of the design and manufacturing process. Hardware assessment can draw upon well established engineering procedures involving both component analysis and testing.

Software assessment is a new field of endeavor. In general some or all of the following 4 approaches are used:

a) Quality Arguments - The design and review documents are scrutinized and a qualitative judgement based on various indices of engineering excellence is made.

b) Precedent - The operating experience of equipment or a software product is monitored. If the system has stabilized and has been subjected to an environment similar to the one intended, without undue problems, then certain confidence for future use is warranted.

c) Mathematical Analysis - software is amenable to mathematical analysis. "Static Analysis" techniques, which are related to "Formal Methods" for design, are available to provide a rigorous
analysis of source code. Application of these techniques require a difficult transformation from natural language specifications into mathematical based format which can then be compared with the formal code analysis. Techniques also are being proposed to verify the compiled binary object code against the source code and thus check the correctness of the compiler. Further, mathematical analysis has also been used to verify the correctness of microprocessor hardware designs. These techniques are most effective and economic when Formal Methods are applied from the start of specification and design.

d) Testing - In addition to the usual systematic testing programme statistical usage testing can be carried out. Statistical testing based on expected time history behaviour of inputs has the potential of providing objective support for a quantitative reliability estimate for "first-use" systems such as reactor shutdown systems, where no statistical basis of performance under accident conditions is available.

2.5 Design

The design of hardware and software should be approached as an inter-linked activity. The system architecture and type of hardware can affect the complexity of the software. For example, a distributed microprocessor system architecture may use reasonably simple and well separated software modules. Yet too many hardware components may result in complicated communications software and perhaps lower system reliability.

Competing architectures should be investigated at the conceptual engineering phase. Complex algorithms can be moved into separate processors and thus facilitate testing, especially on-site testing after a software modification. As well the use of ROM for programme instructions and secure memories for important variables should be considered.

Most software products include self-checks to monitor the hardware for failure. It was felt by the committee that these software checks should be deliberately engineered to detect those failures which have a significant effect upon reliability. It is not considered good
practice, in fact it may be counter productive in terms of increased
code complexity, to check for every conceivable hardware failure. A
study of hardware failures is needed, and only those that are deemed
important need to be checked. In this way specifying reliable hardware
will have the added benefit of simpler software.

Incorrect and ambiguous requirements, and incorrect translation
into software or hardware, are major sources of design faults in
complex systems. Mathematically based "Formal Methods" are available
to combat these problems. However they can be very expensive if not
introduced at the earliest possible stage.

2.6 IAEA Support

There is a general concern that a set of comprehensive,
understandable tools to evaluate the reliability of computer systems be
made available. This concern ranges from specifying the purchase of
new or replacement computer systems, writing data bases, using software
packages for calculating plant parameters, as well as operating and
maintaining process and protective systems.

The IAEA should take a position of leadership in the transfer of
computer related knowledge to the plant designer and operator in the
following areas:

a) quality assurance manual for hardware to complement
   TRS # 282 for software
b) tools for hardware & software testing and the analysis of
   this testing
c) analysis of vendor proposals perhaps by providing
   consultants to assist the evaluation process.
d) make available a data base of failures or malfunctions of
   computer systems.
e) provide guidelines on the maintenance of computer systems to
   ensure continued reliability.
f) advise on security procedures.
3.1 Introduction

The experience in operating plants has shown that plant computers have to be changed or replaced every 10 - 13 years. That means that during the Nuclear Power Plant (NPP) life cycle 3 - 4 generations of different plant computer systems dedicated to plant supervision and operator's aids are used in a NPP. Each new generation of plant computers brings its own new benefits and improved functions or new functions. With the increased complexity of the systems some new problems can arise that are connected to the system reliability, availability, design, testing, management and planning of the replacement activities in the running NPP. To avoid such problems, before the decision for the plant computer replacement is passed, a plant has to carefully check if serious reasons for the plant computer replacement exist. Two groups of reasons are recognized that can lead the plant management to pass the decision about plant computer replacement.

- New functional needs:
  - System expansion needs that have reached the existing plant computer limits
  - New application development, that can not be done on the existing system
  - Improvement of Man-Machine Interface (MMI)

- Obsolescence of the existing system:
  - Loss of the capability to maintain hardware and software
  - Spare parts not available or too expensive
  - Hardware and software can not be updated to the present state of the art of process computers technology.

The goal of the Plant Computer Replacement is to eliminate reasons that forced us to replace plant computer. The latest experience shows that the Plant Computer has to be considered as a system of much wider
and complex functions. The term Process Information System (PIS) can cover much wider area of plant process data acquisition, computing, data storage and retrieval, and Man-Machine Interface (MMI) than Plant Computer. In the following material both terms can be seen (Plant Computer and PIS) depending on the scope of the functions that we speak about. A new PIS has to provide means of expandability (modular design) and upgradability with the new releases of system software and hardware without significant system architecture changes. The system must allow the user to develop new applications. The MMI may need to be improved to take advantage of advances in MMI technology, maintenance has to be simple and not expensive.

3.2 Plant Computer Replacement Management

3.2.1 Planning

The following activities should be recognized during the planning of plant computer replacement:
- preparation phase
- design phase
- validation and verification phase
- implementation

Detailed planning scheme should be applied to each module of the plant computer replacement process. Preparation phase is very important and even if it is sometimes too long, efforts that are done during that phase will be paid back by smaller number of problems in later phases.

During the preparation phase special attention should be taken to:
- Specify own functional needs
- Discuss functional needs inside a plant
- Review guidelines, recommendations, QA requirements, definition of the interface to the existing plant
- Take existing operator's and operating experience into account; follow good practice from the old system
- Think about the possibility of the usage of the same system in simulator configuration
- Discuss possible licensing problems that can appear
- Think about the response time of the Real Time (RT) system, do not overload that system with so many functions that make response too slow
- Think about the applicability of the step by step replacement (if possible) rather than whole replacement in one step.
- Investigate the possibility of parallel operation of the old and new system during the testing period.

3.2.2 Organization

The plant computer replacement project should be supported inside the plant with the strong interdisciplinary group of experts from QA/QC; I & C, computer specialists, Main Control Room (MCR) operators and specialists for equipment maintenance and surveillance. Tight communication and cooperation between manufacturer/vendor of the plant computer software/hardware and plant project team should be established from the very beginning of the project.

3.2.3 Design Phase

Prerequisite for the successful design is the accurate and complete plant data collection and precisely defined technical and functional system requirements.

Modular design approach should be followed in all cases where possible. Validation and verification should be applied to each design module and repeated during different steps of module integration.

3.2.4 Testing

Testing can be accomplished through three phases:
- Testing at vendor's plant
- Dynamic testing by simulator
- On site testing after the installation

The dynamic testing in configuration with simulator can give the best results, but such approach will not be available for all plant computer replacements because of its cost and complexity.
3.2.5 **Implementation**

Implementation is performed through preparation, generation of documentation needed for installation, training of operators, installation of hardware and software and integrated testing, start up and operation.

During the implementation phase care has to be taken not to disturb MCR operations.

3.3 **Design Basis for Plant Computer Systems in NPPs**

3.3.1 **Design Basis**

a) System architecture has to be based on professional and reliable unique data acquisition system, advanced MMI, capable computer power for real time support to operators in MCR and powerful computer for sophisticated extended real time processing, for process data history files management and for the network support to the "OUT MCR" users of process data history files. The hierarchical architecture where three levels can be recognized is recommended as a good practice:

- **Level 1:** Real Time Data Acquisition Level for data acquisition and simple, repetitive RT calculations on the process data
- **Level 2:** Real Time Computer Level for extensive RT computing, limited process data history files and MMI support
- **Level 3:** Extended Real Time Computer Level for extended real time computing and time consuming computing, process history data base management and storage, LAN support for the OUT MCR users of the process data.

b) Special functions requested by nuclear regulations (Safety Parameter Display System (SPDS), Emergency Response Facilities (ERF), Technical Support Center (TSC)) should be incorporated in the new process computer system concept as special functions on the same hardware architecture, rather than on the isolated, dedicated hardware. For some special functions data acquisition hardware redundancy can be increased, additional computing power can be installed, but basically that has to be done in the same system architecture.
c) The integrated process data base that includes RT data base and process history data base should be established.

d) Reliability and availability study applied to the system architecture has to show what are the weak points and adequate redundancy should be applied.

e) System should be designed in the way not to lose any of its functions or capabilities in the case of appearance of any single hardware failure.

f) Expandible and Modular Design

Plant information system should be designed in such way to enable modular system to expand in hardware and software structure on all system architecture levels.

g) Process Information System should have capabilities to collect and integrate process data or equipment monitoring data that come out of the dedicated computerized measuring systems or from some of the process computers that are left in the plant as a residue of an older plant process computer system after the plant computer replacement.

h) Maintenance should be performed with own trained personnel. Hardware troubleshooting has to be simple, mostly automatic, and repairs based on the modules replacement.

i) Special care should be taken to prevent common mode failures in hardware and software. For most critical functions of PIS diversity and redundancy have to be applied to reduce probability of common mode failures.

j) The vendor's hardware and system software product line should ensure that future upgrades of the hardware and system software will be possible with no significant system architecture changes.

k) The system architecture with distributed functions should contribute to the fact that even in the case of a fatal system failure, or more than one failure at the same time, system capabilities are being gradually decreased. Most critical functions should have the highest reliability and availability.
3.3.2 **Advance Applications**

Recent plant computer replacements and the new plant computer installations have shown needs for the following advanced applications.

a) **Plant operation management**
   - new intelligent measuring systems
   - validation of measurements
   - computerized guidelines for operators
   - experts systems and artificial intelligence

b) **Plant diagnosis management**
   - diagnostic applications (vibration monitoring, loose-parts monitoring, leaks monitoring etc.)
   - special input signals
   - guidelines for operator's actions
   - integration into operational management
   - collection of PSA data
   - regulatory requirement implications
Annex

PAPERS PRESENTED AT THE
TECHNICAL COMMITTEE MEETING
REGULATORY REQUIREMENTS FOR IMPROVEMENTS IN MAN-MACHINE INTERFACE USING COMPUTERIZED DISPLAY SYSTEMS

R.E. TOUZET
Comisión Nacional de Energía Atómica,
Buenos Aires, Argentina

Abstract

An analysis is made of accidents originated or worsened by the action of man, in order to determine their generic causes and to provide an adequate orientation of preventive methods and corrective actions.

Two groups of human failure are considered separately: those made by the operator in the control room and those made by the field operator during components testing.

As a result from the analysis it is strongly recommended that IAEA proceeds to review the 50-SG-D1 design safety guide, in order to introduce a safety requirement related with the information that should be available to the operator in the control room.

The Argentine national authority's requirement of installing an Integrated Information Display System in the control room is described.

Finally, the use of probabilistic safety analysis as a suitable tool to detect operator's action requiring computerized support is discussed.

I
INTRODUCTION

The safety implication of using versus non-using different computerized support tools in the control room must be evaluated with an equivalent level of knowledge for both situations.

The use of computerized control systems require previously a clear definition of:

- Parameters to be measured.
- Diagnosis methodology.
- Corrective action procedures.

A lack of this knowledge is many times the root cause of some human errors.

Safety improvements, when replace manual action by automatic action, are reached in general because the knowledge improvements needed during this process of computerization.
II
CAUSES OF ACCIDENTS

Two elements are sometimes present in nuclear accidents that were neither supposed nor taken into account by the analysts, and they are:

a) The installation present an unexpected configuration not foreseen in the working hypothesis and not due to the failure in a component, but due to the fact that the protection systems are put out of service. This situation is not foreseen by neither the analyst nor the designer.

b) The operation personnel voluntarily and deliberately -not by mistake- decides actions against safety that worsen the seriousness of the situation.

These two elements, which have been decisive in the generation of accidents, must be considered in the regulatory activity through two actions:

- The improvement of the information presentation, and
- The establishment of a safety culture.

III
THE NEED FOR AN ADDITIONAL BASIC SAFETY REQUIREMENT IN DESIGN

When the operator makes voluntarily actions against safety, this is obviously not because his intention is to cause an accident in which he will be involved, but because he is basically wrongly informed about the existing situation.

Design guides, particularly IAEA's 50-SG-D1, derived from the Code of Practice 50-C-D, state that in order to warrant safety, three general safety requirements must be satisfied:

(1) "Means shall be provided to safely shut down..."
(2) "Means shall be provided to remove residual heat..."
(3) "Means shall be provided to reduce the release..."

Are the three conditions sufficient to say that an NPP is safe? Perhaps this may be correct only in the case of wholly automatic plants in which the operator on no occasion has the possibility to block, either directly or indirectly, a protection system.

The fourth basic requirement ought to be:

(4) Means shall be provided to keep the operator permanently informed on existing situation

On the basis of this requirement, new safety functions related to the man-machine interface should be developed.
IV
THE INFORMATION DISPLAY SYSTEM

Since the TMS-2 occurrence in 1979, it became evident that during complex transients the operator is confronted with an avalanche of simultaneous information in the control room that he cannot read and still less analyse, so that, based on his own experience, he only observes the indications having the greatest importance for safety.

Since the US NRC established in 1981 the first criteria for parameters monitoring during emergencies (SPDS), the progress in informatics and computers led most of the countries to set requirements to avoid overburdening the operator and to assist him in the diagnosis of the situation.

At the present time the following basic functions are considered indispensable to avoid the problem of the lack of adequate information for operators:

- State of safety functions
- Hierarchy of alarms
- Verification of compliance of automatic actions
- Diagnosis and choice of procedures
- List of available safety systems
- Core cooling assistance
- Future state prognosis based on trends
- Advanced estimate of dose to the public

This information must be permanently and simultaneously located in some places and centres away from the NPP so as to permit the performance of the support actions during an emergency without the need for the active participation of the operation personnel in the communications.

The established requirements for the heavy water plants in Argentina intend to cover this need.

V
REGULATORY REQUIREMENT

1. Every nuclear power plant must have an integrated information display system (I.I.D.S.) permitting to know at all times the state of the plant from the safety point of view.

2. The system should be able to display the information simultaneously in the main control room as well as in the following additional places:
   - secondary control room
   - personnel withdrawal room for emergencies
   - main center for technical support to the installation
   - emergency control center.

3. The system must be independent from the installation's normal instrumentation and control systems and should have an adequate galvanic insulation from them to prevent that a failure may cause disturbances or interferences in the reactor's control and protection systems.
4. The system's main objective is to display all basic safety information in a clear and concise manner, avoiding overloading the operator with an excess of irrelevant information - as it frequently occurs during emergencies.

5. The system shall neither be able to start any action by itself nor replace any of the functions of the installation's hard logic. Its functions will be informative only with the purpose to shorten the time necessary for diagnosis during complex situations and to avoid knowledge mistakes from the operator.

6. The "integrated information display system" shall be at least fulfil the following basic functions:

6.1. **State of the plant**, consisting in the display of the state of the main safety functions:
   - reactor reactivity and power level
   - core heat extractions
   - integrity of the primary system
   - availability of the containment system
   - main radiological parameters inside and outside the containment.

6.2. **Ranking of alarms**, consisting in the abridged display of the alarms in the order of their relative importance for safety and in chronological order according to their occurrence.

6.3. **Verification of automatism**, consisting in the sequential display of the automatic actions that occur after triggering of a reactor protection system. The display should clearly show the components that failed to act automatically and thus require manual corrective actions.

6.4. **Diagnosis and choice of procedures**, consisting in a display that can assist the operator in making a diagnosis of the causes of an accident and the required actions (this can be accomplished by a screen displaying the decision logic tree for cases of break or failure of the primary or the secondary cooling systems, emphasizing the branch of the decision tree that is coherent with the information coming from the plant).

6.5. **Available safety systems**, consisting in the display of the operating condition and availability of those safety systems that can mitigate the existing situation.

6.6. **Core-cooling assistance**, consisting in a graphic display to assist the operator during the reactor cooling stage in order to keep at all time the primary circuit's pressure and temperature within adequate values to avoid boiling.

6.7. **Forecast of future state**, consisting in a display based on the trend of the relevant safety parameters and permitting to know in advance the time available to avoid or mitigate a dangerous situation. The system should permit to anticipate events such as the exposure of the core or the loss of a cool source.

In this particular case or a plant provided with a real time simulator to carrying out a follow-up of the plant's processes, their basic function will be fulfilled by the simulator and continuously transmitted to the I.I.D.S.

6.8. **Estimation of dose to the public**, consisting in the display on the screen of the plant's geographic area of influence with indication of the expected dose to the public according to the discharge through the stack and the meteorological conditions.
7. The integrated information display shall have an adequate informatic architecture based-as far as possible-on standard components to facilitate the interconnection between the nuclear power plants of Embalse, Atucha I and Atucha II with the Atomic Center of Constituyentes and CNEAS’s Headquarters where the Emergency Control Center will be located. Furthermore, the software used to fulfill the basic functions described in point 6 above, must be possible to use in personal computers compatible with those in use at the above mentioned centers from both the utility and the Licensing Authority.

8. The system shall have a flexible informatic architecture permitting to extend its capacity and its functions to meet future requirements as may be established by the Licensing Authority.

9. The group responsible for the Nuclear Power Plants shall develop a program for validation of the system and its software prior to its commissioning in the control room. The latter will be authorized by the Licensing Authority upon approval of that program. During such testing stage, simulations of various transients and possible accident scenarios will be performed.

10. During the system’s validation stage, the operations personnel shall be trained in its use, and practical evaluations similar to those required for obtaining a specific authorization will be carried out.
APPLICATION OF COMPUTERIZED PROCESS CONTROL IN NUCLEAR POWER PLANTS WITH WWER 440 REACTORS IN CZECHOSLOVAKIA

P. KRS
Nuclear Safety Inspectorate,
Czechoslovak Atomic Energy Commission,
Prague, Czechoslovakia

Abstract

Significant improvements in the last czechoslovak WWER 440 nuclear power plant design in the area of process control are realized. Continuing technological developments in computers and electronics, coupled with an effort to increase safety and reliability resulted in the application of a new computerized technological process control system. Development of this new system is also performed with perspective to replace older plants systems.

This paper draws up requirements on this system used for the first time with the WWER 440 reactors in Czechoslovakia and describes basic technical solutions used when realizing these requirements. Simultaneously outlines measures accepted to assure all of the nuclear safety requirements, especially of hardware and software reliability.

1. Introduction

Operational results are indicating that czechoslovak WWER 440 nuclear power plants are highly reliable and safe. Nevertheless, when a following nuclear power plant design with this unit was assessed in early eighties, it was decided to replace the analogue systems until that time used in the technological process control with computerized systems. This step was made with endeavour to achieve higher availability and reliability of those systems and NPP at all.

It is important change in standartized design, but without big differences in the primary or secondary technology. In addition, there are no changes in building layout - a partial analogy with replacement of originally installed system in older plants is evident.
It is important to carry out this improvement in such a way, that pre-existing functions are accomplished with an equivalent or greater level of reliability and safety. This resulting reliability and safety depends on determination of the single-valued requirements. It means requirements to:

- the scope of system functions
- the system reliability parameters, service life, availability, checking possibility and resistance against outside influences

Fulfilment of these requirements starts in design process and continues with design verification in laboratories or polygon tests, verification in operational conditions and fulfilment of the quality assurance programmes.

Successful fulfilling of given requirements depends on many aspects, in particular on the following:

- an optimum degree of computerization must be determined to get design with requested safety and reliability together with the maximum system structure simplicity
- system design must eliminate in maximum opportunities in man/machine interface to avoid operator/maintenance human errors
- the use of computers must free the operator from tedious, distracting, stressfull tasks to allow him to concentrate on more strategic tasks
- used hardware and software must allow maximum degree of diagnostic, so the operational staff have all necessary information about system
- application of computers in control system must lead to cost reduce and plant capacity increase

There will be significant improvements in using computerized technologic process control and information system in the last czechoslovak WWER 440 units. These improvements are realized in tight cooperation with the Soviet Union. The result of this cooperation will be a hierarchic, three level, fully computerized, decentralized, process control and information system with bus architecture, that exploits improvements in computers, electronic display and communication technologies of the 1980s.
2. New system conception

New Automated Technologic Process Control System has a classic, current, hierarchic, three level conception in accordance with the plant technological structure:
- the **basic (first) level** with interface to technology on one side and to
- the **block (second) level** with the computer information and control system on the other side
- both are connected with the **plant (third) level** information system.

There are two areas of progress in comparison with older systems - the high degree of computer application in the basic level and considerable improvement in man/machine interface design in the block level of this process control.

3. Basic level HW and SW

The resulting safe and reliable design ensures a choice of used basic level hardware and software at the begining.

**HW and SW complex DERIS 900** with **unified, modular and unit-construction conception** was used in our case. The DERIS 900 system can be divided in a number of parts: logical subsystem, analogue regulation subsystem, subsystem of remote control and monitoring, subsystem of two levels of bus-cores. Designer can compose typified units when combining these subsystems and that leads to **unified designing** of measuring, regulating, informing and operating circuits.

The same way of connection between input-output modules and between input-output modules and computer modules is used. It is performed by lower level bus controled by own trafic director. The bus is an integral part of each module and box. This unit-construction conception allows assembly of a functional units in compliance with system design and following **hardware debugging and software compilation separately from technology** in specially equiped laboratories. These function units can be connected with a higher level bus composed by a multicore cable. A number of independed circuits can be interconnected with this type of bus. Naturally, an interconnection between these
independent circuits is possible when computer module includes a multiply interface to higher type of bus. This possibility, maximum length of higher level bus /3000 meters/, climatic resistance of boxes and unit-construction conception enables to design a fully decentralized system. This kind of conception saves a considerable part of cables and together with special construction of boxes represents major contribution to fire resistance and safety at all.

Power supply of such systems has an essential influence on reliability. Therefore unified power supply with 24-volts direct-current voltage was used at DERIS system. This enables, among others, simple power supply redundancy with batteries in case of main power supply failure.

System is working on numeric principle and all functions are programmable. An integral part of user's tools is software which enables to work up all functions to all designers and technologists without a special training.

4. Design and reliability

Technologic unit automatically gives basis for designing of such systems. Under normal conditions customer decides system extensiveness and a degree of automation in dependence on price. But the most important requirements in nuclear engineering is system reliability and availability. When we take the hardware and software reliability as a final, increase of system reliability /in such systems as DERIS/ is possible only with redundancy. However, resulting reliability at the end depends on simplicity of system and redundancy is in contradiction with it.

If we want to get design with required simplicity, attention should be given to reliability calculations. Required reliability level must be strictly observed. Safety reserve in most of the cases complicates system structure and in fact reduces resulting reliability.

The degree of automation should be investigated very carefully. Full automation should be used especially in those circuits, where danger, that operator is not able to perform correct action in some accident cases, exists. These are especially circuits with relatively high speed, very complicated
dynamic behaviour and complicated control algorithms. Automation also should transfer the low level, distracting and stressful procedural tasks from the man to the machine. On the other hand, low speed circuits, not important for safety, with trivial dynamic behaviour is possible to provide with simple control system or without automation. Designer must select an optimum solution.

One of the first activities in design process should be choice of system's space layout. Satellite parts of the system can be placed in nearness of technology or, at least, in nearness of power supply part of design. System decentralization enables very simple separation of main and redundant buses and power supply cables, so that in case of fire or other accident they are not hit at the same time.

The algorithm work up should be next activity in the process control system designing. Its influence on resulting safety and reliability is clear, and it is in relation with requested level of automation.

After all, the reliability analysis should be made. Usual serial models for unreserved circuits and parallel models for redundant circuits can be used in the reliability calculations with good recommendation.

A starting value of module reliability parameters is predicted. The data have a statistical character and can be calculated according to US MIL-HDBK-217 E for example. But when HW manufacture starts, these predicted data must be verified in terms of a special methodology. If reliability parameters will not be in agreement with required, design must be corrected or changes in HW construction must be made.

Another important reliability value must be investigated at the same time - a medium time of repair. It depends on parameters, on which designer has considerable influence, mainly on utilization of diagnostic. The distribution of system disturbances to failures, that could be detected by automatic diagnostic or only by repairs and prophylactics, depends on applied degree of diagnostic. According to our experience, this distribution determination is very complicated, but have a considerable influence on final results of reliability analysis. Diagnostics to module level should be utilized in these complicated control systems. On the other side, applied
A few ways of diagnostic can be realized at computer systems with bus architecture. There is good experience with "Watch Dog" method, when computer modules generate dynamic signals, which can be sent to special "diagnostic" computer. When missing, visual and acoustic alarm can announce indication of defective module. Unit-constuction enables relatively high speed of exchange of this unit. This kind of diagnostic was utilized in DERIS system with good results in tests under operational conditions. The diagnostic of I/O modules is more difficult than diagnostic of computer modules. In redundant systems we can make diagnostic with comparing channels connected to one signal source. This way we can identify with high probability defective plate in principle of two-of-three. In principle of one-of-two selection we are able to identify only defective channel, but this information can also lead to relatively high speed of repairs. The degree of diagnostic is bound to another system structure complication. So the utilized degree of diagnostic depends on required reliability parameters of each measuring, remote, regulating or other circuits.

On base of successfully performed reliability analysis it is possible to set up definitive configuration of the whole basic level system according to functional and reliability requirements.

Ensuring of resulting control system safety and reliability is not ending with the end of designing, but continues with quality assurance, development HW and SW for installation and operational testing, documentation of all above mentioned activities in manuals, handbooks and operational procedures, etc.

5 Block level - requirements to man/machine interface

The Information and Control System— the block level— of the last Czechoslovak NPPs with WWER 440 unit is realized with multicomputer hierarchic system. Reliability of this system is ensured with processor reduplication together with the whole computer system redundancy.
Design of this block level is the result of cooperation with the Soviet Union. **Requirements** to this information and control system were single-valued: there must be a new quality in man/machine interface design together with keeping up current control room planning and the number of operational staff. This includes the following:

- the operational staff must get enough information to evaluate, that process corresponds with defined unit work conditions and to form a judgement of actual state of plant and control system
- on base of this system must give to operator a chance to make appropriate intervention to process and to check over the response of these interventions
- usage of high level, easy to use, programming language must enable the staff to system reconfiguration and parameter correction.
- control room must utilize standard keyboard/CRT based operating consoles for interaction and banks of CRTs for information displays, the utility must have more capability to influence operational procedures and make changes over the life time
- the traditional large area of panels containing complex configurations of handswitches, instruments and indicator lights must be eliminated; a sit-down computer consoles that will provide information to the operator and enables him to control the process should be utilized

One entirely new improvement will be in last czechoslovak NPP with WWER 440 unit control room design. The control room environment will be dominated by two large "blackboards", one for the primary and one for the secondary circuit. One "blackboard" will display all relevant events in both circuits, in fact they will depict the major equipment and system status of entire plant. In addition, "blackboards" present information to everyone in the control centre without censoring because of limitations in the size of regular displays. Current plant status will be available on console CRTs.
6. Conclusion

Application of automation to the Technologic Process Control System is carried out in order to remove tedious, distracting activities and provide the operator with tools that frees him to concentrate on more strategic matters and enables him to work on the level of a situation manager, who organizes activities and solves problems. But these improvements that flow up from computerization of process control are connected with new problems, like investigation of reliability of such systems and working up safety-related designs. In new control room the operator will work with some additional tools, that was created to work on his tasks and result should be in increase of operator reliability.

References

1. HAJIČ, J., "Utilization of DERIS system in NPPs", 1989
Computers have been used for reactor regulation and other major process control functions in CANDU nuclear power plants since 1971. There are now 21 computer controlled CANDU units in service and 9 under construction. Dual computers, with self checking, automatic switchover, and fail-safe outputs, provide high reliability and safety. The computer process control functions provide a high level of automation. In most units, the Digital Computer Controller (DDC) system includes a CRT graphic operator interface system, with a number of CRT display stations integrated into the main control panels.

Separate independent safety systems are provided for reactor shutdown, fuel cooling and containment. Minimum reliability and safety requirements for the reactor regulating system are defined in a Canadian standard issued in 1982 (CAN3-N290.4-M82). This standard defines some special features that are considered part of acceptable design practice when computers are used for the control logic associated with the reactor regulating system.

Experience with these dual redundant DDC systems has been very good and has contributed to the excellent performance record of CANDU units. Based on this experience, an advanced Distribution Control System (DCS) is being designed for the new CANDU3 nuclear plant design.

The DCS is not seismically qualified. Separate independent seismically qualified safety systems are provided.
Introduction

There are currently 21 computer controlled CANDU units in service and nine under construction [1] [2] [3]. Four of these units have been in service for more than 15 years. Operating statistics have demonstrated high reliability and safety, contributing to the excellent performance record of CANDU units. Dual-redundant digital computer controllers (DCCs) are used for reactor regulation, boiler level control and other major process control functions, providing a high level of automation. Completely separate special safety systems are provided for reactor shutdown, emergency core cooling, and containment. The basic reliability and safety features incorporated in the design of the DCCs include self-checking, automatic switchover, and fail safe action. These design features are documented in the Canadian Standard CAN-N290.4-M82, "Requirements for Reactor Regulating Systems of CANDU Nuclear Power Plants".

Based on this experience, an advanced digital control system is being designed for the new CANDU 3 plants [4]. The CANDU 3 (450 MW(e) net) is the latest version of the very successful CANDU line of nuclear power plants. The design requirements for the CANDU 3 include low capital cost, short construction schedule, use of proven components and concepts, and incorporation of the latest safety requirements and improvements.

The distributed control system (DCS) for the CANDU 3 combines modern proven programmable controller and data-highway technology [5] [6] with proven CANDU dual-redundant DCC design principles. The system makes a significant contribution to cost and schedule reduction, by reducing equipment and engineering costs, and by reducing the time required for the installation, checkout, and commissioning, of plant wiring.

CANDU 3 Safety Principles

Safety related systems are defined as those systems which perform or support the following safety functions:

a. shut down the reactor
b. cool the fuel
c. limit the release of radioactive material
d. monitor and control the plant to maintain the above functions.

All plant systems in the CANDU 3 are assigned to one of two "groups", each of which is capable of performing the above safety functions. The Group 1 systems are the systems used for normal plant operation. The Group 2 systems are the backup safety systems which are provided to mitigate the effects of failures of the Group 1 systems, including failures which may be caused by postulated events such as earthquake, flood, fire and tornado. The Group 2 systems include the four "special safety systems" (shutdown system number 1, shutdown system number 2, emergency core cooling system, and containment system), a backup feedwater system, Group 2 support services (service water and electrical power), plus monitoring and control facilities, including post accident monitoring and a secondary control room.

The Group 2 systems are seismically, environmentally and tornado qualified, and physically and functionally separate from the Group 1 systems, in compliance with Canadian regulatory requirements and the Standard Plant Licensing Basis for CANDU 3 plants. The two groups use diverse means of performing the safety functions. The diversity and separation of the two groups provides protection against common-cause failures due to events such as fire, missile, design error or maintenance error.

Adequate reliability of the safety related systems is confirmed by probabilistic safety analysis for a set of postulated initiating events.

44
**System Scope**

The DCS is an integrated plant-wide system which performs signal scanning and processing functions for monitoring and controlling most of the Group 1 systems. This includes functions previously performed by relay logic and analog control devices. A separate computer-based "plant display system" (PDS) is linked to the DCS to provide plant monitoring, operator interfacing, and data storage functions. Separate control systems are provided for a few Group 1 systems with special requirements, e.g. the shutdown cooling system, the fuel handling systems, the turbine governor system, etc. Separate seismically qualified monitoring and control systems are provided for the Group 2 systems.

The scope of the DCS includes all signal scanning and processing functions for the following systems:

- reactor regulation
- moderator and auxiliaries
- heat transport and auxiliaries (including pressure control and pressurizer level control)
- shield cooling
- boiler level (feedwater) control
- boiler pressure control
- unit power regulation
- conventional plant process systems
- service water systems (RSW and RCW)
- heavy water management
- irradiated fuel bay cooling.

The signal scanning function includes all Group 1 alarm scanning and data acquisition for PDS. The signal processing function includes interlocking, sequential control and feedback control of valves, pumps, heaters, reactivity mechanisms, etc., as well as higher level group control and system automation.

**System Architecture**

The DCS is a geographically distributed digital system consisting of a number of stations linked by data-highways. It is based on the PROCONTROL P (P13/42) product line manufactured by ASEA BROWN BOVERI [5]. Figure 1 illustrates the geographical distribution of the DCS stations around the plant.

The DCS uses programmable control processors, distributed among the stations, to perform logical (binary) and numerical (analog) signal processing functions. The data-highways use a proprietary digital data transmission system (local area network), on standard 50-ohm coaxial cable in a bus configuration.

The DCS is divided into three separate control channels (A, B, C), each of which consists of a number of stations (10, 5, 10) linked by two separate highways (A1/A2, B1/B2, C1/C2). The three pairs of highways are linked by two transfer stations, TS1 for A1, B1 and C1, and TS2 for A2, B2 and C2 (see Figure 2). This configuration provides two separate communication networks linking all the stations. The same data is transmitted independently over both networks. Each highway is controlled by a separate pair of redundant address transmitters, and is linked to the plant display system via a separate interface module.
FIGURE 1  DCS GEOGRAPHIC DISTRIBUTION

FIGURE 2  DCS ARCHITECTURE
An additional highway is used to link some stations to a special PDS interface, to provide a high resolution contact scanning function for event sequence recording.

Group 1 instrumentation and control devices (signal sources and sinks) are assigned to channels A, B or C, and connected to input modules and output modules in DCS stations in the corresponding channel.

Electrical power for most source and sink devices is provided via the DCS input modules and output modules. However, interposing relays are used for most binary output signals, in order to provide sufficient voltage and/or current for the load.

In general, each DCS station is used by all signals assigned to the corresponding channel in a particular area of the plant, irrespective of process system or function. However, some functional partitioning is being considered, in order to simplify the probabilistic safety analysis.

The data-highways operate in a deterministic manner. Signals are broadcast using fixed length “telegrams”, each of which contains a source address and a 16 bit data-word. Signals are updated cyclically, with cycle times ranging from about ten milliseconds to about 1.3 seconds, depending on the signal category.

Signal transmission between modules in a DCS station is via a passive local bus which also operates on a cyclic broadcast principle. The local bus cycle is 5, 10 or 20 milliseconds. Control processors operate on a fixed cycle of 20 milliseconds.

The use of a deterministic cyclic broadcast principle for signal transmission avoids timing problems and provides constant active signal checking. Transient errors have no significant effect on plant control. Message acknowledgement and retransmission procedures are not required, and there is no possibility of data overload.

Two diagnostic stations are linked to the highways, DS1 for A1, B1 and C1, and DS2 for A2, B2 and C2. The diagnostic stations provide on-line facilities for fault annunciation and identification to the module level, for displaying signal values from any station, for inputting test data, for displaying and adjusting control system tuning parameters, and for reading the contents of any application program memory (EPROM) in any control processor, bus coupler or highway address transmitter.

Safety Reliability Requirements

Any failure that requires activation of a safety system to prevent unacceptable release of radioactive material is defined as a “serious process failure”. One of the basic CANDU safety design requirements is that the combined frequency of all serious process failures does not exceed one in three years. The reactor regulating system in the CANDU 3 is required to be consistent with Canadian Standard CAN3-N290.4-M82. This standard sets a design target of one in 100 years for “loss of regulation”, i.e., a serious process failure caused by a failure in the reactor regulating system. Since the control logic for the reactor regulating system is performed by the DCS, this target must be considered in the design of the DCS. However, the impact of DCS reliability on the probabilistic safety analysis of fuel cooling functions is expected to be more significant than the impact on loss of regulation frequency. This is partly because the provision of independent reactor stepback logic in the DCS provides a very good defense against potential loss of regulation failures. A safety reliability target of one in 100 years for potentially serious failures of a single DCS control channel, due to independent random component failures, has been set.
The main requirements in Canadian Standard CAN3-N290.4-M82 which relate to DCS safety reliability address the following topics:

a. reliability targets  
b. redundancy  
c. fail-safe design  
d. use of general purpose control computers  
e. testing  
f. maintainability  
g. power supplies  
h. environmental conditions  
i. equipment quality and qualification  
j. equipment and software identification  
k. quality assurance  
l. documentation

The standard contains a number of general design principles and specific requirements which are applicable to the DCS. It also contains some specific design features to be included when signal processing and logic associated with the reactor regulating system is performed by general purpose control computers. Most of these design features are directly applicable to the DCS, but in some cases the underlying objectives are met in a different way. The features are as follows:

a. Self-checking routines to check system and reasonableness of inputs and outputs. Detected errors shall result in appropriate action. (The DCS does not check outputs.)  
b. Use of watchdog monitor to provide fail-safe action. (The DCS complies.)  
c. Watchdog monitor to use redundant components and should be testable. (The DCS uses distributed watchdogs and self-checks, with off-line testing.)  
d. Adequate redundancy in switchover equipment between redundant computers. (Redundancy in switchover equipment is not necessary in the DCS to meet safety reliability targets.)  
e. Use of good design practices such as modularity in hardware and software design. (The DCS complies.)  
f. Indication in the control room of which computer is in control (DCS status information is available in the control room.)  
g. Quality assurance and documentation requirements are generally applicable to both hardware and software. (The DCS complies.)

The DCS complies with all other applicable requirements of CAN3-N290.4-M82.

**Equipment Reliability**

The DCS uses electronic modules that were specifically designed for distributed control applications in power plants. The modules have been proven in a number of power plant applications for several years, and low failure rates are well established. Typical module failure rates are in the range 0.1 to 0.01 per year.

The environmental design limits for the modules are 0 to 70 degrees C (component temperature), 0 to 95% relative humidity, and 1 g vibration, 4 to 40 Hz. Power dissipation in the modules is fairly low, so forced air cooling is not required in ambient temperatures up to 40°C. However, consideration is being given to the provision of special ventilation ducting to reduce module failure values and avoid failures due to local steam leaks or fires.
No DCS equipment is located inside the reactor building, except for two stations which are not connected to the highways. These stations are used for scanning some input signals for the Plant Display System which are not required after a reactor shutdown. Outside the reactor building, protection against environmental hazards is provided for all abnormal events with a frequency of more than 0.001 per year, by avoiding hazardous locations or by the use of suitable barriers.

The DCS modules are unaffected by electromagnetic interference up to 10 V/m over the frequency band from 27 MHz to 500 MHz. The data-highway signal transmission technique provides very high immunity to electromagnetic interference and incorporates very effective error detection. Invalid address or data words are not used. Signals are updated at frequent cyclic intervals, so transient errors have no significant effect on the process systems.

Input modules and output modules are not damaged by overvoltage transients up to 1000 volts, and each station is isolated from the highway cables by an isolation transformer rated at 2000 volts.

**Firmware Reliability**

The programmable DCS modules include permanent fixed firmware which is not application specific. This firmware is mature and has been well tested in many applications for a number of years. Program interrupts and multi-tasking operating system software are not used.

**Application Software**

The application software consists of address lists in the highway address transmitters and bus couplers, and signal processing programs in the control processors. The signal processing programs are designed and documented by means of function diagrams, using a functional language (P10) designed by ABB. This language is specifically designed to implement signal processing functions for control systems. It uses standard function blocks based on IEC standard 117-15. Signal transfer between blocks is defined graphically by connections between function blocks. An example of a P10 function diagram is given in Figure 4. The diagrams are designed, documented and translated into processor code using computer aided design tools. Signal processing for each function block is executed directly by fixed firmware in the control processors.

No programming is required for memory allocation, memory initialization, input-output, or program flow control. All function blocks are executed every 20 milliseconds. The programs are designed by control engineers rather than software engineers. The program documentation is in the form of function diagrams which are relatively easy to understand. The programs are checked and tested in accordance with project procedures, which also include procedures for change control and configuration control. The programs are installed in non-volatile read-only memories (EPROMs) which are installed in the modules. The contents of any installed application EPROM can be read back at any time for comparison with an approved master copy. Special maintenance procedures are required to ensure that the correct EPROMs are installed in each module.

**Redundancy**

Within each DCS control channel dual-redundant fault tolerant design concepts are used to provide high reliability. Two independent highways and associated communication modules and inter-channel transfer stations provide two fully redundant communication networks. The two networks are linked to the PDS via separate interface systems. Control processors, highway address transmitters, and local bus controllers are also used in
FIGURE 3  TYPICAL P10 FUNCTION DIAGRAM
dual-redundant pairs. Power supplies are also redundant. Figure 3 illustrates a typical DCS station.

Built-in hardware and software self-checking provides automatic transparent switchover to the standby network or module when a fault occurs in the active network or module. Switchover between redundant components can be tested on-line. Built-in fault diagnosis features are provided for fast identification of a faulty module or highway cable. The faulty module or cable can be replaced on-line. Special procedures will be required to ensure a low frequency of maintenance error when replacing a faulty module or highway cable.

The only modules that are not dual-redundant are input modules, output modules, and local bus termination modules. Important sensors are triplicated and connected to separate input modules in three DCS control channels, so additional redundancy is not necessary. All other input modules and output modules are dedicated to single devices or process systems, to allow replacement of the module without affecting more than one device or system. Redundant binary output modules are being considered for a few special applications. The local bus end-module and the passive local bus itself are not redundant, because they have very low failure rates.

Fail-Safe Design

Hardware and software self-checking features are distributed throughout the system. When faults or data errors are detected the data is flagged as invalid. Distributed watchdog timers in the bus couplers and output modules check for failure to receive valid addresses and data for each data word. The control processors are programmed to take appropriate action if input data is invalid. Output signals automatically reset to "zero" if they are not updated with valid data for about 3.3 seconds (binary) or 10 seconds (analog). Process system actuators are designed to "fail safe" when the control signal is "zero". (For binary control signals the "zero" state is zero volts. Magnetic latching interposing relays may be used in a few special cases. For analog control signals the "zero" state is four milliamps, unless there is a power supply or output circuit failure.)
The following signal checks are included.

a. Data words on the local bus are transmitted on two separate lines, in normal and inverted form. Data "validity" is checked by each receiving module by comparing the two signals, and invalid data is rejected. This check detects failures of signal sources, or transmission errors due to faults, electrical noise, or simultaneous transmission by two modules.

b. Address words on the local bus include a parity check bit. An address word with a parity error is ignored. All local bus modules check for cyclic receipt of valid addresses.

c. Highway signals are subject to very stringent checks, including timing and parity checks on address and data words. These checks detect failures of signal sources, or transmission errors due to faults, electrical noise, or simultaneous transmission by two stations. Each bus coupler has separate watchdog timers for each address. These timers check that each required valid address and data words are received every four seconds to update each required signal. Invalid or stale data is not transmitted by the bus coupler.

Each control processor has a watchdog monitor which checks the processor power supply voltages, the sequential operation of the firmware, and the periodic execution of a special function block at the end of the application program. When a fault is detected, transmission of output signals to the local bus is blocked. External devices are used for watchdog status indication and manual operation of the blocking logic.

Channelization

The comprehensive use of self-checking and redundancy provides high immunity to independent random component or connection faults. The use of three separate channels provides an additional dimension of redundancy, and also provides high immunity to dependent common-cause failures, e.g. failures caused by fires, steam leaks or maintenance errors.

As in previous CANDU plants, triplicated instrumentation and redundant process devices are used selectively in the process systems, to provide high reliability. Three separate power distribution systems, A, B and C are provided for instrumentation and control devices. Redundant process devices are assigned to channels A and C to maximise reliability. Almost all of the non-redundant process devices are distributed between channels A and C, to distribute the load on the two main electrical power systems, and to reduce the effect of failure of either of these power systems.

Instrumentation and control devices assigned to a particular channel are connected to the corresponding DCS control channel. The basic control logic for each individual device or loop is implemented in the DCS station connected to the control device. This includes logic for safety related functions, e.g. reactor stepback. Higher level control logic for group control or system control, e.g. reactor regulation, is implemented in separate DCS stations in control channel B.

The appropriate use of the channelization concept in the design and application of the DCS ensures that failure of one DCS control channel will have a limited effect on important process control functions. The frequency of independent coincident failures of more than one DCS control channel is predicted to be very low, less than $10^{-4}$ per year. The frequency of dependent coincident failures of more than one channel is minimised by functional independence, physical separation, electrical isolation, and signal decoupling in the equipment which links the channels. Coupling modules connected to the highways include 2000 volt isolation transformers and data buffer memories.

Where necessary, separate rooms are used for each of the DCS control channels to reduce the frequency of environmental common-cause failures.
Conclusion

The DCS for the CANDU 3 incorporates many features which enhance reliability and safety, including the use of proven equipment and firmware, totally distributed self-checking and fail-safe features, redundancy, and channelization. We are confident that a very high level of reliability and safety will be achieved. This will be confirmed by appropriate probabilistic safety analysis, by experience with a prototype system, and by operating experience.

References


THE THIRD GENERATION CANDU CONTROL ROOM

R.A. OLMSTEAD
CANDU Operations,
Atomic Energy of Canada Limited,
Mississauga, Ontario,
Canada

Presented by W.R. Whittal

Abstract

In CANDU stations, as in most complex industrial plants, the man/machine interface design has progressed through three generations.

- **First Generation** control rooms consisted entirely on fixed, discrete components (handswitches, indicator lights, strip chart, recorder, annunciator windows, etc.) Human factors input was based on intuitive common sense factors which varied considerably from one designer to another.

- **Second Generation** control rooms incorporated video display units and keyboards in the control panels. Computer information processing and display are utilized. There is systematic application of human factors through ergonomic and anthropometric standards and cookbooks. The human factors are applied mainly to the physical layout of the control panels and the physical manipulation performed by the operators.

- **Third Generation** control rooms exploit the dramatic performance/cost improvements in computer, electronic display and communication technologies of the 1980's. Further applications of human factors address the cognitive aspects of operator performance.

At AECL, second generation control rooms were installed on CANDU stations designed in the mid 70s and early 80s. Third generation features will be incorporated in the CANDU 3 station design and future CANDU stations.

There have been significant improvements in the man/machine interface in CANDU stations over the past three decades. The continuing rapid technological developments in computers and electronics coupled with an increasing understanding and application of human factors principles is
leading to further enhancements. This paper outlines progress achieved in earlier stations and highlights the features of the CANDU 3rd generation control room.

INTRODUCTION

The man/machine interface represents an exceptional opportunity for industrial plant designers to realize significant gains through cost avoidance, operational reliability and safety. This opportunity exists because of rapid technological development in computers and electronics, coupled with significant progress in the behavioural sciences that greatly increases our knowledge of the cognitive strengths and weaknesses of human beings.

Significant event data from operating nuclear plants in many countries consistently indicates that the root cause of events leading to equipment or safety barrier impairment results from operator/maintenance human error in 40-60% of the cases. The contribution of human error to the accidents at Three Mile Island and Chernobyl further underscores the need for design features that accommodate human cognitive strengths and weaknesses. Equally important, the significant events attributed to human errors represent a large cost iceberg in operating power stations.

In CANDU stations, as in most complex industrial plants, the man/machine interface design has progressed through three generations.

- **First Generation** control rooms consisted entirely of fixed, discrete components (handswitches, indicator lights, strip chart, recorder, annunciator windows, etc.). Human factors input was based on intuitive common sense factors which varied considerably from one designer to another.

- **Second Generation** control rooms incorporated video display units and keyboards in the control panels. Computer information processing and display are utilized. There is systematic application of human factors through ergonomic and anthropometric standards and cookbooks. The human factors are applied mainly to the physical layout of the control panels and the physical manipulation performed by the operators.

- **Third Generation** control rooms exploit the dramatic performance/cost improvements in computer, electronic display and communication technologies of the 1980's. Further applications of human factors address the cognitive aspects of operator performance.

At AECL, second generation control rooms were installed on CANDU stations designed in the mid 70s and early 80s. Third generation features will be incorporated in the CANDU 3 station design and future CANDU stations.

There have been significant improvements in the man/machine interface in CANDU stations over the past three decades. The continuing rapid technological developments in computers and electronics, coupled with an increasing understanding and application of human factors principles is leading to further enhancements. This paper outlines progress achieved in earlier stations and highlights the features of the CANDU 3rd generation control room.

A. **SECOND GENERATION MAN/MACHINE INTERFACES**

The control centre in the four operating CANDU 6, single unit stations represent a typical second generation man/machine interface (See Figure 1). Some of the features are described below:
FIG. 1. CANDU 6 control centre.
The Dark Panel Concept

Human factors research and experience in the aircraft industry has made this concept standard practice in the cockpit. In the CANDU 6 control room, a light always signals a situation that requires operator action - an annunciator, handswitch discrepancy, a computer program that has failed, etc.

The Fifteen Minute Rule

There is sufficient automation to ensure that no operator action is required in the first fifteen minutes of the worst case dual failure event, analyzed as part of the safety analysis for the plant. Consequently, CANDU operators have, as a minimum, fifteen minutes to perform diagnostics and planning before taking direct action but for single event cases at least 10 hours is available.

Automation

The use of computers in process and safety systems has, in many cases, freed the operator from tedious, distracting, stressful tasks to allow him to concentrate on more strategic matters. For example, the boiler feedwater transient after a reactor trip requires no operator attention. Automatic warm-up and cool down of the primary and secondary process systems is another example.

Human Engineered Testing

In the later second generation units, some periodic testing has been automated to reduce human errors that are often associated with tedious, boring, repetitive tasks. When manual tests are required, the design ensures that the tests are "non-intrusive". This ensures that maintenance staff do not modify or contact the internals of the plant equipment to carry out the tests.

Reduced Panel Congestion

This was accomplished in three ways:

1. Reducing the number of annunciator windows by limiting their use to major alarms and group alarms.
2. Use of CRTs to present displays that integrate information from different systems and equipment.
3. Automation of tasks previously accomplished by operator manipulation of control panel devices.

Good Anthropometrics

Making reference to the appropriate design "cook books", the size, shape, slope, illumination level, and many other parameters of the physical interface were optimized to accommodate the physical characteristics of the operator.

Good Control Panel Layout

The design incorporates logical grouping and clear delineation of panel switches and indicators. Panel mimics are utilized with hand switches located to represent the location and status of the controlled device as it relates to the mimic. The design incorporates standard shapes, position codes, colour codes, and a systemic and consistently applied method for labelling panel components. The alarm annunciation system classifies, sorts and allows conditional suppression of unnecessary alarm messages.
B. THIRD GENERATION MAN/MACHINE INTERFACES

Future CANDU stations will include a third generation man/machine interface. The principles underlying many of the design requirements are based on theories established by the discipline of Cognitive Science that seeks to integrate engineering and psychology to describe the behaviour of humans as components in an information processing system. In particular, the work of Rasmussen(1), Weiner(2) and Woods(3) has had a significant impact.

The superordinate goals for the design of CANDU third generation controls rooms are the following:

1. **Cost Reduction**
   
   Reduce cost, avoid schedule risk and increase plant capacity factor.

2. **Operational Design Objectives**
   
   Change the design process so that high level operational objectives drive the detailed design of the cognitive and physical man/machine interface.

3. **Elevate the Role of the Operator**
   
   Apply additional automation selectively in order to remove tedious, distracting activities and provide the operator with tools to function on the level of a situation manager who plans, organizes activities and solves problems.

4. **Context Sensitive Information**
   
   Package and present information, to suit the context of a particular situation, so that the operator can quickly absorb the relevant data.

5. **Keep the Operator in Touch with the Plant**
   
   Provide information and activity that will keep the operator alert and in touch with the plant.

6. **Flexible Control Room**
   
   Provide the operating utility with a control room that uses a minimum number of standardized components in a flexible interface that can be tailored to suit a different operating philosophies and methodologies.

**The Nature of Man**

For the third generation man/machine interface, the designer must be aware of certain unique characteristics of men that set them apart from machines. Figures 2 and 3, for example, list some intuitively derived strengths and weaknesses of men and machines in performing plant control functions.

**Exploiting Human Creativity**

Some of the features of the third generation control room are designed to facilitate man's unique ability to synthesize volumes of information and make good decisions, even when the data is incomplete or inconsistent. This is the key to ensuring an adequate response to the unanticipated or obscure cause events that are a fact of life in complex industrial facilities.
MAN

+ CREATIVE
+ USE OF JUDGEMENT, EXPERIENCE, HEURISTICS
+ MAKES DECISIONS OUT OF INCOMPLETE DATA
+ CAN SYNTHESIZE SUPERORDINATE OBJECTIVES

- FORGETS
- GETS OVERLOADED
- TUNNEL VISION
- SUBJECT TO FATIGUE AND EMOTIONAL INTERFERENCE
- LOGIC AND REASONING FAULTS OCCUR

FIG. 2. Strengths and weaknesses of men in performing plant control functions.

MACHINE

+ REPEATABLE RESULTS
+ PREDICTABLE CAPACITY
+ NOT SUBJECT TO FATIGUE OR EMOTION
+ CAN SIMULATE LEARNING AND JUDGEMENT
+ CAN PERFORM COMPLEX COMPUTATION AND LOGIC

- NEEDS COMPLETE SET OF INPUTS TO FUNCTION
- LIMITED ABILITY TO LEARN
- SUBJECT TO DESIGN ERROR
- REQUIRES MAINTENANCE
- SOMETIMES FAILS CATASTROPHICALLY

FIG. 3. Strengths and weaknesses of machines in performing plant control functions.
A Fresh Perspective

Regardless of the quality of the man/machine interface design, the public perceives human variability to be such that any task given to man has a relatively high probability of being performed in error. This perception tends to suggest that there are higher probability failure modes than those identified in the random equipment failures covered in the probabilistic safety analyses.

The familiar concepts of redundancy and diversity will be applied so that a second human is available to confirm the safety critical actions of the operator. The most difficult requirement is to ensure that the redundant human is also sufficiently "diverse". This means his knowledge, training and recent activities should be sufficiently different to ensure that he does not make the same cognitive error as the first man and become part of a common mode human error. In CANDU stations, separation of perspective is achieved through the roles and activities assigned to the shift supervisor and the first operator respectively.

Rationalizing Conflicting Objectives

The Chernobyl and the Three Mile Island incidents were partly the result of conflicting operational objectives. Procedures in these plants did not adequately resolve the potential for inappropriate action. For example, at Three Mile Island, the objective to cool the fuel conflicted with the objective to maintain two phases in the pressurizer. For the third generation MMI, man/machine interface detailed procedures and the detailed interface design will be systematically derived from a complete set of high level operational objectives. If implicit objectives are present, they must be made procedurally explicit.

The Information Interface

Figure 4 illustrates the concept that the plant operator performs both procedural and strategic/judgmental functions. Note that the "human" interfaces with the plant mainly through information while the direct manipulative interface, by comparison, is trivial. The interface is not man to machine but to information about a machine. (See Reference 6)

Information will be available to the operator in the context of his specific objectives in a particular situation. This means that, instead of organizing information in association with systems, areas of the plant or equipment, the operator will have access to information and control facilities focused on functions such as maintenance of fluid or energy balance, achievement of poison override or execution of an emergency operating procedures.

Automation

For third generation control rooms, automation will seek to transfer the low level, distracting and stressful procedural tasks from the man to the machine. Both manipulative and cognitive tasks of this type will be automated. For example, the normal equipment sequencing required to valve in the shutdown cooling system will be performed by the machine. This will allow the man more freedom to perform at the level of a planner or situation manager. When complex manual sequences are automated, a few manual operations will be retained in order to keep the operator aware of and involved with the process.

Flexibility

In the past, the control room design left the operating station staff with insufficient scope to apply their experience to determine the form of information presentation or to define operating methodologies. Third generation control rooms will utilize standard keyboard/CRT based operating consoles for interaction and banks of CRTs for information displays. The utility will have more capability to influence operational procedures and make changes over the life of the plant.
Changing the Design Process

For the advanced CANDU control room, the design process is a significant departure from previous practice. The traditional approach was to break the information interface down by plant system or equipment. Each system designer then specified the alarms, displays and control interactions they believed were adequate in that narrow context. The station technical unit was then given the job of creating operating and emergency procedures based on the design as given. In the new approach, after the basic plant operational requirements are established, draft procedures will be produced. Then, a mixed team of designers and operating staff will define an information/interface system design that will be based on the real objectives, tasks and activities of the operators.

Context Sensitive Information

The traditional large area of panels containing complex configurations of handswitches, recorders, meters and indicator lights will be eliminated. The control room will be a compact module containing a few sit-down computer consoles that will provide information to the operator that has been processed to reflect the context of his specific objectives and tasks in each particular situation. Figure 5 illustrates these features. The detailed operating procedures are written at the beginning of the design and form the basis for the information system design.

"Blackboard Displays"

The control room environment will be dominated by several large dynamic colour graphic mural mimics. One will depict the major equipment and system status of the entire plant.
Another will provide an easily interpretable picture of critical plant parameters and how they are changing or interacting. These displays are the "blackboards" upon which information is presented to everyone in the control centre without censoring because of limitations in the size of regular CRTs. Current plant status at the most detailed level will be available on both the "blackboards" and console CRTs. Traditional annunciation windows will be replaced by indications on the blackboards and pattern displays on the CRTs. Figure 5 illustrates these features.

Computer Assisted Procedures

Computer assisted procedures will minimize the need for paper procedure books. The operators will use CRT screens that present integrated text, graphics and check lists, possibly supported by a computer synthesized voice. The displays will guide them in a systematic and rapid execution of the procedure. A particularly valuable aspect of the procedure presentation is an Event Confirmation Field which, at each stage of an event specific procedure, indicates to the operator if plant conditions are confirming the correct event diagnosis. Some of the procedures will be "context sensitive" in that the computer will edit and simplify them based on its knowledge of the actual state of the plant (e.g. it will not display an instruction to turn on a pump that is already on).

Decision Support Facility

In advanced, third generation control rooms a knowledge based decision support system utilizing several online expert systems will provide the operator with information and, when appropriate, a "what if" query facility to help him anticipate and plan for future action. Associated with this facility are knowledge based event diagnostics that will help locate root cause events. The output is in the form of recommendations with the rationale for each recommendation provided on request.

Already available is a system to inform the operator which channel to fuel next and another to indicate the exact channel containing a defective fuel bundle.
Pattern Recognition

Cognitive science recognized that humans are particularly effective in learning to associate significant meaning from shapes and patterns. Control room displays will seek to exploit this factor by presenting alarm configurations and plan parameter deviations in the form of interpretable patterns.

Critical Safety Parameters

Critical safety parameters, a short list of "vital signs" relating to the public safety defence barriers, will be prominently displayed in graphical pattern form permanently on a dedicated CRT screen or blackboard displays.

Voice Annunciation

Voice annunciation will be utilized in a few selected situations where redirecting the operators' attention is imperative. For example, voice will be used to announce that the entry conditions for an Emergency Operating Procedure have been realized.

Equipment Configuration and Status Display

Plant Equipment Status Schematics on the control room CRT will be operated directly from the plant Computer Aided Design and Drafting data base. The state of devices such as locally operated valves will be semi-automatically updated on the CRT displays from bar code readers connected into data highways by the plant operating personnel.

Operation Information System

The basis for an Operation Information System will be provided. This capability will electronically integrate and automate many of the tedious, labour intensive activities associated with operating a nuclear station. For example, maintenance records, work control, man-rem statistics, equipment status, event logging and reporting and work scheduling. The result will be a significant reduction in operating costs and operator stress levels and perhaps operations staff. This facility will be developed by the operating utility associated with the plant.

Computer Annunciation Alarm Overload

With approximately 6000 measured and calculated variables for a single nuclear unit, there are operational circumstances when so many alarms can arrive that an overload situation develops. Such alarm overloads can impose severe demands upon the operator and have significant implications in terms of training, the structure of procedures and safety.

To some extent, the problem is a consequence of the availability of better instruments and tools to handle direct and derived data. Computerized techniques have contributed to the problem; they will also be part of the solutions. It is easy to present a very large volume of alarm data spanning many different fault scenarios with various degrees of importance and credibility. The challenge is to package the messages that are relevant in a particular situation and time and to articulate the alarm information in such a way that it directs the operator's attention to the remedial task at hand. Notice that we are not proposing to suppress information but rather to package and prioritize it in ways that make sense in a particular situation.

Recognition of the above problems has stimulated development of solutions. These include the following:

- The use of a high level, easy to use, programming language so that the station staff will be able to introduce the results of real operating experience.
- Improved alarm **categorization** strategies, including:
  
  (a) **Plant State** (e.g. reactor shutdown or at power, heat transport system pressurized hot or pressurized cold, class IV power available or not).

  (b) **Action Time** (e.g. Operator action within one hour, maintenance action within 8 hours, longer term maintenance action).

  (c) **Response Category** (i.e. plant diagnostic message, equipment status message, maintenance message, software and hardware error messages).

- Increased use of interpretable shapes and patterns for presentation of alarms and deviation displays.

- Nuisance alarm suppression.

- Selected voice annunciation.

**Standardization**

Although there may be several design and architect engineers performing the detailed design, the layout, architecture, ergonomics and control philosophies of the entire control room will be universally consistent.

**Access to Control Room Data**

Because all plant data is available on high speed data highway, simple interfacing will provide controlled access to all control room information for use in the plant management computer system or on terminals on or off the site.

**Cost**

The elimination of fixed panels, utilization of standard operator consoles, the application of computers to operational configuration control and the reduction in trunk cabling will yield significant cost benefits.

**CONCLUSION**

Third generation CANDU control room brings together the principles of cognitive science, new technology and lessons learned by CANDU operators. In this control room, the operator will work with tools that were crafted to serve his objectives and work on his tasks. Most important, he will function on a level that exploits his unique ability to innovate and form strategies to deal with unanticipated obscure cause events.

This design approach should result in improved operator reliability while, at the same time, reducing costs.

**ACKNOWLEDGEMENT**

The author wishes to acknowledge a significant contribution to the content of this paper made by the staff at Atomic Energy of Canada Limited - CANDU Operations, particularly R.F. Moore, J.E.S. Stevens and R.E. Ashwell. An equal contribution was made by the staff at the Chalk River Nuclear Laboratory, particularly J.J. Lipsett, R.R. Shah and L. Lupton.
REFERENCES


ENSURANCE OF RELIABILITY OF REACTOR OPERATOR SUPPORT SYSTEM AS A FACTOR TO INCREASE NUCLEAR POWER PLANT SAFETY

A.I. GORELOV, M.N. MIKHAILOV, N.A. SAZONOV
Research and Development Institute of Power Engineering, Moscow, Union of Soviet Socialist Republics

Abstract

Safe maintenance of modern nuclear power plants (NPP) cannot be ensured without use of operator support systems. Their use is conditioned by the fact that in the process of NPP development there considerably increased and continues to increase the number of monitored parameters, an essential part of them being parameters important for safety estimation which can be received only by calculation.

It is evident that operator support system reliability is one of the most important factors, influencing NPP plant safety. In all the world this problem attracts large attention.

Ensurance of reliability of operator support systems may be achieved only at complex approach by:
- using high-quality components;
- system designing on the basis of corresponding principles;
- thorough debugging of the system on a special tester-equipment with the use of adequate models of object and equipment;
- organizing maintenance process.

The paper deals with all stated above aspects of reliability ensurance of reactor operator support system. It is noted that the use of expert systems allowing to improve operator working conditions and to reduce requirements to his qualification.

Most of the methods of reliability increase considered in the paper are realized in information-calculation systems of reactor RBMK-1500 at Ignalina NPP and are developing for use in perspective systems.
1. INTRODUCTION

An integral part of automatized reactor monitoring and control systems (ARMCS) of modern nuclear power plants (NPP) is reactor operator support systems. Their appearance in ARMCS composition and use are conditioned by constant increase of the number of parameters monitored by the operator, an essential part of them being parameters important for safety estimation which can be received only by calculation. Thus, for example, in the reactor operator support system at Ignalina NPP 37 parameters are calculated, including 24 which are calculated for each of 1660 reactor channels.

It is evident that reactor operator support system reliability is one of the most important factors influencing NPP safety.

Ensurance of reliability of operator support systems may be achieved only at complex approach by:

- using high-quality components;
- system designing on the basis of corresponding principles;
- thorough debugging of the system on special tester-equipment with the use of adequate models of object and equipment;
- organizing maintenance process.

Figs 1,2 show principles of ensurance of reactor operator support system reliability.
PRINCIPLES OF ENSURANCE OF REACTOR OPERATOR SUPPORT SYSTEM RELIABILITY

- Use of high-quality component
  - Use of computer means to the performance for NPP
  - Complex tests of the system at manufacturer's plant
  - Use of verified technical solutions, laid down in computer means

- System design on the basis of corresponding principles
  - Organizing principles
  - Structural-functional principles
  - Technical principles
  - Program principles

- Debugging of system on tester-equipment
  - Tester-equipment as a representative fragment of the operator support system
  - Availability of special means of debugging process automation
  - Availability of models of an object of different degree of complexity
  - Availability of elements of real apparatus in the tester-equipment composition

- Organization of operation process
  - Teaching and certification of operating staff
  - Creation of automation means for operating staff activity
  - Development of precise rules of organizing activity of the operating staff

FIG. 1. Principles of ensurance of reactor operator support system reliability.
FIG. 2. Principles of reactor operator support system design.
2. USE OF HIGH-QUALITY COMPONENTS

In the Soviet Union there are special rules of development and production of automation means delivered to NPP. The supervision over rule observance is placed on Gospromatomenergonadzor.

These means are to pass special reception for correspondence to the performance requirements for NPP which consists of several stages, including monitoring of completing items and their selection, corresponding testing of the stock-produced apparatus, furnishing the system and testing of its operation, according to tests and check tasks. The tests are carried out at the manufacturer's plant before sending to the NPP. In tests representatives of the consumer may participate.

An important condition of use in the composition of ARMCS of different computer means is of verified technical solutions laid down in them, stable indices of their quality during batch production, their application experience on objects of other industry branches.

3. MAIN PRINCIPLES OF SYSTEM DESIGN

3.1. Classification of principles

Principles of reactor operator support system design and main system-technical solutions laid down in the system bring an important contribution in the reactor operator support system reliability.

The design principles increasing the reliability of the system under design can be conditionally devided into four groups:

- organizing;
- structural-functional;
- technical;
- programme.
3.2 Organizing principles
To the organizing principles one should refer:
- competition of project of system under development;
- independent investigation of project;
- maximum possible use of design automation system on all stages of development;
- obligatory breadboarding and debugging of new solutions laid down in the system;
- coverage of all life cycle of the system (stages of development, integration, maintenance, modernization);
- carrying out all work under the leadership and personal responsibility of the design chief.

3.3. Structural-functional principles
To the structural-functional principles reflecting experience of this country and of other countries in the field of reactor operator support system development one should refer:
- distribution of the system, its decentralization according to technological, functional, technical, territorial and organizing indicators;
- hierarchy of the system according to functions of information treatment, reliability, response to the action, ensurance of internal diagnostics;
- functional reliability of the system by realization in it functions increasing directly or indirectly its reliability.

The principle of system distribution follows from particularities of organization of process control by such a complex object as a nuclear plant is. It is evident that in this case the distribution and decentralization should be combined with the possibility of centralization of information reception.
and acceptance of decisions on control on high level of hierarchy, for example, reactor as a whole.

The system distribution may be characterized by the following indicators:

- technological, when a part of the system handles an exclusive enough part of the whole control object;
- functional when a definite part of the system fulfills a completed function;
- technical determining part of the system as a set of interconnected technical means;
- territorial determining expediency of formation of local parts of integrated system depending upon their location;
- organizing taking into account, for example, development of a separate system by a definite organization, people collective as well as particularities of subsequent operation.

In accordance with the principle of hierarchy on low levels of the system one should fulfill more simple functions but with a high degree of automatization, reliability, short time of solution, etc. As the level hierarchy rises the functions usually become more complicated but in this case requirements for reliability of their fulfilment, degree of automatization, time duration of fulfilment etc. reduce.

For example, on low levels it is reasonable to realize the function of signalization, at the same time on high levels of the system complicated calculations may be made, including calculations for forming settings with their subsegment transfer to low levels. As to the volume and contents of information there should be also observed the principle of the hierarchy which may be interpreted as follows: on low levels there are information of simple type (measurement results) according to which it is difficult to take decisions on control but as the level rises on
the basis of processing of all set of information, reception of qualitatively new information including, there may be taken based solutions concerning control. It is also important to fulfil to the principle of hierarchy as to ensuring internal diagnostics of the system, namely, on low levels most simple functions of checking of operationability and selfdiagnostics are to be fulfilled, while with the help of high levels more complex algorithms of maintenance and detection of faults are fulfilled, and these algorithms may be included into operation according to results of selfcheck and to other reasons, for example, periodically or on operator request.

The principle of functional reliability ensurance supposes that it is obligatory to realize in the system the functions ensuring complete or partial operationability of the system at failure of channels of information measurement, system equipment or its software.

To these functions one may refer:
- check by different methods of truth and rejection both the measuring and calculating parameters (entering operating range, mutual check of correlating parameters etc.);
- automation of processes of load, run installation and restart of the system;
- reconfiguration of the system;
- automatic diagnostics of operationability of technical and program means of the system;
- monitoring and control of system functioning, with the use of apparatus of check points, check and recovery of operationability of communication lines, check of task run-time etc.
3.4. Technical principles

To technical principles followed from trends of computer means development one should refer:

- information input from the object, as a rule, only through one highly reliable device with information conversion to digital form and subsequent transfer to all systems-consumers preferentially through digital channels of communication;
- use of multi-channel computer means, as necessity occurs, operating under control of corresponding operating system and fulfilling mutual check of operationability of one another;
- redundancy in the system of resources for memory, productivity, channels of input and output of information for its subsequent development and modernization;
- wide use of optofiber communication lines for organization of intermachine connections due to their high error protection and good characteristics as to information transfer speed;
- use in maximum possible degree of serial computer means, including those ensuring automatic selfdiagnostics and possibility of selftesting.

3.5. Programme principles

To programme principles also reflecting experience of development of operator support system of this country and other countries one should refer:

- preferential use of programming languages of high level which, as a rule, considerably reduces the number of hidden defects of software;
- use of functionally oriented batches of program modules, installing for operation in a concrete system of software, which at system development ensures the use of solutions verified earlier, speeds up the process of development and reduces the number of hidden defects of software;
Fig. 3. Reactor operator support system of Ignalina nuclear power plant.
- functional decomposition of the program system allowing to ensure parallelism of development of not connected or weakly connected components of the developing system speeding up the process of development.

The above stated structural functional principles were used, in particular, when developing reactor operator support system at Ignalina NPP, the structure of which is shown in the fig.3. These same principles are used for newly developing problems as well.

4. DEBUGGING ON TESTER-EQUIPMENT

Debugging of reactor operator support systems is fulfilled on stands-polygons specially created for this purpose.

An ideal variant of such a tester-equipment is a full-scale system of operator support allowing debugging of any solutions laid down in this system. In real life such an approach is used rarely enough because:

- the cost of such a full-scale system as a rule is high enough;
- comparatively large expenses for maintenance of such a tester-equipment;
- it is required the creation of powerful enough (as to the number of channels) apparatus of signal imitation at inputs of this tester-equipment;
- beginning with a definite moment expenses for increase of imitation apparatus power are not compensated by real use received from the tester-equipment;
- factor of total utilization of equipment of such a tester-equipment is comparatively low.

Thus proceeding from our own experience, a larger part of time (~50%) is spent on independent debugging of system
components, 35% of time is spent on complex debugging of separate subsystems and 15% of time occupy actually complex debugging of the system as a whole.

It is more efficient and considerably cheaper, by our opinion, to use an approach at which the tester-equipment represents a representative enough fragment of operator support system. In this case several variants of its functioning are realized for making debugging of different components and the whole system but with some reasonable limitations.

One should note several main moments which should be taken into account when creating and developing such tester-equipments:

- as service life of such tester-equipments is comparatively long and they, as a rule, are created for debugging of several parallely developing systems, from the beginning there should be laid down the possibility of replacement of morally obsolete equipment by new one;

- the whole equipment of the tester-equipment should be located in neighbouring rooms which will allow to reduce the number of operating staff, to reduce the volume of additional equipment and the length of communication cables, to ensure operative preparation of the tester-equipment to solution of new problems;

- the tester-equipment should be equipped with special means of automatization of debugging process which may considerably increase its effectiveness;

- there should be ensured the correspondence between variants of tester-equipment configurations and concrete purposes of each of the stages of debugging, different factors being taken into account.
The following examples of special means debugging process automation may be given:

- generators of test data sets allowing to imitate changes of input information according to different laws;
- models of an object of different degree of complexity;
- activation means on CRT display of information, coming from the system on traditional means of information reflection (signal elements, devices, recording instruments, base mimic panels);
- means of automatization of loading installation and run of the software of the tester-equipment itself and operator support system software as well;
- means of reception of information about dynamic characteristics of the debugging system (processor loading, intensity and time of exchange with external devices, time of fulfilment of tasks etc.).

The proposed approach was realized when creating the tester-equipment for debugging reactor operator support system at Ignalina NPP and it proved to be completely correct.

The table shows volumes of equipment of the real system and that of the tester-equipment.

Table: Volumes of equipment of real system and of tester-equipment

<table>
<thead>
<tr>
<th>Type of the equipment</th>
<th>Operator support system</th>
<th>Tester-equipment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computational complex CM-2M, pieces</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Operating place of operator-industrial engineer, pieces</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Concentrators CM-1M, pieces</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>Terminals of communication with object, pieces</td>
<td>38</td>
<td>2</td>
</tr>
</tbody>
</table>
Fig. 4 shows the structure of the tester-equipment. The number of realized configurations of the tester-equipment on which the reactor operator support system debugging was carried out is equal to 3.

5. ORGANIZATION OF OPERATION PROCESS

Considerable increase of reactor operator support system reliability may be achieved by means of improving preparation of operating staff, automation of his activity and corresponding organizing measures.

The operating staff of reactor operator support systems includes:
- remedial maintenance personnel;
- operative personnel.
The remedial maintenance personnel deals with maintenance of technical means of the system. His preparation contains:

- teaching at courses of qualification improvement at the manufacturer's plant of technical means of the system;
- a monthly period of probation for debugging computer means in the shops of the manufacturer's plant.

An alternative solution may consist in centralized maintenance of separate systems by specialized organizations. But in the Soviet Union this type of maintenance is developed very weakly yet and the quality of such maintenance does not meet the requirement level, demanded by NPP.

Operating staff is also educated at courses of qualification improvement at the manufacturer's plant of computer means but on their own program. To acquire stable skill in the work with the system it is reasonable to carry out probation of operating staff on tester-equipment at the final stages of complex debugging of the system and immediately after completion of its debugging.

Besides all operating staff passes regular certification of knowledge of corresponding documentation and availability of required skill in the work.

As to automation of operating staff activity at present works for creation of the operating staff support information system are under way. They include:

- expert system of diagnostics of condition of technical means of the reactor operator support system;
- system of automatized keeping of operating journals;
- reference system giving to operating staff text materials of operating documentation, organized in the form of hypertext;
- information-reference system of monitoring the condition of measuring channels;
system of representation of current condition of technical and program means of the reactor operator support system;

- system of planning and monitoring of fulfillment of schedules of remedial maintenance and preventive maintenance.

Technical realization of the operating staff support information system is assumed in the form of the network of personal computers of the type IBM-PC/AT.

To organizing measures increasing operator support system reliability one should refer obligatory preparation of precise rules of fulfillment of such operations as:

- keeping of documentation on the system and updating documentation;

- keeping of operating archives on software and internal database of the system and updating them;

- eliminating defects detected in the system in the course of its production run;

- system advancing not depending on the reasons causing it;

- carrying out preventive and remedial maintenance on system equipment.

All these measures allow to reduce requirements to operating staff and reduce its size, shorten the period of time for search and deletion of defects, to create more comfortable conditions for operating staff work.

CONCLUSION

The paper deals with principles of reactor operator support system reliability increase, used by the authors in their practical activity.

The ensurance of required reliability of reactor operator support systems may be achieved only by complex approach to solution of this problem taking into account a complete set of
factors influencing upon system reliability at the stage of its design and during its production run and modernization.

REFERENCES

5. Lipaev V.V. Program testing, Moskow, Radio and communication, 1986.
THE SAFETY AND OPERATIONAL BENEFITS OF THE
I&C COMPUTERIZED SYSTEMS OF THE FRENCH
NUCLEAR POWER PLANTS AND THEIR ACCORDANCE
WITH SAFETY CRITERIA

J.F. ASCHENBRENNER
Electricité de France,
Villeurbanne,
France

Abstract
The use of data processing in the I&C systems of French NPP, highlights the way in which safety criteria are applied. Furthermore, safety greatly benefits from new improvements. The French nuclear program takes into account the experience feedback from the 1300 MW plants which is being applied to the N4 series. The later uses a fully computerized I&C system including a control room designed with experience gained from the S3C Project.

INTRODUCTION

This paper is a support for the IAEA Technical Committee. We would like to thank all the authors whose ideas presented in previous meetings and congresses have helped in the preparation of this paper.

Before starting the technical part, we review French PWR NPP policy. The safety approach involves two main items.

- The French NPP have been designed from an American licence with a French probabilistic study addition to the deterministic design rules in order to improve safety.

- EDF is both the Architect Engineer and the Plant Operator. So, as a basic rule, EDF’s interest is to take into account experience feedback. Feedback improves safety and plant operation. The analysis of the incidents allows corrections which are applied to all the plants.

I - THE EARLY SIXTIES

Before extending computerized process control in the 1300 MW NPP, EDF had two main experiences.

1.1 - The Gas-Graphite NPP

In the sixties, EDF experimented with data processing systems in the NPP I&C, as well as in thermal plants.
As a matter of fact, the Gas-Graphite NPP needed elaborate on-line processing functions such as the detection of fuel element burst slug. Redundant computers have been used in association with protection channels based on hard-wired technologies.

The 500 MW "Saint Laurent des Eaux" plant started in 1969 using computers ordered in 1965. The complexity of the start-up and short term control requires a computer aided automatic control system.

1.2 - The PWR series

The 900 MW PWR series, with its easy to operate process, did not need computers. EDF used a general I&C architecture organised with a conventional control room (alarm windows, pushbuttons, ...) with a main console for normal control and a rear panel. An information data processing computer provided data logging and measurement monitoring. The whole control and protection systems are made with hard-wired cabinets using relays. Careful consideration was given to the system design and operation to avoid spurious trips.

The plant computer had no safety criterion and was only a support for the operators.

The manual safety actions and alarms are directly connected to the relay cabinets.

The 900 MW series includes 34 plants distributed in three sub-series (CPO, CP1, CP2). The generalized feedback policy allows for a general implementation on all plants.

This previous control room organisation has been revised to implement a safety display panel and to upgrade the plant computer.

II - THE 1300 MW COMPUTERIZED SYSTEMS

2.1 - The 900 MW policy improvement

EDF adapted the 900 MW policy to improve the new 1300 MW plant I&C and generally to take into account the post-accident operation:

- Implementation of increased performance algorithms (DNBR)
- Development of alarm processing
- Design of new operating procedures
- Improvement of testability and reliability
All these goals were achieved because of the availability of the following new technologies and study methodologies.

- Microprocessors
- CAD tools
- Software rules

Furthermore, the implementation of modern technologies would make possible significant performance improvements and enhance operating conditions.

Microprocessors allowed all these improvements while respecting safety criteria (single failure, independence, qualification, reliability, tests ...).

The VLSI technology necessitated the design of new architectures to respect safety goals, because it does not have a fail safe system.

2.2 - Description of the main systems

The 1300 MW I&C architecture mainly includes:

- the control room and its computer
- the SPIN protection system
- the CONTROBLOC computerized control cabinet.

. CONTROL ROOM

The 1300 MW Control room looks like the 900 MW with alarm windows, pushbuttons and CRTs, but its organisation has been completely reviewed. The design is quite different from the previous one because it includes the post-accident operation directly.

In addition, the CONTROBLOC provides alarms for the operator with only the original one following an event, exclusive of those resulting from actions due to the said event.

The plant computer, not important for safety, delivers systematic views of the plant.

The Safety Panel function is included in the design, and provides centralized information for post-accident aid.

. SPIN

A new designed protection system "SPIN" has been studied since 1977. It is mainly characterized by the use of microprocessors. It was developed according to
a rigourous and systematic procedure, incorporating safety rules and qualifications. A special software development methodology was established with recommendations (IEC, EWIC), because there were no precise texts dealing with software. The main feature is the "V life cycle" based on the independence of the programming and verification teams.

The complete SPIN system was assembled at Merlin Gerin company, for an extended test program prior to site delivery.

**CONTROBLOC**

The 900 MW relay control systems, are replaced by microprocessor-based programmable control cabinets. This new microelectronic controller performs plant control and provides alarms. It has the capability of self diagnosis and is designed to survive the first failure.

Nearly 100 cabinets are used in each plant and are connected to the control room alarm windows and CRTs.

Alarm processing using powerful data processing to the CRTs is designed to reduce the number of alarm windows (1300 in the 900 MW and only 300 in the 1300 MW).

These two main systems (SPIN and CONTROBLOC), studied since 1977 with mock-up phases, were the first fully computerized systems used in NPP, achieving protection functions.

The first NPP, "PALUEL" was fuelled up in 1983.

The design of these systems gave EDF and manufacturers a priceless experience.

**III - FEEDBACK AND TMI 2 ACCIDENT CONSEQUENCES**

3.1 - Experience feedback

The main goals of the experience feedback in FRANCE are:

- to systematically collect data and transmit them to the design teams,
- to associate designers, operators and manufacturers,
- to implement modifications and take them into consideration for future plants.
The present situation, based on a series of plants, is very suitable. It is in EDF's interest to carry out detailed studies which can be applied to all its plants.

The example of the 1300 MW microprocessor based systems is interesting. In each plant, these systems represent nearly 150 electronic cabinets, so the feedback is quick and valuable.

The main features of this feedback are:

- System improvements
- Performances
- Architecture
- Technology
- CAD
- Cost

- Powerful and Accurate computation
- DNBR (Protection & Monitoring)
- DMAX (Rod Control)

- Man-Machine Interface
- Control room
- troubleshooting

- Management
- CAD
- thousands of REPROMS

- Obsolescence
- microprocessors

All these problems can be solved more easily when the policy of construction is a power-range policy enabling the same standardization development advantages to be taken for the design of several units.

3.2 - TMI 2 accident

The TMI accident, directly implicated human error in the control room, especially in:

- the operator's role
- the instrumentation
- the organisation

After the accident, EDF provided additional studies dealing with the experience gained. A working group established an action plan with items concerning:

- Improvement of man-machine interfaces (safety panel in the 900 MW plants)
- Implementation of margin to saturation and reactor vessel level
- Approach of accident based on pre-determined accident or physical state oriented approach.

This new approach is able to suppress the operator's difficulty when the unusual situation clashes with his mental model.

The first answer to the question is the improvement between 900 and 1300 NPP in the control room, but EDF's idea is to use a computerized control room.

The S3C project started in 1981, has four main goals:
- To verify that man is able to operate the plant in normal and accidental situations,
- To validate the general organisation of the control room,
- To validate the alarm processing, dialogues and displays
- To have a full scope simulator for the N4 operators.

IV - THE EXTENSION TO THE N4 I&C

4.1 - N4 Control room

The N4 control room is directly designed from the experience feedback gained with the S3C design and operation. The design teams were able to validate at full scale, the overall design and ensure that it would be adequate for controlling the plant under all circumstances.

This simulator brings to an advance stage, the man-machine interface operational specifications with the corresponding CAD facilities.

The whole N4 system operates with redundant computers and workstations. So, this new design led to the decision to review all the other I&C systems in the plant, dealing with control and protection to provide many validated information.

There are three workstations in the control room (two for operators, one for the shift supervisor and the safety engineer). A fourth one is in the technical room. But a large wall mimic gives a general view of the whole plant with information updated from the control
and protection systems. This mimic is a reference and it is used as a link between the operators.

A conventional panel is also directly connected to the CONTROBLOC system in case of a general failure of the control room computers.

In normal and accidental situations, the operators only use the workstations, that give them the same means of control and the same mental model.

4.2 - Systems and classification

All the control and protection systems have been upgraded to improve the whole data processing in accordance with the control room needs and technological capabilities.

The global N4 I&C structures include:

- the computerized control room
- a wall mimic with panel
- the CO3 system including SPIN
- the P20 programmable controllers
- the MICROREC turbine control

All these systems achieve functions in accordance with design criteria determined in the safety classes (1E, 2E, IPSNC and HS):

1E: This class concerns the systems necessary for the reactor trip and other safety functions. SPIN and CONTROBLOC are 1E. They have to respect redundancy, independence, qualification, periodic tests and other design rules (IEC 880).

2E: This class concerns the systems necessary for the post-accident monitoring. MIMIC and auxiliary panel are 2E. They have to respect qualification, tests and design rules.

IPSNC: This class concerns the system useful for post-accident operation. THE CONTROL ROOM (and its computers) is IPSNC and has to respect reliability, test facilities and design rules. The system has redundancy such that the single failure criteria is met, independence between each electric train. It has no special test, but it is used during normal operation. Software is designed with IEC 880.
4.3 - CO3

CO3 is especially designed to implement the following functions:

- Reactor protection (SPIN)
- Nuclear flux and Rod instrumentation
- Rod control systems
- Core Monitoring

The 1E class concerns SPIN and protection instrumentation whose main objectives are:

- Safety
- Availability
- Performance
- Tests
- Qualification

The SPIN architecture is 2 out of 4 redundancy, with differences from the 1300 MW, taking into account feedback and new technologies (especially Networks).
4.4 - P20

The P20 CONTROBLOC system makes general automatic control and exchanges with the control room.

Its architecture is based on a redundant network linking several blocks realizing functions according to a predetermined traffic arrangement.

This sub-system called Cluster, communicates with the control room. Nearly thirteen Clusters work together. The internal redundancy of the cluster and the blocks can be managed in relation to the requirements (safety, reliability ...). The whole system is remote loadable for a progressive commissioning.
4.5 - MICROREC Turbine control

This system is not important for safety, but its design is subjected to requirements concerning availability. So its architecture is organized at three levels:

- Actuator (position loop)
- Regulator (speed adjustment)
- Control (load variation)

Each position loop receives informations from the three redundant computerized regulators with a 2/3 vote. An important qualification program is also carried out to demonstrate the behaviour and the fault tolerance.

V - IMPROVE THE COMPUTERIZED PROTECTION SYSTEM

5.1 - SPIN functions

The reactor protection system takes priority over all others in ensuring reactor safety, by continuously monitoring plant variables. This system automatically initiates all actions necessary to restore the plant to safe conditions and to mitigate the consequences of abnormal operation.

SPIN assures the reactor protection using a 2 out of 4 redundancy with four protection channels, eight protection networks and eight voting logic units. In addition, it is designed with internal redundancies to improve safety, availability and tests.
Two external units collaborate with SPIN.
US for the core monitoring
UD for troubleshooting
They are not 1E, but have redundancy.

5.2 - SPIN improvements

The new N4 SPIN takes into account experience feedback, improvements in hardware technologies and software developments.

One of the more important is the limitation of human intervention inside the cabinets (In a NPP nearly 60% spurious trips are due to the operator). These improvements are:

- remote loading
- aid to troubleshooting
- automatic configuration after a failure.

On the other side, the weak points of SPIN reliability have been solved with a dual acquisition unit with on-line input testing. This concept enables the functional test to be carried out every 1.5 years.

The Hardware improvements include new processors with distributed units linked by a special safety network "NERVIA" designed by MERLIN GERIN to be incorporated in Safety Systems.

High level software with C language and SAGA tools are most effective.

5.3 - SPIN Description

The 1300 System, including test unit, redundancy and wiring is complex and expensive. In particular the architecture needs exchanges between the four channels to have a first level voting logic.
The N4 system has been re-designed with up-to-date technique to achieve the following objectives:

- safety
- availability
- reliability
- performance
- cost
- ease of use

The structure shows that exchanges between channels have been suppressed. This is possible by using a new structure with networks, which simplifies the cabinets and offers a better reliability.

This architecture, easier to implement retains:

4 protection channels (UATP)
8 trip breakers
2 Safety features trains (ULS)
1 functional test unit (UTC)

The main features of the NERVIA Network are:

- Token passing protocol
- 2 Mbits/s
- Redundancy
- Optical fibre or coaxial
- Distributed traffic controllers.
Inputs from the process are transmitted directly to two data acquisition units (UA1 and UA2) which are activated simultaneously and provide mutual back-up.

These signals are processed by five functional units (UF1 - UF5) in accordance with requirements.

The association of two data processing units and five functional units is called an UATP.

SPIN comprises four such units in a 2 out of 4 redundant configuration.

In each UATP, a redundant protection network links UA and UF via standard stations implemented directly on the CPU card.

This network uses a deterministic protocol. All the stations receive the message and respond in a Round Robin sequence.

Safeguard and reactor trip are initiated by two logic units (ULS A and ULS B) which receive signals from the four UATPs and develop 2/4 vote.

Each logic is connected to two independent signal transmission networks with the control room and control cabinets.

Each logic unit comprises four redundant processing units (UTP) in order to respect safety criteria (simple failure, test ...). They are further processed by 2/2 array.

The protection system has a built-in continuous self checking capability and is also periodically tested via a centralized test console.

Periodic tests are performed from the console, which controls six local test units in the four UATPs and the two ULS.

5.4 - Classification

The SPIN is 1E, so it has to respect criteria. Some of these have already be described in the previous chapters.

The 1E software, is based on a validation structure independent of the design structure. An independent team validate the results obtained by the design team, as requested in the IEC 880, in total accordance with the work done in the previous 1300 SPIN.

A safety forecast study demonstrates that the failure probability of emergency shut-down is extremely low (less than 10^-5) for this purpose, each card involved
in emergency shut-down was subjected to a particular study determining the failure probability on the basis of the failure rates of each component defined in the CNET Reliability Data Report and in MIL-HDBK 217.

Cover by self tests and periodic tests is incorporated into this analysis to estimate the non-sure failure state. Using the Markov-graphs, optimization of self-tests and periodic tests can be carried out to obtain a failure probability compatible with functional requirements, taking account of system redundancy.

5.5 - SAGA

The N4 CO3 system greatly uses a software design workshop, called SAGA, especially developed by MERLIN GERIN to realize the SPIN protection system.

SAGA is based on:

- a synchronous data flow specification language,
- a graphic man-machine interface
- a top-down design method.

SAGA has been designed to develop a very rigorous and reliable method with consistency checks at every step.

The SPIN protection system software has importance with safety constrains and is developed in accordance to the IEC 880 norm and the EWICS recommendations which lead to a software life cycle with validation procedures and independent teams.

The use of SAGA tool extends the assistance to the programmes by providing formalism and facilities.

The main advantages proved during the CO3 development are:

- SAGA brings a common language to all the teams
- SAGA facilitates the verification team work
- SAGA allows great re-use of validate components
- SAGA gives a high level documentation quality.

SAGA has been developed with a high level language in order to reduce the gap specification and implementation. SAGA verifies object coherence throughout the process. All the data and functions are typed.

The design process begins from a very high interface level, and then progressively refines functions and data.

SAGA is a new step in the design of high quality software, next steps will include new functions as complexity measures and properties proving.
VI - DRAWING AN INFERENCE

By the end of 1989, EDF greatly benefits from its situation, due to the fact of being at the same time the Architect Engineer and the Plant Operator, with a wide experience gained from previous developments in the sixties and feedback from the 1300 series with SPIN and CONTROBLOC.

There are three main points to be considered.

1/ Safety is based on a continuous and careful approach with a large quality integration. So feedback is a trump especially in the case of EDF whose program is among the few in the world not complying with the experimental law of non standardization.

The N4 series follows the 20 plant P4 series.

2/ I & C computerized systems increase safety with new possibilities resulting from technological, improvements:

- sophisticated algorithms,
- accurate digital computation,
- high level alarm processing,
- high level languages,

and resulting from organisation and management:

- software design (880),
- CAD,
- test quality,
- man-machine interface.
3/ High level computerized I & C such as N4 is not possible without respecting standards and safety criteria. In the case of EDF, the N4 general design (SPIN, P20, CONTROL ROOM) especially includes standards, such as IEC 880 that incorporates the results of the previous software design development used in the 1300 MW SPIN.

In conclusion, designing computerized systems, necessitates a mentality, which takes into consideration experience feedback.

It is also very important to consider that habits and practises have to change to meet the demands of new technologies and CAD tools.
APPLICATION OF SIMULATORS IN OPERATING NUCLEAR POWER PLANTS

R. HAMPEL
Technische Hochschule, Zittau, German Democratic Republic

Abstract

For a safe operation of NPP it is necessary to improve the reliability and availability of the instrumentation. For this end simulators for calculating parameters which are not to be measured directly as well as testing the accuracy of parameters to be measured directly will be used. Further more applications in operative management, strategic management and in research will be described briefly.

In this connection the paper presents some problems regarding the improvement of instrumentation e.g. for level measurement in steam generators. For experimentally checking and verifying the methods for measuring value correction and measuring system diagnosis a pilot plant was installed (pressure 4 MPa). The scheme of the experimental arrangement and some results are presented. A new measuring method for determining the steam content distribution and steam bubble velocity will be demonstrated, too. It is based on the electrical conductivity measurement.

1. Introduction

In consequence of high requirements for nuclear safety and availability the number of parameters to be monitored and the number of measurement points in nuclear power plants have been increasing continuously. By introducing systems for supervising the function in automatic control systems and the use of support systems as well as expert systems this trend has been continued. It is a technical necessity to limit this trend. That will be possible, if information of measurement points, which are available, is used in a better way. In this way some fundamentals of the development of automated process control will be shifted to the field of software development. In this connection the real
time simulation gained more and more importance. The paper presents some problems regarding the further improvement of the instrumentation quality e. g. for the level measurement in steam generators.

2. Application fields and tasks of simulators in Nuclear Power Plants

Diverse types of simulators have been defined in the last time related to the development of trainers for educating service personal. It is possible to distinguish between:

Single principle simulators
- Simulating special physical effects or technological equipments

Basic principle simulators
- Simulating physical and technological processes without reference to a concrete technical equipment

Complex-Simulators
- Simulating physical and technological processes with a concrete technical equipment including all the elements of man-machine-communication.

Requirements concerning simulation accuracy are dependent on the application field. In many cases it will be sufficient to relate the accuracy to the user perceptibility or the precision of measuring and recording devices. This applies to static as well as dynamic processes.

On applying simulators in NPP process control for supporting operative management the following tasks can be formulated.

Application in operative management (short-term-problems)
- Computing parameter transients for planned operating regime changes (for example support)
- Monitoring operating regime at planned and unplanned operating regime changes (for example disturbances, redundancy changes)
- Monitoring the function of technological equipment and control equipment
- Perception disturbance
- Monitoring safety-related parameters, i. e. defence in depth.
Application in the strategic management (long-term problems)

- optimal start and shut-down process control
- optimal power alteration control (periodical and non-periodical)
- long-term trend analysis of safety-related and availability-related parameters (especially for indirectly measurable parameters)

Respective optimization parameters are for example:
- fuel costs, efficiency, thermal and mechanical strain, material and energy consumption.

Application in research and development

- optimal operation regime development
- analysis of the effects of technological and safety-technical reconstructions
- soft- and hard-ware tests for automated control systems
- Testing methods for man-machine-communication

For accuracy and reliability improvements model-based measuring methods will be used in powerful automatic control system.
This is especially effective, when disturbance parameters or process parameters are not measurable directly.

The use of these methods for static and dynamic corrections and function diagnosis in automated control systems with hierarchic structure is presented in Figure 1. It is possible to distinguish between three layers /2/.

In the first layer there exist generally small requirements concerning the accuracy but high requirements with respect to the reliability and availability. Monitoring the measuring parameters and the measurement device therefore will be concentrated to the normal device function, for example through monitoring the power supply.

In the second layer there exist higher requirements regarding accuracy in connection with permissible tolerances for automatic control. It is necessary for example for the level measurement at pressure vessels based on the hydrostatic principle to consider the steam content in the vessel and the divergence from the
standard conditions concerning density and pressure parameters. The software for this problem is in general very simple.

In the third layer the validity of the measured parameters will be find out by comparison with diverse measurement quantities as well as comparison with results of simulator calculations. In contrast to accident analysis relatively simple dynamic models will be used. The calculations must be implemented in real time. This third layer is the most important field of simulators for model-based measuring methods.

3. Application of model-based measuring methods for steam generator level measurement

In NPP with PWR (WATER type) horizontal steam generators will be used. This results in special peculiarities for level measurement. In order to avoid steam generator and turbine damages the water steam mixture level ($h_g$) in the steam generator must be observed.
very exactly. This is also necessary regarding pressure transients and power transients.

If the mixture level is higher than permissible, the water separators and the turbine will be damaged, if the mixture level is lower than permissible the heating tubes will be damaged.

As you can see in Figure 2 the permissible limiting quantities can be exceeded at some points after pressure transients. By monitoring the real level of the water steam mixture model calculations are urgently necessary. This will be realized by two simulation modules

- steam generator module
- measuring system module

FIG. 2. Representation of level limits for steam generators and transients of the measured level after pressure drop.
The functional principle of these modules is shown in Figure 3.

The hydrostatic pressure-difference measurement will be applied as a measuring method at the horizontal steam generators. For the simulation of both modules the same conditions can be applied /2/.

**mass balance**  
\[
\frac{dm}{dt} = \pm \dot{m} = \pm \frac{d(s_i, v_i)}{dt}
\]

**energy balance**  
\[
\frac{dE}{dt} = \pm \dot{Q} + \pm \dot{m} h = \pm \frac{d(s_i, v_i, h_i)}{dt}
\]

\(m\) - mass  
\(E\) - energy  
\(\dot{m}\) - mass flow rate

with defining the steam content \(\varphi\)

\[
\varphi = \frac{v'}{v' + v''}
\]

\(v'\) - water volume in vessel  
\(v''\) - steam volume in vessel
and simplifying through the acceptance of the thermodynamical balance

\[
\frac{d\varepsilon_i}{dt} = \left( \frac{\partial \varepsilon_i}{\partial \rho} \right)_p \cdot \frac{d\rho}{dt}
\]

and

\[
\frac{dh_i}{dt} = \left( \frac{\partial h_i}{\partial \rho} \right)_p \cdot \frac{d\rho}{dt}
\]

enables to formulate a simple equation system

\[
K_1 \frac{dp}{dt} + K_2 \frac{dp}{dh} = \gamma_m \text{ (+)}
\]

\[
K_3 \frac{dp}{dt} + K_4 \frac{dp}{dt} = \gamma_h \text{ (+)}
\]

with

\[
K_1, K_2, K_3, K_4 \text{ - parameter constants}
\]

\[
\gamma_m \text{ - disturbance-related mass flow rate}
\]

\[
\gamma_h \text{ - disturbance-related energy}
\]

The level of the water steam mixture will be calculated as a function of the steam content as well as the water and steam mass flow rates. With the scheme presented in Figure 3, it is possible to show two applications:

1. The real-time calculation of the water steam mixture level, not to be measured
2. The diagnosis of the measuring device function.

Another possibility of model correction presented can be used only to a small extent.

4. Experimental works for verification

For experimentally checking the dynamic behaviour of the pressure vessel and the level measuring methods a pilot-scale plant was installed at the Technical University of Zittau. The scheme of the experimental arrangement is presented in Figure 4. 

For simulating real operation transients the following manipulations are possible

- to feed water with varying temperatures into the lower vessel part (water-filled room)
The pilot plant is designed for a pressure of 4 MPa. For demonstrating the generation of experimental data the comparison vessel instrumentation for the hydrostatic level measurement is presented in Figure 5. A very difficult problem is the determination of the loss of steam and water from the comparison vessel into the pressure vessel.
For model calculations and the interpretation of the experimental data the steam content distribution and the steam bubble velocity have to be known. /3/

Figures 6 und 7 present the principle for the measuring method developed for this purpose. It is based on the fact, that steam and water have different electrical conductivities. Hence the contact time of the steam bubble can be determined by the sensor owing to the transient electrical signal. By integrating the
FIG. 6. Measurement of the steam content (for calibration).

![Diagram of a sensor measuring device](image)

time values $t_K$ and $t_F$ the local steam content $\gamma_L$ during the measuring period can be determined:

$$\gamma_L = \frac{\int t_K \, dt}{\int t_F \, dt}$$

Experimentally determining the steam bubble velocity results in greater difficulties. For this end a method with sample-recognition was developed. Therefore it is possible to determine the velocity of such bubbles, which will be caught centrally.
A quantity for this criterion is the difference between a standard function for the reciprocal time difference, illustrated in Figures 8 and 9. Dependent on the sensor type the following measuring failures are to be mentioned.

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Steam content measurement</td>
<td>5 %</td>
</tr>
<tr>
<td>Steam velocity measurement</td>
<td>10 %</td>
</tr>
</tbody>
</table>

![Graph](image1)

\( n : 0 \ldots \) comparator level
\( t_i : \) time period between comparator level sequence

**FIG. 8.** Scanning the analog signal for the determination of the steam bubble velocity.

![Graph](image2)

**FIG. 9.** Real function and standard function for value \( 1/t_n \).
5. Concluding remarks

Applying simulators for increasing the accuracy and reliability of automatic control systems will be possible and is useful with the hard-ware available. The most important work is the development of useful and reliable soft-ware.

For verifying this soft-ware it is necessary to develop special pilot plants including the development of specific measuring methods. Material and intellectual expenditure for verification is much greater than the efforts for soft-ware development.

REFERENCES

/1/ Scholz, A.  Traineranlagen für Kornkraftwerke

/2/ Hampel, R. et al  Ausgewählte Probleme der Höhenstands-
messung für Druckbehälter in KKW mit WWER

/3/ Hampel, R. et al  Experimentelle Untersuchungen zur
Höhenstands messung an liegenden Dampf-
erzeugern für KKW mit WWER
Wiss. Berichte TH Zittau 1989
Konferenzbeiträge Session VI p. 61
APPLICATION OF COMPUTERS FOR
CONTROL AND PROTECTION FUNCTIONS
IN RESEARCH AND POWER REACTORS

G. GOVINDARAJAN
Reactor Control Division,
Bhabha Atomic Research Centre,
Bombay, India

Abstract
This paper describes the application of Computer/Microcomputer
based systems in Indian Reactors at present and in future. The
concepts of fault tolerance, redundancy, isolation of control
and safety functions, avoidance of error propagation, continuous
monitoring and diagnostics are being followed in all configura-
tions. Many standalone systems have been designed and installed
for Research Reactors DHARUVA, KAMINI and 235 MWe PHWRs. Whereas
for 235 MWe programme, the task has been to upgrade and modernise
existing controls, the 500 MWe arena is mainly for developing new
concepts.

The areas of computerisation included computer control of on-
power fuel handling systems for 235 MWe PHWRs, Microprocessor
based control and trip systems for KAMINI, Operator Support/
process information systems such as channel temperature and
flow monitoring Digital Recording etc. The present development
include, programmable Digital comparators for the generation of
trips and alarms, PHIT Pressure, Boiler Level and pressure controls
for 235 MWe Units, microprocessor based shut down systems, Reactor
Regulating Systems, Channel Temperature Monitoring with set back
functions etc. for 500 MWe Units.

The microsystems are configured in fault tolerant mode to have high
availability of the systems and also yields for on-line servicing.
Dual computer configuration with hot standby or three channel con-
figuration with 2 out of 3 coincidence voting logics/median selection
modes of operation are being envisaged for critical functions.

The hardware design of Micro is inhouse and incorporate features
not generally available from standard manufacturers. These include
fine impulse testing and output read back facility, software and
hardware watch dog timers, output freezing due to CPU malfunctions.
Auto calibration of Analog inputs etc.
Since the software in an important aspect for reactor use care has to be taken from beginning of the development. A structural programming approach is being adopted. Modularisation of programme functions, minimising interface between modules, fault detection and diagnostic programmes, verification and validation of software, simulated extensive testing of the systems for normal and abnormal condition of inputs are being the guidelines of development. Hardware reliability analysis also forms a part of the programme.

1.0 Introduction

It has been recognised that the use of computer based control in Nuclear plants enable incorporation of advanced control algorithms, providing greater flexibility and sophistication, self checking features and better man-machine interface for superior information presentation. To exploit these advantages of computer based systems, a judicious step by step approach was felt necessary mainly to gain expertise in development, operation and maintenance of these systems. Computer based systems have already been developed for applications like Data Acquisition and Plant Monitoring, Fuel handling controls (Narora Atomic Power Project), Channel Temperature Monitoring (NARORA and Madras Atomic Power Station), Process information, control and trip system for 30 KW Thermal Research Reactor KAMINI.

The present development of computer based systems include programmable Digital Comparators, Boiler Pressure and level, PHT Pressure controls and Advanced Fuel Handling Controls for 235 MWe Units, Reactor Regulating Systems, shut down systems and channel temperature monitoring with set back etc. for 500 MWe units. These systems have flexibility of being interconnected through High Speed Dual Redundant data high-way being presently under development. The concept of computer control for these systems, including proposed micro based shut down system for 500 MWe, are described along with the philosophy followed in development of hardware and software with emphasis on safety and reliability. It is to be mentioned here that the
functioning of control system is delinked from performing safety functions in order to have a higher reliability and guard against spurious actuations.

2.0 On-power Refuelling of PHWRs

A computerised control system has been implemented for control of Fuel Handling System (FHS) of Narora Atomic Power Project (235 MWe) reactor. The FHS provides on-power refuelling of reactor channels, remotely. These operations are carried out by two Fuelling Machines, mounted on bridges and carriages on the two sides of horizontal reactor calandra and two Fuel Transfer Systems, which provides new fuel bundles to the machines, receive spent fuel from it and transfer them to the storage bay. The operations of these four systems/machines are controlled remotely by a computerised control system.

The fuelling machines become a part of the Reactor System during on-power refuelling operations. The machines handle reactor coolant (heavy water) which is radioactive and is under high pressure and temperature. They also store hot spent fuel bundles during transit from reactor channel to the storage bay. The machines are inaccessible during these operations because of high nuclear radiations and hence the components and equipment of these machines have to be highly reliable. Thus safety and reliability aspects have been important criteria in the design of mechanical and hydraulic systems as well as in the design of the control system.

2.1 Computer control system for FHS

The control system is configured as a dedicated network of one minicomputer as a supervisor and two microcomputers each controlling one fuelling machine and one fuel transfer system. To ensure high level of safety, all computer outputs to the machines are routed through external hardwired safety interlocks. Figure 1 shows the scheme of control adopted for FHS.

The control system can be operated in three modes, i.e., full Auto, Semi-auto and Manual modes. Normal operations are carried out in full automode. In case of a fault in any mechanical or hydraulic component, retrieval operations can be done in semi-auto mode. Since semi-auto mode is provided by microcomputers, this mode can also be used to carry out all machine operations in case minicomputer fails. In case of microcomputer failure, operations can be carried
FIG. 1. Computer control of fuel handling system for NAPP.
out in manual mode which provides simple push button operations through hard-wired safety interlocks. Thus degraded modes of operations during partial system failures has been provided.

The microcomputers use simple cycle based real time executive and no interrupts are allowed during active cycles. Flow of control during active cycle is predetermined, to enable effective on-line check on software. Since the operation of the machines is predominantly sequential in nature with some continuous logic checks required on all parts of the system, the logic is divided into sequential Steps and process Tasks. The steps and tasks are written in a simple block structured Process Control Language (PCL) developed for this purpose. The PCL codes execute under the control of an interpreter.

This configuration enables thorough checking and verification of on-line software. The executive incorporates on-line diagnostics which check memory and input/output boards. Flow of control of software is also checked and a watchdog timer trips and halts the machines on detecting any fault.

The control system incorporates a very elaborate operator's console for operation in the three modes. Status of all sensors on the machines are displayed independent of computers. In addition comprehensive status of operations and fault conditions is displayed on CRT displays and is also logged on printers. This ensures that operator's are fully informed of the system status.

The control system as described above has been commissioned at reactor site. It is recognised that full potential of computer control can be realised, if algorithms for monitoring the health of machines and hydraulic components are incorporated in the control system. The control system can monitor the performance of various components and report degradation in performance. This shall enable maintenance/repair to be carried out such that chances of failures during on-line operations are minimized. Work on incorporation of these features has been taken up.

3.0 KAMINI Reactor Control and Protection System

KAMINI (Kalpakkam Mini Reactor) is a 30 KW swimming pool type reactor using U-233 fuel, moderated and cooled by light water for Neutron Radiography of fuels and Radiation Physics Experiments.
The reactor is controlled with the help of two safety cum control plates made of cadmium.

The reactor is operated from a control panel which houses three CRTs for control and information display as well as conventional controls and display instruments. The control and Interlock system is structured around microprocessors. A dedicated CRT along with associated key-board is used for operations like reactor start up normal operation and shut down. The operator is guided regarding sequences of operations through messages on CRTs. Suitable software based interlocks and logics have been incorporated to prevent undesirable actions by the operators leading to unusual occurrences. Elaborate diagnostic messages are given on the CRT to identify the cause if intended action is not carried out.

The process information system acquire and display plant status in the form of dynamic pictures, mimic diagrams, tables, trends, bar graphs etc. The alarm annunciation system process digital signals to warn the operator about disturbances in the plant through alarm windows and CRTs. The microprocessor and CRT based controls and display system has completely replaced conventional controls, meters recorders etc. The Kamini reactor can be operated through key board commands and all relevant data for safe operation is conveniently displayed in CRTs.

The Reactor trip system is fed with 16 digital inputs as shown in Table 1. If any of the trip input goes to a trip state for at least 50 ms, the trip system deenergises the clutch coils of safety control plates. Two separate independent channels with 1 out of 2 strategy for the trip output are employed. The trip system is independent of the control system.

4.0 Digital control of PHWR processes

The process control of critical sub-systems of PHWRs such as Primary Heat Transport system and Steam Generator pressure and level control were based on analog type hardwired modules in earlier plants. During the present decade, the problems of obsolescence and difficulties in achieving high reliability of assorted instruments used, combined with the availability of reliable and in-expensive digital hardware, provided the motive force for introduction of digital computer for future plants.
### TABLE 1. KAMINI TRIP INPUTS

1. Linear Power High  
2. Log Power High  
3. Log Rate High  
4. Nuclear Channel Unhealthy  
5. Reactor Tank Temp. High  
6. Demineralisation system not ON  
7. Water Activity High  
8. Vault Radiation High  
9. Reactor Lid Open  
10. Reactor Lip Open  
11. Vault Doors Open  
12. Reactor Tank Leakage  
13. Safety Plate not Top Position when control plate not at bottom limit  
14. Reactor Tank Water Level Low  
15. Ventilation system not ON  
16. Manual Trip

Microcomputer based system can perform system monitoring and control functions with far greater flexibility, precision and reliability and thus advanced control algorithms can be easily incorporated. To ensure safety and improve reliability, dual computer system (main system with hot stand-by) and 2 out of 3 systems are considered. Fig.2 indicates one of the proposed schemes.

Safety features of the new control systems for steam generator and primary system controls include:

1. Easier and more extensive testing  
2. Improved man-machine interface minimising erroneous operations leading to unsafe situations  
3. Extensive self-checking to isolate faulty hardware  
4. Arrangements for testing alterations in control algorithms and settings before its final implementation.
5.0 Reactor Regulating System for 500 MWe Reactor

The regulating system is designed to provide automatic control of reactor power between $10^{-7}$ F.P to full power. While maintaining the overall reactor power at the demanded level; to maintain neutron flux profile close to its design shape, zonal power control is exercised through level control in light water compartments in the core. Solid control and adjustor rods also take part in zonal power control in addition to global power control. The reactor has 21 adjustor rods, 4 control rods and 14 light water compartments for exercising the overall control strategy.

The control system has both set-back and step-back features that are activated under abnormal operating conditions.

The reactor regulating system is a distributed digital control system networked via dual redundant high speed data link. All control nodes have dual redundancy for high reliability and fault tolerance. Fig. 3.
Information and command flow between the systems and the operator is provided through a centralised RT based control console. Real-time graphic presentation of the reactor process offers a comprehensive man-machine interface. The scheme under development is shown in Fig. 4.

6.0 Programmable Digital Comparator System

The PDC process various analog process parameters (3 x 128), refer Table 2, to detect whether these are in normal operating band or outside it. In the later case the system gives alarm output in the form of relay contacts for use in interlock logic systems controlling the reactor equipment and processes. Fig. 5.

The advantage that the system provides over conventional indicating alarm meters is that the set points can be altered or monitored by a central display unit. Set point variations are effected by keyboard entries rather than potentiometer adjustments, which required verification by disturbing the input parameter.

The system is organised as a triplicated microprocessor based core unit called the Alarm Unit coupled via serial communication links with a display unit - maintaining functional and electrical isolation between the safety section and the operator interface.
FIG. 4. Reactor shutdown logic system.

TABLE 2. TYPES OF PROCESS INPUTS TO PDC

1. PHIT Header Pressures (4/20 mA)
2. Boiler (steam gen) Levels (4/20 mA)
3. Calandria (D₂O) level (4/20 mA)
4. Heat Exchanges Inlet Temp. (RTD)
5. Coolant pump
   - Seal cavity temp. (RTD)
   - Oil temp. (RTD)
   - Gland injection flow (4/20 mA)
6. End shield coolant outlet temp. (4/20 mA)
7. Coolant channel flows (4/20 mA)
8. D₂O storage tank level (4/20 mA)
9. Cross PHIT T (4/20 mA)
10. Bleed condenser level (4/20 mA)
11. Boiler ΔT (4/20 mA)
12. Fuelling machine vault temp. (RTD)
13. Control rods coolant flows (4/20 mA)
14. Absorber rods coolant flows (4/20 mA)
15. BPC Controller Set Points
16. Steam Generator Inlet Temp. (3/20 mA)
Data presentation in the form of tables and menus on a CRT make the information comprehensive and the operator can grasp the situation easily.

Fail-safe design philosophy has been adopted for both hardware and software as outlined in the following:

2. Hardware qualification and testing.
7.0 Safety Aspects of Computer Based Reactor Control & Protection Systems

7.1 General
a. The Fail-safe feature is provided through both hardware and software routes.

b. A computer system, being an intelligent programmable system, is able to incorporate self-diagnostic facility.

c. Emphasis is put on software verification. To enable complete verification, modular structure is adopted for software also, as is done for hardware. Diagnostic program module is separate and independent of other modules so that maximum test coverage is achieved.

7.2 Testing and Fault Detection
a. Two modes of testing/fault detection:
   i) Resident on-line testing by internally generated stimuli
   ii) Off-site asynchronous testing by externally generated stimuli

   Either mode perform end-to-end testing i.e. from input interface to output interface.

b. Testing Modes:
   i) Hardware checks software
      (for control flow of the programs)
   ii) Software checks hardware
      (for data flow paths and memory/data storage elements)
   iii) Software checks software
      (for data and program integrity as well as range checks and acceptance checks of critical program variables).

c. A computer system depends on sequential execution of instructions in a programmed order. So the foremost concern in using computers in reactor instrumentation is:
   i) Halting of program execution (or infinite looping)
   ii) Program execution along improper path
   iii) Restart after power fail
Since hardware and software are two diverse aspects of a computer system - detection of above software faults should be implemented by hardware (doing timed signature checking of the program control flow). This method generates greater confidence than software checking by software. However, both may be complementary.

7.3 Software Features

i) Multiple-version of software to eliminate common bugs

ii) Looping and branching avoided to the extent possible.

iii) In the loops - infinite looping is prevented even under conditions of faulty state variables

iv) Each module has single entry and exit point to reduce program complexity

v) Static order of priority assigned to each module so that control flow remains the same. This enhances the predictability of software and verification of control transfer from one module to its successor module is easy.

7.4 Fail-safe and Fault Tolerance Features

a. To make the overall system fail-safe, fail-safe outputs are to be generated by the hardware upon detection of software fault.

The hardware peripheral sub-systems are designed to sense software fault signals to go to preprogrammed failsafe states (or in certain cases frozen to the last valid states (values)).

b. Instead of centralised realisation/processing of all functions - distributed processing of various functions should be adopted so that one redundant channel can borrow the results of its unavailable function from another channel. This can be done via redundant data high ways networking the distributed nodes. Such implementation will enhance system availability.

c. Intercomparison of results from redundant channels can be done to detect disagreeing channel - to reject the same to take action according to the safer (e.g. calling for lower rate of withdrawal of control rods) channel. Under all healthy conditions median value or average value may be adopted.
d. Power-fail and Power-on Restart

Since high density ROMs and RAMs are available restart need no more involve transfer of program from a magnetic storage medium to semiconductor memory. So system qualification for seismic conditions are possible. Also power supply monitoring circuitry are so well developed that system can load current program information on non-volatile stack. So also data in non-volatile RAM. So on power-on restart, system can begin from where it left - thus achieving bumpless 'return to normal' on severe power dips.

8.0 Hardware Design and Qualification

8.1 Design considerations for hardware

1. In general, design undergoes FMEA (failure mode and effect analysis) so that the hardware is failsafe to the extent possible.

2. For the residual unsafe failure modes on-line testing and reporting features are incorporated.

3. All external connections (inputs & outputs) are galvanically isolated from the system. Isolation tested to 500 VDC or AC peak.

4. Since systems often employ multiple DC supplies, on system AC power ON, the DC supplies are applied in ordered sequence to avoid over-stresses on the devices.

5. Design of PCB connectors takes care of possibility of removal or insertion of PCBs on-power - since this is the normal tendency of maintenance personnel.

8.2 Hardware qualification and testing

In order to ensure high reliability required for reactor instrumentation system, the following procedures are adopted:

1. Procurement of components:

High reliability components are used. These are manufactured to MIL standards relevant to the component class.
b. Components like connectors, MIL-C-83503, MIL-C-55302 resistors MIL-R-10509, capacitors MIL-C-11015, cables etc. are subjected to batch acceptance tests (including destructive tests).

c. Printed wiring board layouts follow the military specifications MIL-STD-275. Laminates are flame retardant glass-epoxy. Seismic considerations are applied to component orientation and mounting.

Edge connectors are not used. Instead two piece male-female connectors are used. For flat ribbon cables strain relief and locking types of connectors used.

2. Instrument racks and enclosures are reinforced for proper damping under seismic conditions:

3. Sub-systems are tested after packaging for withstanding DC power supply extremes, shock and vibration conditions. Functional tests on integrated sub-systems are also carried out at temperature extremes (0°C/55°C).

4. Integrated overall system is tested at AC power extremes. As per JSS 55555 the system is tested at high temperature ambient (45°C) keeping all cabinet doors closed and internal cooling off. This test is carried out for 100 hours continuously to check for excessive build-up of temperature gradient and hot spot generation.

9.0 Software Design and Development Methodology

The software used in computer based reactor I & C systems forms one of the vital components contributing to the reliable and safe performance of these systems. Due to the fact that design and development of software proceeds through complex and inter dependent phases it has been recognised that formal and systematic approach to its design and development is necessary to produce reliable software. The nature of software further complicates the verification and validation activities. One overall software design and development approach uses well accepted practices. All stages in software design and development are formally identified. The design process is based on progressive and systematic decomposit-
ion of requirements leading to structured design and set of documents. At each stage verification/review is carried out to ensure fulfilment of requirements at the previous stage. The various phases in design and development of software are briefly described below:

9.1 Program design and development method

The various design and development activities relating to software run parallel to other activities such as hardware design and development quality assurance and test procedure design and documentation preparation interacting with them at different stages. This is illustrated in accompanying figure 6.

The software design begins with the customer supplied system requirements in the form of Design Basis Report (DBR). The software requirements are then jointly evolved (with customer participation) and subjected to review to ensure that all requirements are being met. This results in to software requirement specification document which forms the basis of design and development. Although use of formal tools is contemplated, presently requirements are expressed in natural language.

![Figure 6. Software design and development process.](image-url)
Next, the software design proceeds using top-down approach which leads to translation of software requirements into tasks/modules with well defined scopes and interfaces to other tasks/modules. State transition, diagrams or graphic diagrams showing interrelation of various tasks in the system with each other are employed to express software design in more comprehensible term. This software design is subject to internal review for ensuring compliance with the software requirement specification.

Coding is the next phase. This phase is supported using editors, cross assemblers, cross compilers (pascal, C) which are widely supported by industry and have been in use over long periods. The unit/module tests also supported by emulators, debuggers with program break point/program tracing facilities. Critical module execution times are measured to ensure satisfaction of system timing requirements.

System integration and validation testing is the next step. The system validation testing is carried out as per approved test procedure. System tests are carried out as far as possible with full system configuration and fully simulated digital and analog input/output. The tests are aimed at fully covering the analog input ranges, system timing under normal and peak load conditions, accuracy and correctness checks on outputs, conformity of information content and format with the requirement specification system access security checking and full functional checking. The results of system validation checks are jointly reviewed.

9.2 Special considerations for safety and safety related systems

The methodology outlined above is applied to all development projects related to reactor I & C systems. In case of systems applied in safety or safety related areas the recommendations of IEC-830, relating to use of operating systems, use of interrupts, proper identification and partitioning of critical and non-critical software, simplicity of design diagnostic checks etc. are being followed.
PLANNING, DESIGN BASIS AND REQUIREMENT SPECIFICATIONS FOR THE PLANT COMPUTER REPLACEMENT IN KRŠKO NUCLEAR POWER PLANT

D. MANDIĆ
Krško Nuclear Power Plant,
Krško, Yugoslavia

Abstract

Nuclear Power Plant Krško (NEK) has been in operation for almost eight years. Most of the equipment installed in the plant was purchased more than ten years ago and this equipment is mostly the state of the art of the technology of early 70’s. In our plant we use Westinghouse P-2500 as a main plant computer and a large variety of different process computers or data acquisition systems (more than 15) from micro grade, mini grade and large computers as it was considered 20 years ago. Some of these computers are used just for process supervision, alarming and data logging, some for sophisticated on line calculations as support to the operators, and some for real time closed loop process control.

In the past years we were facing serious problems in the field of process computers, so we have decided that we will introduce a new process computer system based on professional and reliable unique data acquisition system, advanced MMI, capable computer power for real time support to operators in the MCR and powerful computer for sophisticated extended real time processing, for process data history files management and for the network support to the “OUT MCR” users of process data history files.

In this material we will explain what is our plan how to perform such a complex function, what are the design basis for future Process Information System and what are the system requirements specification. The main items from our material called “DESIGN BASIS AND REQUIREMENTS SPECIFICATION FOR THE PILOT PROJECT OF THE PROCESS COMPUTER REPLACEMENT IN KRŠKO NPP” (Lit. 6.1.) will be discussed too.

1. INTRODUCTION TO THE PROBLEM

1.1. The main problems with our process computers, that forced us to think about process computers replacement and integration can be summarized as follows:

- Impossibility to develop new applications or to expand the old ones on most of the existing computers.
- New requirements and regulations force us to implement new functions and to improve MMI (Man Machine Interface) but this is not possible on the existing equipment.
- There is no data link between the existing equipment and it is impossible to create something like history files or to centralize process data collection.
- The data from all process computers are not available in the MCR because many process computers have only locally mounted MMI devices.
- Maintenance of hardware equipment from more than 10 different manufacturers is very complicated and expensive.
- Spare parts for most of the existing hardware equipment are not available.
1.2. Our goal is to build up new Process Information System (PIS) according to the design basis and system requirements specifications defined by NEK. We already know that during the design and implementation period we will have to face the problems among them the outstanding problems are:

- Some of the existing process computers will have their place in the new system too. The new process computer system has to provide means of data integration in spite of different manufacturers and computer technology concepts.
- New field cable pulling has to be minimized.
- Existing plant computer and corresponding data acquisition system has to be replaced in one outage.
- After the outage, when the old plant computer will be replaced, all software that will supersede software on the existing plant computer has to be implemented and operable on the new system.
- Some new field sensors have to be installed to satisfy new requirements and regulations. Some of them have to be installed on the safety related equipment or components, that can complicate design verification and regulatory licensing.
- The main control room outlook will be changed, some operational procedures for operators have to be changed, and operators behavior and customs have to be changed.

2. NEK PLANT COMPUTER REPLACEMENT PROJECT PLANNING

We have decided to build the new process computer system based on the design basis and system requirements specification defined by NEK and NEK expert's experience. As the first step we are trying to collect all technical information from potential suppliers and manufacturers. We think we can get a feeling about the state of the art of vendors solutions and technology only by an example of the real project. We can get some opinion analyzing vendors references but comparing two different solutions of two different manufacturers would be impractical because references are usually not the same. Problems that we want to solve are complex and we think we would waste our time if we tried to announce something like a tender and requested from the manufacturers a fixed and final proposal. Proposal for a complete project cannot be done without some hard working man/months spent on our site and even then we are sure that during the design phase many things will be changed. Our decision is that we have to start with something that we have called a PILOT PROJECT. We made material that we called: "DESIGN BASIS AND REQUIREMENTS SPECIFICATIONS FOR THE PILOT PROJECT OF THE PROCESS COMPUTER REPLACEMENT IN KRSKO NPP". Such PILOT PROJECT will never be completed in the very same scope as it was specified in the referenced paper. In that paper no solutions for the nuclear specific applications were requested. That is a simple and relatively small system of data acquisition, MMI and computing power. We expect different vendors to give us solutions for the PILOT PROJECT using their hardware and software tools, the same as they would use for a big system in a NPP. All technical documentation describing their technical solution for our PILOT PROJECT was welcome and kindly requested (schematics, drawings, manuals, system descriptions, maintenance procedures, example of program listings, catalogues, technical specifications, etc.). After receiving proposals for the PILOT PROJECT we hope we will be able to select the solutions that will suit our needs best. We have already spent two years by preparing the main project. We believe we are very close to be a hundred per cent sure what exactly we want out of the main project. After technical evaluation of the PILOT PROJECT proposals we will be ready to request a few suppliers to prepare, working together with NEK experts, a final proposal for the main project. After the technical and commercial evaluations of such main project proposals are made we will be ready to give the contract to that supplier that will best suit our needs and capabilities. The project plan and schedule has been established, general schedule is given in App. I, and the main activities in the process of NEK Process Computer replacement are listed on the next page.
2.1. PREPARATION PHASE

2.1.1. Collection of literature, informations and other plants experiences.
2.1.2. Establishing Functional Requirements (interviews, studies, discussions).
2.1.3. Defining Design Basis and Design Basis acceptance.
2.1.4. General System Requirements Specification, validation and verification.
2.1.5. PILOT PROJECT definition, Design Basis and Requirements specification, bidding for proposals.
2.1.6. Criteria specification for Pilot Project different solution evaluations.
2.1.7. Pilot Project proposals evaluation.

2.2. CONTRACT PREPARATION PHASE

2.2.1. Detailed requirements - scope specification (with the most convenient vendors on the basis of Pilot Project).
2.2.2. Technical & commercial negotiation process (request for quote, proposals, evaluation, decision about vendor).
2.2.3. Preparation of contract, signing the contract, purchase order.

2.3. DESIGN PHASE

2.3.1. Detailed hardware architecture design
2.3.2. Detailed software functional specification
2.3.3. Software system design
2.3.4. Detailed program modules specification
2.3.5. Program modules design
2.3.6. Software integration and testing

2.4. DESIGN VERIFICATION

2.4.1. System Mock-up installation (Vendors plant)
2.4.2. Hardware and software system integration and testing
2.4.3. NEK personnel design verification and training

2.5. NEK SITE INSTALLATION

2.5.1. New sensors and cabling installation
2.5.2. Field cabinets installation & testing
2.5.3. MCR equipment installation and testing
2.5.4. Hardware and software system integration and testing
2.5.5. PIS start-up and operation

3. SYSTEM DESIGN BASIS

After detailed study of the problem and our goals we have made several conclusions that established system design basis:

3.1. We will introduce a new process computer system based on professional and reliable unique data acquisition system, advanced MMI, capable computer power for real time support to operators in the MCR and powerful computer for sophisticated extended real time processing, for process data history files management and for the network support to the "OUT MCR" users of process data history files.

3.2. Special functions requested by nuclear regulations (SPDS, ERF, TSC,...) will be incorporated in the new process computer system concept as special functions on the same hardware and not as a special function on a dedicated hardware. For some special functions data acquisition hardware redundancy can be increased, but basically that will be done in the same system architecture.

3.3. We will establish centralized (centralized just from the user's view, not needed to be real hardware centralization) real time process data base, centralized and unique process data history base and capability to the "OFF MCR" users to reach that process data history base.
3.4. We would like to reduce complexity and the cost of the process computers hardware maintenance, so we would like to train our people to be able to maintain the new equipment by themselves. Hardware troubleshooting has to be simple, mostly automatic, and repairs based on the PC boards replacement.

3.5. SYSTEM ARCHITECTURE: The Pilot Project General Schematic in the Appendix 2, gives the system architecture according to the best of our present knowledge and experience. Vendors can propose different system architecture, if they guarantee same or better performance than requested in our Pilot Project Requirements. The PIS has to have three main hardware levels:

- RT (Real Time) DAS (Data Acquisition System) LEVEL - Level 1, for real time data acquisition, and simple RT calculations.
- RT (Real Time) COMPUTER LEVEL - Level 2, for extensive RT computing, limited process data history files and MMI support.
- ERT (Extended Real Time) COMPUTER LEVEL - Level 3, for extended real time and time consuming computing, process history data base management and storage, LAN support for the OUT MCR users of the process data.

3.6. REDUNDANCY: All data links between levels 1 & 2, and 2 & 3 have to be redundant. Level 2 CPU has to be installed in the redundant configuration. Redundancy for the Operator Work Station (OWS) is performed by the following rule - On each operator's location, the number of the peripheral equipment of the same kind (complete OWS, or only VDU, KYB, PRNT etc.) has to be at least one more than the requested minimum for that location. Redundancy inside DAS (input channel for single process input) is not requested. Redundancy for the input signals is usually done by multiple sensors of the same process variable, connected to different FIELD DAS units. Power supplies inside the cabinets for electronic circuitry DC supply voltage have to be redundant in hot standby mode (slightly different output voltage, parallel connection of both power supplies and diode actuation-selection between active and passive PS, or something similar).

3.7. Some process signals for DAS are already cabled to the MCR (MCR DAS), and some have to be collected in the field by locally installed DAS equipment.

3.8. Some process computers from the existing process computer system (CPU A, B, C, D) will have their place in the Pilot Project (and real final project) too. One of the functions of the CPU A-D will be to pass process data and calculations performed by those CPUs to the new PIS. The device called FEP&MUX acts as an interface between old CPUs and new PIS. Data link between CPUs and FEP&MUX is a simple RS-232/c serial link. Data from CPUs to the FEP&MUX are sent in the data stream of the fixed format, so FEP&MUX can recognize each data by its order-location in the data block. FEP&MUX has to perform all needed data formatting, time tagging and communication protocol handshaking to pass the information to the Level 2 computer.

3.9. Project for PIS has to give solution for the remote OWS, that has the same capabilities as OWS in the MCR.

3.10. Operating system and application software for the hardware of level 1, level 2 and data communication have to be written in the way that enables the trained computer personnel to make all necessary changes that can be required by application tasks growth or number of system inputs growth.

3.11. System has to be designed in the way not to lose any of its functions or capabilities in the case of appearance of any single hardware failure.
3.12. EXPANDIBILITY AND MODULAR DESIGN - The Pilot PIS (and later the main real project) has to be designed in that way to enable the modular system to expand in hardware and software structure on all system levels.

4. SYSTEM REQUIREMENTS SPECIFICATION

Detail system requirements specification for our PILOT PROJECT are given in material specified under the Lit. 6.1. In the following text selection of the most significant requirements will be explained.

4.1. DATA ACQUISITION

4.1.1. FAST ANALOG SCANNING OPTION: For selected, and limited number of inputs, the system has to have capability to activate fast scanning, triggered by program (Sequence Of Events or others), and for limited time scan with high scan frequency.

4.1.2. EXTERNAL INTERRUPTS (EI) SERVICING: EI are type of Binary Inputs that are equipped with additional hardware which provides servicing of the Binary Input that has just changed the state on the interrupt basis, not scan basis as all other Binary Inputs. EXTERNAL INTERRUPTIONS have to be proceeded from DAS to RT CPU for servicing. System has to be designed in the way to insure no EXTERNAL INTERRUPT lost in case of different EI appearing.

4.1.3. TIME TAGGING: Each data collected by DAS has to be time stamped in the very same time of appearing or collecting from the field. Master real time clock runs inside the RT CPU, and all other FIELD DASs, MCR DAS and FEP&MUX with their local RT are synchronized to that master clock. RT clock resolution is 1 ms (1 kHz). AI and BI get the time stamps that correspond to their scan time. EI gets the time stamp that corresponds to the very same time of EI appearing ± 1 ms of RT clock resolution. If the synchronization between RT CPU clock and RT clocks of CPU A, CPU B, CPU C, i CPU D can not be achieved, data from those processors get their time stamp when they arrive in the FEP&MUX. All process data manipulation and RT CPU DBMS has to be designed to support and to reference time tagged data.

4.2. RT CPU & PERIPHERALS

4.2.1. RT CPU has to be real 32 bit processor (32 bit parallel processing, bi-directional 32 bit data bus, 32 bit address bus), with floating point processor, with hardware interrupt capability and all other powerful features that are listed in our material from Lit. 6.1. Main memory has to be equal or greater than 16 MB.

4.2.2. CPU COMMUNICATION AND REDUNDANCY: RT CPU has to be redundant, synchronized and closed coupled in the way to insure no PIS breakdown in the case of the active RT CPU failure. The other RT CPU has to be always in hot standby mode and capable to take over all RT CPU functions without system performance degradation from the MCR operator or DAS viewpoint. Shared memory by two RT CPUs is allowed but not requested by this requirements. All solutions that can satisfy stated requirements are allowable.

4.2.3. OPERATOR WORK-STATION / MAN MACHINE INTERFACE: In the running plant like NEK is, no significant changes can be done on the main control board. Control panels are "U" shaped with vertical and horizontal control board sections. To improve MMI in such MCR, only the cluster of operator work-stations can be installed in the middle of MCR, in front of the "U" shaped panels. Special care has to be taken during the design phase. Operator work stations are special powerful graphic processors, whose main goal is to provide adequate MMI.
4.3. SYSTEM SOFTWARE AND TOOLS

4.3.1. RT CPU OPERATING SYSTEM: The real-time operating system software supplied has to be the latest version of the operating system widely in use for RT computer industrial application. The operating system shall have the following characteristics: Good performance and convenience, a multi-tasking operating system, multiple & dynamic software priority levels & dynamic system memory allocation, virtual memory support, system procedures for task activation and support, control and servicing of standard peripheral devices including queued I/O support, support for on-line program development and testing, file management support, services, a failed device program has to be provided to switch to the alternate device if a device fails, a software configuration and Control System has to be provided, control & control data communication between tasks, control task I/O handling, capability to recognize, share and manipulate with I/O resources. Operating System that cannot be disturbed by the hard disk failure (Memory Resident OS) is greatly appreciated. In such case hard disk is used only during the System loading, for the extensive process data history file storage and during the new application development linking and loading. The aim of such an approach is to eliminate all movable parts which failure can cause the System to crash.

4.3.2. RT CPU DBMS: has to provide capabilities for

a) RT process data storage and retrieval
b) Short-term history data base storage and retrieval
c) Calculations based on the data from a) and b), storage and retrieval of such calculated values.
d) Data tables altering, extension or generation.
e) Data sorting
f) Data base security
g) Forms, reports, screens or printouts generation

RT DATA TABLE and EVENT TRIGGERED DATA TABLE (during generation process) have to be main memory resident. SHORT TERM PROCESS HISTORY DATA BASE can be the hard disc resident. All RT Data Base to be main memory resident is preferred solution. Data base has to have features that provide RT data base Integrity, Consistency and Data Security.

4.3.3. EVENT TRIGGERED DATA TABLE: In addition to the RT data table which is updated on the predefined periodic basis, RT DBMS has to have capability to define and create EVENT TRIGGERED DATA TABLE. Such data table is created with optional number and types of inputs or calculated values, scanned usually with different frequency than normal scan frequency for those inputs, and created on an event triggered basis (hardware interrupt, operator request or program request).

4.3.4. SHORT TERM PROCESS HISTORY DATA BASE is created from the RT DATA TABLE values. When the new RT DATA TABLE value arrives, before it is written to the RT DATA TABLE, "old" input value with all its attributes is stored to the SHORT TERM PROCESS HISTORY DATA BASE. Such data base has to be organized in the way to be capable to store at least history data from the last 2 (two) hours of all process inputs and outputs and calculated values. Data older than 2 hours are lost if not sent to the level 3 ERT computer or used by some application in the level 2 RT computer.

4.3.5. ON-LINE SYSTEM TESTING AND TROUBLESHOOTING: Each intelligent unit in the Pilot Project PIS has to have some means of automatic self testing, troubleshooting and failure reporting to higher level hardware and to the operator.
4.4. APPLICATION SOFTWARE & SPECIAL FUNCTIONS

4.4.1. ERF & SPDS: Emergency Response Facility (ERF) and Safety Parameter Display System (SPDS) have to be integrated in the new Process Information System. The guidelines are given in Lit. 6.2., 6.3., 6.4. and 6.5.

4.4.2. SPECIFIC APPLICATIONS FOR NUCLEAR POWER PLANT: Most of the hardware, system software and even application software can be used for plant computer in any technological process or fossil power plant. Among the other applications, the set of application software for nuclear power plant has to have following:

a) Reactor control and protection system supervision - RCS AVG loop temperature setpoint supervision, PRZR level setpoint supervision, rod cluster control deviation alarms, reactor protection system monitoring package.

b) NSSS Process Supervision - OP and OP & delta T trip setpoint, Power Range channel signal calibrate check, Reactor Dynamic Thermal Output (RDTO), SG total thermal output from the secondary side (SGTTO), reactor thermal output (RTO), unit net efficiency, tilt print program, reactor load follow and search package, movable incore detector program - flux mapping.

c) In-core Thermocouples Analysis - two dimensional power distribution in the core, calculation of the relative power density distribution, calculation of radial tilting factors from relative power measurements.

d) BOP performance calculation and monitoring - heat rate evaluation, HP-turbine evaluation, MSR moisture removal effectiveness, heaters and pumps effectiveness, condenser vacuum.

4.4.3. SEQUENCE OF EVENTS (SOE) MONITORING AND ANALYSIS: SOE is special application that helps the operators in the process of post transient (or Plant Trip) analysis. Input data for SOE are logics derived from all Binary Inputs (BI), especially BI considered as an EI, and alarms based on the AI level checking. During some conditions (Plant Trips), generation of logicals (BI, EI, Alarms on AI) is so extensive and so time condensed that Cause and Consequence analysis is very hard. Special Cause and Consequence Tree analysis shall be provided to help the operator to detect the cause of particular disturbance, transient, or Plant Trip.

4.4.4. REDUNDANT VALUES (MEASUREMENT) PACKAGE: provides inputs for the failed sensor substitution. Some failed inputs can be substituted not only by the same type of redundant measurement, but also by the measurement that can after some calculations substitute failed measurement. This package is used for redundant measurement methods and to define failed sensor substitution by redundant sensor on the basis of redundancy logic 2 of 3, or 2 of 4.

4.4.5. ALARM REDUCTION LOGIC: Has to be implemented together with establishing alarms priorities to reduce the number of active alarms. Such logic shall prevent build up of unnecessary alarms (Example: When operator turns an pump off, unnecessary alarm is LOW FLOW, or LOW DISCHARGE PRESS). There are three main principles of reduction:

a) Reduction according to the CCT of events (Example same as above)

b) Reduction according to the signal level (Example: Clear LOW alarm when LOW LOW alarm is reached)

c) Reduction of the alarms that are not important in the moment of transient.
4.4.6. COMPUTER CONTROLLED OPERATOR'S PROCEDURES: Is special feature when operator acts according to the normal operational procedures or emergency procedures which are stored in the RT CPU (or mass memory device). In this mode of operation operator initiates process or process is suggested by menu driven selection from RT CPU (Plant CSD to HSD, Synchronization, Load Operation to HSD or similar). On any screen of OWS VDU there should be few rows of space for next step from accepted procedure. Operator performs actions according to the declared procedure step, and confirms to the RT CPU that action has been performed. Computer checks if the requested action has been really completed, informs the MCR operator if according to the status known to the RT CPU action has not been completed, and rejects display of next step. The MCR operator has to have the possibility to override procedure progress hold initiated by computer. In the normal progress with no RT CPU procedure step hold, as soon as the MCR operator confirms the action (RT CPU sees that is truth), next procedure step is displayed on the screen.

5. OPEN QUESTIONS AND CONCLUSION

In the present moment we are the witnesses of two approaches in the design for the plant computers in nuclear power plants.

The first approach leads to computer system dedicated only to supervision of the processes, data logging, real time or extended real time calculations, as support to the operators and maintenance personnel. Such system is independent from the control and protection system all the way from the field signal sampling to the MMI and data storage.

The second approach has goal to establish integrated process control, protection and supervision system. When we say integrated, it means that the system is integrated from the users' point of view, technology and data information. The performance and execution of different control, protection and supervision functions is divided among different pieces of equipment, but the most important is that the same or similar technology and architecture is used for all functions. Signals are converted from A/D only once, there is no MMI equipment dedicated only to one function, information can be passed to any terminal in the Process Information System.

The second approach has in some countries serious difficulties with regulatory licensing concerning system hardware architecture and verification and validation of software, but we think that the second approach is definitely solution for the future. Application software development for nuclear power plants has to move strongly towards Expert Systems. The main purpose of the real time or extended real time expert systems application in nuclear power plants is:

a) Early process disturbance detection

b) Disturbance analysis and the process disturbance cause detection

c) Disturbance development prediction (real time model accelerator)

d) Corrective action suggestion to the operator
6. LITERATURE


6.2. NRC NUREG-737, Supplement 1, 1982, Clarification of TMI Action Plan Requirements

6.3. NRC NUREG-696, Functional Criteria for Emergency Response Facilities

6.4. NRC NUREG-700, Guidelines for Control Room Design Reviews

6.5. NRC NUREG-835, Human Factors Acceptance Criteria for SPDS

6.6. U.S. RG 1.97., Rev. 3 - 1983, Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant and Environments Conditions During and Following an Accident

6.7. FSAR (Final Safety Analyses Report), NEK - 1979


6.9. Man-Machine Interface In The Nuclear Industry (Control and Instrumentation, Robotics, and Artificial Intelligence), proceedings of the IAEA International Conference, Tokyo 1988


6.11. IEEE Standard 802.3, CSMA/CD Access Method and Physical Layer Specifications, 802.1 Architecture and Interworking, 802.2 Logical Link Control


6.15. IEEE Std. 323-83 (74), Qualifying Class 1E Equipment for Nuclear Power Generating Stations.

6.16. IEEE Std. 344-87 (75), Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.
Appendix 1

SCHEDULE FOR NEK PROCESS INFORMATION SYSTEM
UPGRADE AND REPLACEMENT

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.1.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.2.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.3.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.4.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.5.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.6.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.1.7.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.1.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.2.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.2.3.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.1.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.2.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.3.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.4.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.5.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.3.6.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4.1.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4.2.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.4.3.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.1.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.2.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.3.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.4.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5.5.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

----------|------|------|------|------|------|------|------|

Appendix 2

NEK PROCESS COMPUTER REPLACEMENT
PILOT PROJECT

OUT OF THE PILOT PROJECT SCOPE
SCOPE OF THE PILOT PROJECT

OUT MCR IN MCR
SOFTWARE QUALITY SUPERVISION PLAN
FOR PLANT COMPUTER REPLACEMENT
IN KRŠKO NUCLEAR POWER PLANT

M. SMOLEJ
Krško Nuclear Power Plant,
Krško, Yugoslavia

Abstract

Nuclear Power Plant Krško has decided to replace the Westinghouse P-2500 plant process computer. We have already spent two years by preparing some feasibility studies, design basis and requirements specification for the project. The result of the effort is a material called "Design Basis and Requirements Specification for the Pilot Project of the Process Computer Replacement in Krško NPP" (July 1989). As a matter of fact we will add a new "Operator Aid (OA)" in the main control room to assist an operator in performing his job. The addition of a carefully planned and designed computer based OA should result in an increase in our plant safety and reliability.

Software is playing an ever increasing role in the design, manufacture, implementation and operation of an operator aid. So our utility must be prepared to monitor the supplier during every phase of the software life-cycle.

The paper describes our Plan for supervision of the particular phases of the software life-cycle (for example: study, design specification, design, design verification, operation and maintenance, documentation specification). Some typical check-lists for particular phases are also discussed.

1. Introduction

Nuclear Power Plant Krško has been facing with serious problems in the field of process computers, particularly with the plant process computer. After detailed study of the functional age and technological age factors, such as usability, reliability, maintainability, spare capacity, expandability, and the state of documentation, we decided to replace the Westinghouse P-2500 plant computer. We have spent two years by preparing some feasibility studies, design basis and requirements specification for the project. The result of the effort is material called "Design Basis and Requirements Specification for the Pilot Project of the Process Computer Replacement in Krško NPP" (July 1989).

As a matter of fact we will add a new "Operator Aid (OA)" in the main control room to assist an operator in performing his job. The addition of a carefully planned and designed computer based OA should result in an increase in our plant safety and reliability. We have made several conclusions:

1. We will introduce a new process computer based on professional and reliable unique data acquisition system, advanced Man Machine Interface, capable computer power for real time support to operators in the Main Control Room, and powerful computer for sophisticated extended real time processing, for process data history files management and for the network support to the "Out MCR" users of process data history files.
2. Special functions requested by nuclear regulations (SPDS, TSC, ...) will be incorporated in the new process computer system concept as special functions on the same hardware and not as a special functions on a dedicated hardware.

3. We will established centralized real time process Data Base, centralized and unique process data history base and capability to the "Off MCR" users to reach the process data history base.

4. A computer based operator aid is an evolving entity which requires care to ensure its continuing reliability, availability and usefulness to the operators. We would like to reduce complexity and the cost of the process computers hardware and software maintenance, so we would like to train our staff to be able to maintain the new equipment by themselves.

Besides the hardware, software is playing an ever increasing role in the design, manufacture, implementation and operation of an operator aid. So our utility must be prepared to monitor the supplier during every phase of the software life-cycle too. The Plan for supervision of the particular phases of the software Life-cycle such as: study phase, design specification, design, design verification, operation and maintenance, documentation specification phase, is going to be furnished.

2. Software quality

Software quality may be defined as a degree to which the software conforms to the specified requirements and expectations of the prospective user. A software product and its quality may be described with attributes such as: accuracy, consistency, correctness, efficiency, error handling capability, integrity, portability, reliability, self-containedness, testability, usability, and similar. Every effort should be made to assess the relative importance of all the attributes when specifying software for particular application. This assessment may be achieved more easily through the use of appropriate check-lists and associated priorities. The measurement of quality of a software product will vary with the needs and priorities of the prospective user. It is therefore necessary to specify the precise requirements, including quality, at the onset of a software project, and to develop the requirements formally in a structured and controlled manner through all project phases.

3. Software life-cycle

The software life-cycle may be described as a period of time when a software product is conceived, and ends when a product is no longer available for use. It typically includes: design specification phase, design phase, design verification phase, operation and maintenance phase, and sometimes, retirement phase.

Figure 1 delineate the basic stages through which the software grows and develops from the conceptual stage through to its operation and withdrawal from use. At each of these stages, appropriate controls need to be applied to the associated activities in order that the status of the software is known and controlled and, where necessary, verified and approved. However, for any particular project the whole of the software life-cycle as shown may not apply, or it may be necessary to identify further stages.

In general it is necessary that the software life-cycle is mutually compatible with the hardware life-cycle, and they together constitute the combined system life-cycle.
Each of the software life-cycle activities should be formally defined and should have a formal conclusion, usually with a document that provides tangible evidence that the activity is completed correctly.

4. Need for software quality supervision

It has been mentioned above that is software playing an ever increasing role in design, manufacture and operation of nuclear power plants, and the potential for error and poor quality is very real. The potential for an error exists with computer software at all stages of interaction with computers and the software that runs on them.

A manufacturer of a software must follow their own quality assurance programme during software life-cycle to identify, to all concerned, a basis for the control of all activities affecting quality, and to ensure that the specified quality is achived.

On the other hand the utility which will use the software, which may directly or indirectly influence the safety of the plant, must control performance of the vendor’s quality assurance programm during every phase of the software life-cycle. For such control purposes a special guidelines, or may be even better, a software quality monitoring plan should be prepared. Our utility has started with some of these activities regardless of the fact that is our plant computer replacement project still in an early feasibility study phase.
5. NEK Software Quality Supervision Plan (SQSP)

In general we can state that all materials (hardware and software) and all work, to be performed under Plant Computer Replacement Project, shall be subject to inspection and tests. No hardware or software shall be shipped until all required inspections and tests have been made, demonstrating that the system conforms to the specifications, and the hardware and software has been approved for shipment by the Buyer. It is necessary to take care about the system quality overall and would be very convenient that the buyer has a guideline or a plan to define the monitoring activities.

This paper deals only with software quality monitoring and adequate software quality supervision for our Project. The Plan delineates the purpose and scope, and summaries all activities about the software quality from buyer's point of view. We expect that shall the final software product optimally match the software quality attributes such as: accuracy, communicativeness, consistency, efficiency, error handling capability, ergonomics, integrity, maintainability, portability, reliability, robustness, testability, understandability and usability. Another very important subject is also good and consistent documentation. So our Plan contains the following chapters:

NEK Software Quality Supervision Plan

Contents

1. Purpose
2. Reference Documents
3. Applicability of the Plan
4. Management
   4.1 Organization
   4.2 Tasks
   4.3 Responsibilities
5. Documentation
   5.1 Purpose
   5.2 Software QA Plan Documentation
   5.3 Final Software Documentation
   5.4 Vendor-furnished Manuals
6. Review and Audits
   6.1 Purpose
   6.2 Vendor's QA plan Review and Inspection
   6.3 Minimum Inspection, Review and Audit requirements
7. Testing
   7.1. Purpose
   7.2. Test plans
   7.3. Test Performance
   7.4. Test Reviews
   7.5. Test Reports
   7.6. Acceptance Testing and Certification
   7.7. Unit Design Performance Tests
   7.8. Routine Quality Control Tests
   7.9. Factory Performance Tests
   7.10. Preliminary Field Acceptance Tests
   7.11. Availability Tests
8. Check-lists
6. Conclusion

Nuclear plant process computer replacement project may last few years and a typical schedule is divided into five phases: planning, specification, evaluation and negotiation, implementation, and integration and test. A good project organization, adequate project staffing and strict quality assurance methods, from each of suppliers and utility itself, is expected. Although quality assurance is often expensive and it may appear to impact the schedule, but it has the benefit of producing good and consistent target system.

Krško Software Quality Supervision Plan represents an attempt to monitor a computer software product through its entire life-cycle.

References

1. D. Mandić, M. Smolej
Design Basis and Requirements Specification for the Pilot Project of the Process Computer Replacement in Krko NPP
NEK, July 1989

2. Improving Nuclear Power Plant Safety Through Operator Aids
IAEA - TECDOC-444
Vienna, 1987

3. Computer Systems Interface Guidelines for Nuclear Plants
NSAC/5, September 1980

4. International Atomic Energy Agency
Technical Reports Series No. 282
Manual on Quality Assurance for Computer Software Related to the Safety of Nuclear Power Plants
IAEA, Vienna 1988

5. Software Engineering Standards:

5.1 ANSI/IEEE Std 730-1984
Software Quality Assurance Plans

5.2 ANSI/IEEE Std 828-1983
Software Configuration Management Plans

5.3 ANSI/IEEE Std 829-1983
Software Test and Documentation

5.4 ANSI/IEEE Std 830-1984
Software Requirements Specification

5.5 ANSI/IEEE Std 1033-1985
IEEE Recommended Practice for Application of IEEE Std 828 to Nuclear Power Generation Stations
DEVELOPMENT OF MAN-MACHINE INTERFACE FOR THE NPP PROCESS COMPUTER SYSTEM

A. STRITAR, B. MAVKO
Jožef Stefan Institute,
Ljubljana, Yugoslavia

Abstract

Operator Working Station design of the new Process Computer System for NPP Krško is described. During normal operation the system provides the operator with detailed insight into the current plant status. In abnormal conditions the system helps the operator diagnosing the event. Hardware design is based on 80386 CPU workstations. Graphic software supports presentation of data in different ways: numerical values, changing colors, modifying shapes, etc.

INTRODUCTION

Nuclear Power Plant Krško, the only NPP in Yugoslavia, has some time ago initiated activities to replace its plant process computer system. NPP Krško is Westinghouse 664 MW, two loop PWR, put on line in early eighties. The current plant computer is an old W2500 type. It has limited features and modest man-machine interface capabilities.

Design bases for this new process computer system were defined recently by the staff. The new system should be based on multi-processor configuration, providing maximum possible level of reliability.

Three levels of computer equipment are foreseen:

- Data acquisition, the lowest level, performs analog to digital conversions, time stamping and transforms signals, into engineering units.

- Real Time Level performs extensive real time computing, data base management and man-machine interface support.

- Man-Machine Interface Level displays all necessary data needed for operation.

Reactor Engineering Division of the "J.Stefan" Institute proposed a solution for the Man-Machine Interface Level. During construction, licensing and operation of NPP Krško, extensive experience has been accumulated on safety and operational problems. In parallel, extensive computer supported safety analysis capabilities have been developed, including simplified training simulator studies and plant analyzer based on RELAP5 code.

Hardware and software design of the proposed Man-Machine Interface is described in the following paragraphs. During the design phase a special emphasis was given to the organization of Operator Interface during normal and emergency situations.
OPERATOR INTERFACE

Normal Operation

The basic goal of the Process Computer System is to provide the operator with all necessary data about the plant status in a fast, accurate and consequent manner. During emergency situations it should help him in diagnosis of the event. Since large color video display units are used as the main means of data presentation, it is very important how available display screens are organized. There are several video display unit available in the Main Control Room. One of them is reserved for the display of alarm annunciators, while the remaining units can be used for displaying of other data.

Figure 1 shows the proposed organization screens of available to operator.

Predefined and user selected tables and trends

FIG. 1. Menu organizations of the operator working station.

In the top level the general layout of the plant is displayed together with the most important data of the current plant status. The basic set presents the following parameters:

- reactor power,
- primary pressure,
- primary flow,
- average temperature of the primary coolant,
- primary subcooling,
- SG pressure,
- SG level,
- SG steam flow,
- feedwater flow,
- generator power,
- circulating water inlet temperature,
- circulating water outlet temperature.
In addition to that, the well known presentation of the key safety parameters in changing shape polygonal presentation or in bar graph presentation could be placed at the same top level.

The **second system level** has displays grouped around different systems of the plant. After carefully considering the plant design, it was decided to organize screens in the following groups:

1. RCS - Reactor Coolant System
2. BOP - Balance of Plant
3. AUX - Other non-safety supporting systems
4. EL - Electrical systems
5. ESF - Engineering Safety Features
6. Other - Miscellaneous additional functions.

Each of these six screens shows the introductory overview display with essential data of systems covered by this group (example on figure 3). For example, the RCS display shows the following data:

- reactor power,
- temperatures of the hot and cold legs,
- primary flows,
- pressure, level and temperature in the pressurizer,
- steam and feedwater flow, pressure, level and temperature of SG.

![Operator working station configuration](image)

**FIG. 2.** Operator working station configuration.
This idea is straightforward for RCS and BOP systems, while for other four, which are more diverse, a more general display about the status of different subsystems should be displayed.

The third subsystem level contains screens with detailed drawings of each system and components. The number of screens depends on the number of systems and the detail required from each display. As an example, the screen with the display of pressurizer system should contain a schematic drawing with the numerical display of all the measured parameters: 4 pressure channels, 4 level channels, all temperature measurements, valve positions etc.

At the same level are placed additional displays, which do not represent hydraulic or electrical flow schematics, but are otherwise important for the normal operation of the plant. This
includes most of the graphically depicted LCOs from Technical Specifications (ie. PT diagram, core safety limits, AFD diagram), for which the current computer system does not provide any kind of on-line support.

The fourth subsystem level enables operator to display the current plant status and the operating history in a tabular or graphical trend form (example on figure 3). Each screen at the third level has a number of tabular or trend screens at the fourth level. Tables are divided into two sections: part of each table is predefined. Part may be designed by the operator based on his current needs. The same principal applies for trend screen. Each screen in the third level has a number of process variables available for tabular or trend display. The operator may choose among them when he is creating his personalized screen.

In addition to tables and graphical trends, there are various other additional screens available at this level, supporting operators during the operation. As an example, the required amount of water needed for the dilution is optionally calculated by the computer.

Abnormal operation

In the abnormal situation, following the reactor trip or after the alarm setpoint of selected variables has been reached, the computer system should switch automatically into abnormal mode of operation at least on one of the Video Display Units in the Main Control Room. Since the use of the fully supported expert system for emergency procedures in the nuclear power plant is still questionable, we propose only computerized support in the diagnostic part of Emergency Operating Procedures.

After the reactor trip the operator must follow the procedure E-0, which mainly contains simple checks of status of most important systems or parameters. Without any sophisticated artificial intelligence software, the computer system can provide necessary information for the operator so, that he can go through diagnosis faster. In the same way it can help him in following the subsequent EO procedures.

During transients or accidents, which require the operators to follow EOPs, the computer system will monitor critical safety functions in a graphical form pointing out abnormalities.

DESIGN OF THE OPERATOR WORKING STATION

The Operator Working Station (OWS) design is based around personal computers/workstations. The general layout is presented in the figure 2.

OWS is based on the 80386 CPU computer. It consists of CPU 80386 - 16 MHz CPU unit with 80387 numeric coprocessor, 16 MB RAM, 80 MB hard disk unit for the storage of operating system, additional graphic schematics and application software or, optional, RAM disk unit, Ethernet link to the RT CPU.

The operating system and application software of the OWS may be loaded from the Real Time System. During operation the process data are sent from Real Time System to the OWS via the Ethernet.
OWS Video Display Units are high resolution VGA compatible, 19", high refresh rate. The application software supports the use of 16 different colors.

Functional keyboard will serve the operator to communicate with the OWS. Use of any other input device like mouse or light pen, may be added later based on recommendations following additional studies of ergonomical requirements in the MCR.

There are 3 printers planned for the control room. One will be exclusively dedicated for alarms, the second will be used for logs, and the third for trend and other applications printing. The first two printers should be connected directly to the Real Time computer system, the third to the stand alone like OWS unit.

OWS Graphic Language and Tools provide means for easy creation and for maintenance of existing screens on operator VDUs. The basic set of screens is prepared by the general purpose CAD software on an IBM-PC. The standard set of symbols is available for the creation of new screens. The type of the on-line display is further prepared by the special graphic editor: the set of variables to be displayed on the screen is defined, the position of the numerical display, the change of colors, shapes and positions of different parts of picture, etc.

The application software of the OWS supports program controlled generation of graphs, charts, tables etc. An arbitrary number of drawings at the single OWS may be used. Up to 100 drawings may be stored in a RAM memory for fast access (less than 1 second for redrawing) and an arbitrary number, limited only by the hard disk size, on the hard disk subsystem of the OWS (redraw time of about 2 seconds).

The application software for OWS has the possibility to animate screen images. Breakers, switches and contacts may change their positions and color, valves may change their color according to their position, color of pipes may be changed according to the presence of the liquid or flow, tank levels may be changed, color of the media or mechanical part may be changed according to the temperature.

The OWS VDU presentation system is a combination of screen menu and functional keys driven software. At every moment the operator has an menu line at the top of the screen. Normally, the names of the screens of the second level (RCS, BOP, AUX, EL, ESF, see above) are displayed together with their function keys.

After selecting one of those function keys, additional menu appears showing available selections in the third level. The number of those is different for each of the second level systems. Similarly, the fourth level display appears when the function key is selected in the third level.

At any given moment operator has the possibility to store current screen displayed at the VDU as a disk file in the OWS. The screen is stored as a whole, static picture and current data. In addition to the above screen storage feature, the operator has the option to make a snapshot of the current database values of the observed system. For example, if he is watching the picture of Reactor Coolant Pump and chooses the function key for taking snapshot, all relevant data of that pump at that moment will be stored, even if
they were not displayed on the last picture. That snapshot can be reviewed later on the same or some other OWS, even outside the MCR. The snapshot is stored in the Real Time CPU System.

CONCLUSION

The described system which is presently going through the final design phase, offers an efficient solution for a future Man-Machine Interface in the NPP. It can serve as a basis for the further expansion defined by the operating personnel. Since reliable information about the plant status is of the prime importance, the system should be further developed and build with utmost care to assure its high quality performance. This preliminary design will experience several changes until it is finally approved. The extensive contribution of NPP operators is expected during all phases of the project.

REFERENCE

/1/ Design Basis and Requirements Specification for the Pilot Project of the Process Computer Replacement in Krško NPP, NEK, august 1989
AN EXAMPLE OF PLANT COMPUTER REPLACEMENT:
THE NEW CENTRALIZED INFORMATION PROCESSING
SYSTEM (KIT) IN THE 34 PWR 900 MW FRENCH PLANTS

M. MOULIN*, T. MESLIN**, P. MARCQ*

*Electricité de France,
  Marseille
**Electricité de France,
  Paris
  France

Abstract

The outdated design of the centralized information processing system installed on the PWR 900 MW plants since 1975 and the development of new functions for unit operation led to the system being redesigned and upgraded from 1984 onwards.

After describing the new system, the installation constraints and the different phases of software and data base development, this paper goes on to explain the organization of the setting up operations with particular emphasis on reliability.

1 - BRIEF DESCRIPTION OF THE SYSTEM

. Main functions

Whatever the state of the unit, the information processing system (KIT) affords:

. real-time operating assistance,
. a data base for post-operation analysis.

Operating assistance relies mainly on immediate and continued display of alarms for real-time monitoring of the unit and appropriate presentation of the data in the form of animated mimic boards, tables of lists.

Many additional computer processing functions are available: in-core readings, daily operating records, control assistance with simulation of load profiles, etc. All the information is kept on record for 72 hours and is filed on magnetic supports for deferred processing on other computers.
**System architecture**

The remote acquisition cabinets from the earlier configuration have been retained and the former KIT computer has been incorporated to double the acquisition level (N1). The KPS data processing computer (safety panel), installed as part of the post-TMI operations remains unchanged. Only the KIT processing computer has been added:

### Former simplified configuration

- **Level 2**
  - KIT
  - KPS
  - N1
  - Acquisition

### New simplified configuration

- **Level 2**
  - KIT
  - KPS
  - N1 Master Train A
  - N1 Stand-by Train B
  - Acquisition

Level 1, common to KIT and KPS, presents a redundant structure of acquisition and preprocessing of on-off and analog variables with the diverse electrical supplies. The level 2 KIT computer carries out the processing and the management of the new operating work stations (graphic screens, keyboard and tracker ball).

The KIT system has been developed by French manufacturers: Thomson for level 1 and Semagroup for level 2.

### 2 - INSTALLATION CONSTRAINTS

The fact that replacement will ultimately be implemented on 34 nuclear units already in service has led to additional problems which were not present on the initial installation, which took place at the same time as unit erection progressed.

These constraints were:

- trip over between the former and the new systems must take place quickly and must not perturb unit operation,
- the new system must be implemented in a relatively short time in order to have the improved data processing tool available on all units.
- the system must be capable of handling a substantial amount of data as soon as it is commissioned.

Steps were therefore taken to achieve maximum reliability of the entire system (hardware, software, data) from design to installation. Further details as to these systems are given below.
Although the use of basic software and hardware already tested by EDF and/or widely distributed limits unforeseen mishaps and guarantees reliability, special care had to be applied to the following aspects of the application software in order to limit the risks of anomalies occurring on the unit and to facilitate subsequent maintenance work.

- **Pre-execution phases**
  - Precise definition of the work conditions.

As part of the Quality Assurance programmes and the recommended stipulations of the I.A.E.A. (no.50C QA) and due to its inclusion in classes 3 and 4 in accordance with report 643 of the IEC, the designers had to meet specifications as to quality and to the documentation (development plan, QA manual, etc.).

- **Documentation structure**

In addition to the above general documents, software documentation was organised in 4 levels:

D1 : preliminary design description per functional aim,
D2 : detailed design description per organic module,
D3 : software sources,
D4 : test documents.

- **Drafting of detailed user requirements by a team representing EDF's Generation Division, EDF's Engineering and Construction Division and the designers.**

Clearly established operating aims facilitate subsequent options, such as the priority role of alarm monitoring, and attribute a dedicated monitoring screen to this function. Similarly, the multiplicity of possible displays at any given moment has led to the creation of selection channels which store a dozen or so displays which the operator can instantly call up. The response times have a major impact on structuring the data base.

The specifications for the interface between the two designers were carefully drafted to avoid any subsequent disputes and to permit each group to work independently from the other until integration.

- **Design phase**
  - EDF undertook a thorough examination of the analytical documentation "Preliminary design description per functional aim" (1200 pages).

After internal checking and approval, all the detailed specifications were sent by the designing organization to EDF. The Construction and Engineering Division was responsible for centralising comments and then communicating its observations to the designer by fax to minimize delays. The background to
any changes was stipulated in the cover page of the documents, thereby ensuring full traceability of the specifications.

- Sample checking of the quality of the 3000 pages of general and detailed documentation (level D2) and the documents associated with the software sources (level D3 - 400,000 lines).

EdF does not however take on the role of the designer for checking, particularly regarding software drafting.

- Drafting of an operating acceptance specification for the software (1300 pages) by the designer and approved by EdF.

- A procedure for preventing regression was drafted on completion of design in order to profit from competences and experience acquired throughout the project (400 manmonths) for any subsequent modifications.

Provisions for subsequent maintenance

Two EdF employees were included in the drafting team for the purpose of training them for subsequent software maintenance.

- On completion of the work, a document (limited to level 2 which was considered the most evolutive) set out the summary of computer loads (CPU, available RAM and ROM capacity, etc.). This refined the initial estimates and established the margins available for future modifications.

- Validation phase

After data processing unit and integration tests by the designers the software was validated in 3 steps:

- level 1 acceptance,
- level 2 acceptance,
- general acceptance.

This was possible on each designer’s site through the use of stimulators which generate the appropriate sequences, and level simulators which were missing in the first two phases. In particular, operations at the system limits, which cannot be reproduced easily on site, were tested. This involves maximum dimensioning of acquisition and avalanche phenomena on changes of logic measurements, and the comparison of complex calculations with those obtained using entirely different methods (in-core readings, monitoring of alternator heating, or core thermal balance, etc.). This phase also included 24 hr/24 hr endurance tests on the system and simulations of summer/winter time changeovers, etc.

With the data from the first-of-series unit prepared as described in section 4, overall validation (hardware + software + data) was then as close as possible to actual unit operating conditions.
- **Operation phase**

  . A version identification code is added to each software status distinguishing the application software, the basic software, associated material configuration. Any modification, no matter how slight, will lead to an increment in the identifier numbers. This referencing system is essential to monitor the different versions ultimately installed on the 34 units.

  . A central organisation was set up to receive the anomalies noted by the operators, to advise the designer so that any corrections might be incorporated and a new corrected version issued. Anomaly collection has been simplified by automatic generation of a "black box" which stores all the anomalies; the operator can then call them up on the console after receiving notification of a defect on the monitoring display.

4 - **DATA RELIABILITY**

In a system of this type, the quality of the data base called "Plant Unit Description" is primordial. It was therefore totally rewritten by a team consisting of operators and maintenance staff to ensure uniformity of all the displays and dialogues available to the operators of EdF plants.

Computer tools were developed for systematic checking of syntax, to facilitate data changes in accordance with a formal method close to that applied to software, and to guarantee the coherence of data between the KIT and KPS systems.

This work lasted more than two years and involved some 100 manmonths.

5 - **ORGANIZATION OF INSTALLATION**

  . The extension of this system to the units over a short time and the limited number of specialist teams involved implied that a methodology had to be developed to enable installation to take place outside periods of unit shutdown, especially as the KIT system is particularly solicited during startup and even during unit shutdown. Moreover, the need to limit the blackout time has led to the installation of an intermediary system which groups together the main functions of the former system: unavailability is then limited to the time necessary to trip data inputs between the former system and the intermediary system and then between the intermediary and the new system.

  . The actual installation is covered by special documents setting out the assembly and testing procedures so that the tasks can be scheduled and broken down into those which do not necessitate system shutdown (extension of acquisition capacities, installation of the maintenance configuration) and those executed when the intermediary system is operational. The on-site test procedures are complementary
to those carried out on the designer's site and validate system commissioning in its environment.

A period of four months between first unit installation and the subsequent installations was observed to limit the possibility of defects being repeated on several units; however, it should be noted that this simple precautionary rule has not revealed itself to be indispensable.

Training sessions are organized as soon as the system has been installed both for operators and for the persons locally responsible for maintaining the system. They are based on documentation and on operating and maintenance guidelines which themselves satisfy strict procedural rules. System operation is made easier by the presence of an on-line "operator guide". Moreover, the actual installation is preceded by the distribution of information leaflets and a film presenting the new system.

6 - INITIAL FEEDBACK

After trials and acceptance on the designers' site, which had been delayed a few months compared with the initial schedule, the first-of-series installation took place without hitches and the general introduction of this important modification is now progressing smoothly and rapidly (15 units between January and October 1989). Implementing the above approach has no doubt contributed to this and can be used as a reference for similar operations.
EXPERIMENTAL INVESTIGATIONS OF
EX-CORE POWER CONTROL SYSTEM PARAMETERS
AT NUCLEAR POWER PLANTS
WITH WWER-1000 TYPE REACTORS

V.S. ZHERNOV, V.B. ZVEZDOCHKINA, A.N. KAMISHAN,
A.R. KOSTIZTIN, A.M. LUZNOV, V.H. MESHKOv,
V.V. MOROZOV, Yu.B. PROHOROV, S.G. ZTIPIN
R&D Institute of Instrumentation Engineering,
Union of Soviet Socialist Republics

Abstract

The ex-core instrumentation system (ECIS) mock-up for monitoring the energy distribution over the core volume is described. The experimental investigation of the ECIS mock-up at the running NPP with the use of a representative amount of the reactor conditions has shown the high accuracy and quick response of the ex-core control method of the power and its distribution in the core volume. The small amount of the detectors, the application of the fast algorithms for signal processing make it possible to control the power distribution in the real time. The algorithms for processing detector readings and the results of the tests are also produced.

I. INTRODUCTION

A new approach to a reactor as an object under control with distributed parameters has been caused by the increased single capability of NPP units, by the enlarged cores of WWER reactors, and the higher specific loads in the core. Therefore a great attention has been paid recently to the modification of the ex-core instrumentation systems (ECIS) which permit to control the energy distribution over the core volume.

Neutron detectors located outside the pressure vessel are the base of the ECIS. The small amount of the detectors, the application of the fast algorithms for signal processing make it possible to control the power distribution in the real time. The arrangement of the detectors outside the reactor makes them more reliable and easy for replacement and repair. Due to this
the ex-core systems may be used in the future for the emergency protection, the power regulation and the automatic unloading of the reactor.

The experimental results of the parameters of the ex-core instrumentation system mock-up at the 5th unit of the Novovornezhskaya NPP with WWER-1000 reactor are given in the report.

The aim of the investigations has been to check on the running reactor if the conceptions and principles the system based on are correct, that is:

- to check if the appropriate number and the arrangement of the detectors have been selected;
- to check the mathematical model;
- to exercise the algorithms and programs for the computers;
- to estimate the errors of the values under control.

To save the time and means in achieving the set aim the use was made of the equipment and the computer facilities available on the NPP for the development of a system mock-up.

II. THE HARDWARE COMPONENTS OF THE ECIS MOCK-UP

The assemblies of the ionization chambers were mounted in the vertical channels No. 5, 12, 19 (fig. 1), made within the biological shield of the reactor. Every assembly consists of three gamm background compensated ionization fission chambers spaced 1 m from each other in height (fig. 2).

The cables from the ionization chambers are brought out of the containment to three current-to-frequency converters. Frequency signals are applied over long communication lines to the input of a device which matches these signals with the input of the device (CNCD) intended for the commutation, normalization and conversion of the signals from the information complex CD.
FIG. 1.

IC channel No.

- Sensors of ICIS
- Control rods group no. 8
- Control rods group no. 13
- Control rods group no. 14

FIG. 2.
The information complex CD serves as a communication device for the object. The information is applied from CD to the working memory buffer of the two-processor computer. The information on the thermal power of the reactor, determined by thermal and physical methods, on the position of the groups of the control rods CR (OP) of the safety control system SCS (CY3) and from the in-core instrumentation system ICIS (C8PK) concerning the power distribution over the entire volume of the core also goes into the computer.

III. THE MATHEMATICAL MODEL

The algorithm for processing signals from detectors in ECIS is based on a mathematical model of the connection of separate detector readings with the power distribution in the core. On the one hand, the model shall take into account all the main effects in order to provide the minimum error of the power distribution characteristics under test; on the other hand, it shall permit to construct unlaboured algorithms for processing detector signals, otherwise the main advantage of the ECIS, i.e. speed of response, will be lost.

The point of the mathematical model developed by the authors and used to construct the algorithm is that the problem of connecting the detector readings with the power distribution in the core is divided into subproblems. The first subproblem is to determine the characteristics of the neutron source, formed on the external surface of the vessel at a certain power distribution over the core volume, the second one is to connect the readings of the detector to the characteristics of this surface source.

The advantage, of this approach is that the formation behaviour of a surface source may be revealed only by the calcu-
lation because in this case the geometry is two dimensional, all
the sizes and the contents of materials are well known. The second
subproblem, i.e. to find the connection between the detector
readings and the characteristics of the surface source, may be
solved by means of an experimental surface weight function of
the detector. This function depends only on one space coordinate,
it acquires the features of the anisotropy and spectral sensiti-
vity of the detector, as well as all the properties of the shield,
which separate the surface of the reactor vessel and the
detector. The surface weight function does not depend on the
boric acid concentration, the coolant temperature, the position
of the control rods of the safety control system, the burn-up,
i.e. does not depend on the current condition of the core.
Therefore this function once found experimentally, for example,
at the beginning of the life may be used in the monitoring algo-
rithms during the whole life or even during several lifetimes.
Surface weight functions of the detectors are determined in the
course of the calibration of the ex-core system.

IV. ALGORITHMS FOR PROCESSING DETECTOR READINGS

Without the use of the preset behaviour of the power dis-
tribution formation it would be impossible to obtain the charac-
teristics of the three-dimensional power distribution with a
required practical accuracy by means of the readings of a small
number of detectors placed outside the reactor.

The relation between the radial component of the power
distribution and the position of the groups of the SCS control
rods is such an a priori information for modern algorithms,
which define the rule for the calculation of the power distri-
bution characteristics according to the readings of the ECIS
detectors. An algorithm given below and developed on the base
of the model (described in Section III) of the relation between the readings of the ex-core detector and the power distribution in the core is not an exception.

The algorithm may be divided into 10 steps. The steps 1 - 5 are performed 3 times (according to the number of Assemblies), i.e. detector signals of every assembly are processed sequentially. The steps 6 - 10 generalized the information, obtained from all the assemblies.

1. The calculation of a coefficient of the expansion into a series of the neutron flux density distribution in height on the external surface of the reactor vessel (on an azimuth of the assembly installation):

\[ [A(i)] = [S(i)] \cdot [D(i)] \]

\[ (3,1) \quad (3,3) \quad (3,1) \]

Where:
- \( i \) - is an index of the detector assembly \( i = 1, 3 \);
- \([A(i)]\) - is coefficients of expansion into a series
- \([S(i)]\) - is a matrix, determined during the calibration of detectors
- \([D(i)]\) - are the readings of the detectors of the \( i \)-th assembly.

2. Calculation of a neutron flux density value on an azimuth of the \( i \)-th assembly installation in 10 points on the vessel \( (Z_k; K=1,10) \) distributed uniformly along the core height by means of the found coefficient:

\[ \Phi_k(i) = \sum_{m=1}^{5} A_m(i) \sin \left( m \times \frac{Z_k + \frac{H}{2}}{H} \right); \quad k = 1,10 \]

Where \( H \) - is the core height;
- \( A_m(i) \) - are elements of the matrix \([A(i)]\)
3. Calculation of the power distribution along the core height in 10 point ($Z_k; k=1.10$) by means of the detector readings of the i-th assembly:

$$F_k(i) = C_k \Phi_k(i)$$

The coefficients $\{C_k; k=1.10\}$, used to realize a transition from the height distribution of the neutron flux density on the containment to the power distribution along the core height depend on the position of the groups of SCS control rods. These coefficients for various positions of the groups have been determined before with the application of the calculation programs of the neutron and physical characteristics of the core (of BIPR type) and of two-dimensional (one dimensional) programs of the shield calculation (of DOT, ANISN type).

4. Calculation of a reactor thermal power by means of the detector readings of the i-th assembly:

$$W(i) = \left( \frac{H}{\text{th}} \right) \sum_{k=1}^{10} F_k(i)$$

5. Calculation of the power distribution in core height normalized to unity by means of the detector readings of the i-th assembly:

$$\hat{F}_k(i) = F_k(i)/W(i); \quad \kappa = i,10$$

6. Calculation of the reactor thermal power as a mean value by means of values obtained from individual assemblies:

$$W = \left( \frac{1}{3} \right) \sum_{i=1}^{3} W(i)$$

7. Calculation of an average power distribution over all assemblies in the core height:

$$\hat{F} = \left( \frac{1}{3} \right) \sum_{i=1}^{3} \hat{F}_k(i); \quad \kappa = i,10$$
8. Calculation of an axial off-set (AO), which is equal to the difference of the upper and lower areas of the core referenced to the full power:

\[ AO = \left( \frac{H}{10} \right) \left( \sum_{k=1}^{10} \hat{O}_{k} - \sum_{k=1}^{10} \hat{O}_{k} \right) \]

9. Calculation of a coefficient of the non-uniformity in height:

\[ K_z = H \cdot \max_{k=1,10} \hat{p}_k \]

10. Calculation of a coefficient of the nonuniformity in volume:

\[ K_v = H \cdot \max_{k=1,10} \left( \hat{p}_k \cdot C_k \right) \]

Where \( (C_k^i; k=1,10) \) are coefficients of the power distribution nonuniformity in 10 cross-sections \((Z_k; k=1,10)\). These coefficients depend on the position of the groups of SCS control rods and are numbers beforehand for various positions by means of the BIPR programs.

Note that a priori information on the known formation behaviour of the power distribution is concentrated in the coefficient files \( \{C\}, \{C^i\} \)

V. CALIBRATION

The aim of the calibration is to determine the i-th matrix \([S(i)]\) for every assembly used in the main algorithm. Let us specify the sense of the matrix elements \([S(i)]\). According to the model, if \( \Phi(Z,t) \) is a neutron flux density distribution in height on the detector installation azimuth at the time moment
t, and $T(Z)$ is a surface weight function of the detectors, then the detector reading $D(t)$ may be represented as:

$$D(t) = \int_{0}^{H} \Phi(Z,t) T(Z) dZ$$

(1)

Where $H$ is a core height.

Let us assume, that the distribution in height $\Phi(Z,t)$ may be given with a sufficient accuracy as a series:

$$\Phi(Z,t) = \sum_{n=0}^{N} a_n(t) \sin \left( \frac{n\pi Z}{H} \right)$$

(2)

Substituting (1) by (2), we obtain:

$$D(t) = \sum_{n=0}^{N} a_n(t) \int_{0}^{H} T(z) \sin \left( \frac{n\pi Z}{H} \right) dZ$$

(3)

The integrals from (3) are the matrix $[S(i)]$ elements. For example, if the $i$-th assembly contains three detectors and the surface weight functions of these detectors are denoted as $T_1(Z), T_2(Z), T_3(Z)$, then the matrix $[S(i)]$ has the dimension $3 \times 3$ and

$$S_{mn} = \int_{0}^{H} T_m(Z) \sin \left( \frac{n\pi Z}{H} \right) dZ$$

Thus the elements of the matrix $[S(i)]$ are the integral convolutions of harmonics with surface weight functions involved into the $i$-th assembly of the detectors.

The calibration may be divided into three main stages:

1. The realization of several conditions of the reactor which differ in the form from the power distribution in the core height that is achieved by the displacement of the groups of SCS control rods. The number of these conditions must be not less than the number of detectors in an individual assembly. The reactor conditions with the power distributions in height, given in fig. 3, have been used for the calibration of the mock-up.
2. Recording of the reactor thermal power, determined by thermal and physical methods, of the relative power distribution in the core height (information from ICIS), of the position of the groups of SCS control rods, and of the readings of all the ex-core detectors in each of these conditions.
The recording means the selection of the values of the pointed out parameters and the magnetic tape or disk recording.

3. Processing of the records on the magnetic carriers with the application of a calibration program included into the software, of the mock-up. The calculation and magnetic disk recording of the \([S(i)]\) matrices for the further use in the mock-up programs, which implement the basic parameter controlling algorithm, described above.

After the calibration, which is carried out at the beginning of the life and takes 10-15 hours, the ex-core system becomes completely independent of the other control systems. It determines the reactor power and its distribution in the core volume only according to the readings of the ex-core detectors and the pick-ups of SCS control rod positions.

VI. TEST RESULTS

The ECIS mock-up has been tested at a power of 50% level of the rated one. The tests were aimed at setting up a correspondence of the readings of ECIS and ICIS under the reactor conditions with considerably different form of the power distribution both in height and radially.

The thermal power, its distribution in height in 10 points, the axial off-set, the coefficients of the nonuniformity in height and volume have been calculated with the use of the mock-up program in every reactor condition according to the position of the groups of the SCS control rods and the readings of the ex-core detectors. The obtained values and the values of the same parameters, determined by means of the routine methods (thermal and physical measurements of the power, ICIS) have been recorded on the magnetic tape for every reactor condition.
Thus for 55 hours of the tests more than 600 reactor conditions were recorded.

The power distribution in the core volume varied depending on the position of the SCS CR groups no 5,13 and 14 (the first 29 hours) and in the course of free xenon oscillations (the rest 26 hours).

The graph of the displacement of the SCS CR groups during the tests is given in fig. 4a. The values of the reactor thermal power, obtained by thermal and physical measurements and by means of the mock-up are given in fig. 4b. The graphs of the variations of the axial off-set and the coefficient of the nonuniformity in volume, obtained by the measurements of the mock-up and ICIS are given in fig. 4c,d.
Several typical power distributions in height obtained during tests and taken by the readings of the ex-core in-core systems are given in fig. 5.

After the termination of the tests the values of ones and the same parameters obtained with the use of different systems were compared statistically. For this purpose all the information accumulated on the magnetic tape during the tests, containing the values of these parameters in more than 600 different conditions of the reactor, was processed by means of a specially developed
program. The results of the statistical comparison are given below. The difference of the compared values is characterized by two numbers, the first one is a mean relative disagreement in percents, and the second one is a standard deviation from this mean value.

The thermal power:

The disagreement between the mock-up and the thermal and physical methods - 
\( (0.03 \pm 1.71)\% \)

The ratio of the power of the upper part of the core to that of the lower part:

The disagreement between the mock-up and ICIS - 
\( (0.03 \pm 2.46)\% \)

The coefficient of the nonuniformity in volume:

The disagreement between the mock-up and ICIS - 
\( (-2.50 \pm 4.62)\% \)

VII. CONCLUSION

The test of the power ex-core instrumentation system mock-up with the use of a representative amount of the reactor conditions has shown the high accuracy and quick response of the ex-core control method of the power and its distribution in the core volume. The ECIS assemblies may be placed in the channels of the biological shield on the WWER, three assemblies being sufficient, each of which contains three detectors.

In the case, if the algorithms for processing detector readings are developed on the base of a model, which allows for the effect of the form of the radial-azimuthal power distribution upon these readings, then the amount of power distributions in height required for the calibration may be realized not in the
course of the xenon oscillations, as it is usually made, but by the displacement of the SCS CR groups. In the result, the time of calibration is reduced by 15-20 hours, i.e. the operation of the unit at the lower power (the calibration is carried out at a power of 50-75%) is reduced.

The determination of the thermal power and the coefficient of its distribution in the core do not exhaust all the possibilities of the ex-core control. At present, algorithms are available or under development which permit to improve the accuracy of the power and its distribution control, to localize an area or a cassette with higher energy density to locate the stuck CR and failed pick-ups of the thermal control, to make a diagnosis of the oscillations and displacements of the in-vessel constructions of the reactor. Thus, a reliable, cheap, system with response allowing to improve the technical and economical indices of NPP, to make it more safe in operation may be constructed on the base of the ex-core detectors.
PROBABILISTIC TECHNIQUES FOR
SOFTWARE VERIFICATION

W.D. EHRENBERGER
Fachbereich Angewandte Informatik und Mathematik,
Fachhochschule Fulda,
Fulda, Federal Republic of Germany

Abstract

The various techniques for verification of proper software behaviour can be separated into probabilistic and deterministic ones. Deterministic techniques mainly qualify for small programs with very high reliability requirements. The probabilistic ones qualify for large programs in the first place. They are mostly based on operating experience and on black box testing; the aspects of software behaviour are dominating in contrast to the questions of its correctness. The outcome of the related investigations is typically a reliability figure and a related level of confidence.

This contribution gives some formulae that may be used as rules of thumb. In any particular licensing process, however, things most likely will get so complex that more detailed techniques such as two stage sampling may become important. In these cases it is advisable to engage specialists about probabilistic, because the mathematical complexity of the problem may exceed the scope needed in "normal" engineering.

1. Reason for application

In many cases the software packages are too complex for systematic verification. The related proving techniques e.g. require too much effort as to remain viable methods for getting useful results for any licensing process. In particular do the related logical expressions become so large that no understanding of their meaning is feasible and consequently no statement about software correctness can be made. Similar problems may come up with software analysis, where the aim is to find out and subsequently execute those test cases that test the software exhaustively.

On the other hand in many cases we do not require absolute correctness of the related software package. Our reliability aims may be a bit more modest. It may be sufficient for our software to

- be just better than a conventional system that is to be replaced by our computer system. Or
- to be sure that the risk that is connected to the operation of the software stays below a certain limit. Or it may be enough that the software part is
- not the weakest link in a chain of several subsystems.

Sometimes probabilistic thinking is confronted with a certain suspicion. It is thought that it may not be accurate enough and that it may not fit into exact engineering thinking. Both aspects are only partially true. Inexactness mostly comes up, if either
some of the prerequisites for the application of the related mathematical relationships are not fulfilled or if one has not taken the effort of calculating variances in addition to expected values. In conventional engineering practice probabilistic approaches are used mostly intuitively: in connection with operating experience. Such experience plays a very important role. If somebody has to take over a new item and performs an acceptance test of main functions only, his thinking is also probabilistic to a certain degree: He either believes that the yet untested functions of the item would be performed correctly in the same way as the main functions are; or he thinks that his purposes are fulfilled to a sufficient degree, if the important functions are all right; or both types of considerations may be applied.

In the following chapters we are discussing some basic aspects of probabilistic testing in connection with licensing of nuclear power stations. The focus is on practical applicability and not on mathematical background. The reader should be enabled to judge, if probabilistic techniques would make his particular licensing process easier. The mathematical basis is taken from the related books on statistics /1,2/, or similar ones. All those, who intend to make practical use of the described techniques should refer to the mathematical sources first.

Chapter 2 treats testing of software behaviour. After that, chapter 3 deals with testing software for its correctness. Then software reliability models are shortly dealt with. In chapter 5 we are considering particular problems with applications notably a mixture of probabilistic and deterministic techniques. Considerations on two stage sampling conclude the technical part of this paper.

2. Test of Program - Behaviour

2.1 The probabilistic process and the different types of programs

Sometimes an argument against probabilistic considerations on software is that a failure process similar to the failing of hardware components does not exist. Software faults, it is said, are deterministic by nature after software delivery and they cause program failures deterministically, if they are encountered; therefore the use of probabilistic thinking is not allowed.

Such arguments neglect that probabilistic thinking is always possible, if something comes into play whose outcome is not known in advance; more precisely, if an item "probability" can be defined that follows the related mathematical axioms. Regarding software it is the event of finding faults that cannot be foreseen. The following considerations take the process of encountering possibly existing program faults during operation or test as the underlying probabilistic process.

Normally we may distinguish between programs that operate on demands and programs that operate continuously. An example of the first type of software is a - reactor protection program.
A representative of the second type is an - operating system.
Programs operating on demands react on specific situations in the
first place. By contrast continuously working programs are more or less always in operation. Any practical software system contains aspects of both types of behaviour.

2.2 Programs operating on demands

For reasons of clarity, we are focussing on demand driven software only in this subchapter. A demand can be understood as a change of input data that could possibly result in a change of program output. In order to be able to come to simple formulae we have to put some prerequisites on program behaviour and test design.

Assumptions

1. Sequence and number of test runs do not influence the result of a single test run. (Independency of test runs.)

2. Each input data combination is tested with the same probability, as used during real operation. (Test is a true reflection of the operating conditions.)

3. Each occurring failure is detected. (Test is monitored completely.)

4. The number n of test cases is large, e.g. \( n > 1000 \).

5. Failures are rare.

Starting from these assumptions we are able to show that the failure probability per demand is distributed binomially or according to the Poisson distribution. With that, we are able to make statements about the number of test cases n, the failure probability per demand \( p \) and a related level of confidence \( \alpha \): If the hypothesis

\[ p \leq \left( p = 10^{-k} \right) \]

shall be true with \( \alpha \),

the number of necessary test runs is

\[ n = 3 \cdot 10^k \quad \text{if } \alpha = 95\% \quad \text{and} \]

\[ n = 4.6 \cdot 10^k \quad \text{if } \alpha = 99\% . \]

This is true under the assumption that no failure has occurred during the \( n \) test cases. Should any failure come up, the test would be stopped, the underlying fault searched for and removed and another test started again. In most practical cases it is too costly to proceed with testing, if any failure has been encountered, as more detailed considerations show. For details see /3/.

An example to that is:
if operational considerations require \( p \leq 10^{-4} \) and \( \alpha = 99 \% \),
we need at least \( n = 4.6 \cdot 10^4 \) test cases.

The test cases need not be performed on one site or test harness only. They may be executed on different places in parallel. Operating experience from other sites or from preliminary operation may be included into any calculation. The only prerequisites are the above mentioned assumptions. If they are not fulfilled, more complex formulae apply.
2.3 Programs operating continuously

The time dependent input data process is considered as the random process. The following considerations are similar to those about hardware failure due to change of physical properties. We consider failures during time intervals instead of per demand.

Assumptions

1. The relative reduction of the probability of no failure is constant and proportional to the length of the considered time interval.
2. The operational profile is known and the testing profile is the same as the operational profile.
3. Each occurring failure is detected.
4. Failures are rare; or no failures occur at all.

The test time \( T \) until the occurrence of a program failure is a random variable and has an exponential distribution with a constant parameter \( \lambda \). \( \alpha \) is again the level of confidence. The test consists in a simulation of the operational process.

The probability distribution \( F_r(t) \) of the time to the next failure is given by the following figure and formula.

\[
F_r(t) = \rho(T \leq t) = 1 - e^{-\lambda t} \quad \text{prob. of no failure in } [0,t]
\]

Figure 1: Probability distribution of program failure

We are searching for a relationship between \( \lambda \), \( \alpha \) and the required test time \( t_\alpha \). The hypothesis

\[
\lambda \leq \bar{\lambda} \quad \text{shall be true with } \alpha.
\]

After some calculations it is found:

\[
\bar{\lambda} = -\ln (1 - \alpha) \quad \text{or} \quad t_\alpha = \frac{-\ln (1 - \alpha)}{\lambda}
\]

In other words: test time \( t_\alpha = 3/\bar{\lambda} \), if \( \alpha = 95\% \)

\( = 4.6/\bar{\lambda} \), if \( \alpha = 99\% \).

For details see /4/.
Example: The operating system of the control rod moving computers of the German boiling water reactor plants had to be investigated. Firstly systematic verification was tried. It turned out that some parts were analysable, namely the quasi instructions, the parts for digital I/O and the operating system entry. There was, however, no way to understand the central part of the system, i.e. the processor management. Therefore probabilistic methods were tried. Operating experience from several sites showed that the failure rate of the operating system was below $10^{-3}$ per hour. In detail:

\[ \lambda \leq 5.91 \times 10^{-6} \quad \text{with } \alpha = 95\% \]

This turned out to be sufficient for the purpose of the system. See /5/.

2.4 Considering the input domain

The possibility to test a program as a black box with respect to its input domain may be another question of interest; in particular, if the computer has to process analog signals.

Assumption

The test consists in selecting each input point with equal probability.

The mean distance between such arbitrarily chosen test points is important, because it informs about the accuracy of the test with respect to the input domain. This distance depends on the dimension of the input domain and on the number of test points. The following table gives an overview over these distances in direction of an axis of the assumed Cartesian coordinate system. The size of the input space is considered 1 in each direction.

<table>
<thead>
<tr>
<th>dimension</th>
<th>mean distance of two test points in direction of an arbitrary axis</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\delta = 1/n$</td>
</tr>
<tr>
<td>2</td>
<td>$\delta = \sqrt{1/n}$</td>
</tr>
<tr>
<td>3</td>
<td>$\delta = \sqrt{1/n}$</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>.</td>
<td>.</td>
</tr>
<tr>
<td>k</td>
<td>$\delta = k\sqrt{1/n}$</td>
</tr>
</tbody>
</table>

E.g.: If $n = 1000$ test cases; $k = 3$, corresponding to a three dimensional input domain : $\delta = \sqrt[3]{1/1000} = 1/10$ is the mean distance in direction of an arbitrary axis. I.e. if the related problem requires a more accurate treatment of the input space than 10%, the test is insufficient.
As we see, if \( k \) is large, the accuracy of the test is very limited. Such type of testing is only useful for small \( k \). The size of \( k \) must be shown analytically. It means the number of analog input variables that are treated together.

Before we leaving this subchapter, we have to point out that the actual mean distances between test points are larger than \( \delta \). They are in fact:

\[
\delta_{\text{actual}} = \sqrt{k \delta^2} = \delta \sqrt{k}
\]

### 3. Test for Finding Faults

The next question to be considered is about the possibility to find faults in a program through statistical testing. In this case the test is to be based on program properties and not on program behaviour. The probabilistic process is the selection of the program properties during the test. The assumptions to be made are similar to those of the subchapter 9.1. Number 2 is replaced by:

**Assumptions**

2a. The probability of being selected during the test is equal for each program property and it is independent from the selection probabilities of all other program properties.

2b. The program may be considered as an urn and the program properties as balls in that urn.

2c. The number of balls is estimated to be \( N \); however, no knowledge about their location in the urn is available.

Each test case coresponds to drawing a ball, investigating it about being black (with fault) or white (without fault) and replacing it. The probability of a complete test then is the probability to touch each ball or to investigate each program property.

Calculations give a relationship between the probability \( p_e \) of having all necessary test cases executed, the number \( N \) of such necessary cases and the actual number \( n \) of test runs. Certainly \( n \gg N \) is needed.

\[
p_e = \sum_{j=0}^{N-1} \binom{N}{j} (-1)^j \binom{n-j}{N} = 1 - N \frac{(N-1)^6}{N} + \binom{N}{2} \frac{(N-2)^6}{N} - \ldots +
\]

A result of that formula is given in the following table 2. We assume that our program would be tested completely with 4000 test runs, if it were known which ones were to be executed. The table gives values for particular pairs of \( n \) and \( p_e \). For details see 79/.
Table 2: Relationship between the number of test cases $n$ and the probability $p_e$ of a complete test, if $N = 4000$ test runs could perform an exhaustive test; requirement: each of the 4000 necessary cases is selected with equal probability.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$p_e$</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 000</td>
<td>$1 - 1,49 \cdot 10^{-2} + 1,10 \cdot 10^{-4}$</td>
</tr>
<tr>
<td>75 000</td>
<td>$1 - 2,87 \cdot 10^{-3} + 4 \cdot 10^{-15}$</td>
</tr>
<tr>
<td>100 000</td>
<td>$1 - 5,54 \cdot 10^{-8} + 1,52 \cdot 10^{-15}$</td>
</tr>
<tr>
<td>200 000</td>
<td>$1 - 7,76 \cdot 10^{-19} + 2,9 \cdot 10^{-27}$</td>
</tr>
</tbody>
</table>

The requirement of equal probability of selection of each test case cannot be met in practical cases. Therefore the formula should be applied for the rarely encountered cases only; the $\{n\}$ should consist of that subset of cases only which hold the requirement of equally selecting from the $\{N\}$.

4. Reliability Growth

Now the supervision of the fault removal process at the end of program development is considered. Conclusions are made on the basis of the reduction of the failures observed per test run or per time unit during software system integration testing. Curves of the shape shown in Fig.2 may come up: the mean time between failure (MTBF) or the mean time to failure (MTTF) increases as the failure rate $\lambda$ decreases.

![Figure 2: Changes of removed faults per time unit or per a certain number of test runs, still remaining faults $M$, and mean time to failure (MTTF) or mean time between failures (MTBF) during the debugging phase of a software package - qualitatively](image-url)
Several mathematical models exist that allow to estimate the remaining failure probabilities according to subchapter 2.2 or the remaining faults in the program. See e.g. /6/. The simplest relationship is that from Jelinski and Moranda /7/, which says that

\[ \lambda = \frac{1}{\text{MTBF}} = \text{const} \left( M_{\text{init}} - M_{\text{removed}} \right) \]

Experience has shown, however, that the estimates are not very accurate. For safety purposes such models therefore should be used as the sole verification means only if the required reliability is not very high.

5. Mixture of Systematic and Probabilistic Verification Techniques

In many applications one will be faced with software that has been treated by systematic verification techniques already in some of its parts. The related functions can then be regarded as being always executed correctly. Probabilistic methods will be applied to such functions only whose correctness has not been demonstrated yet. The necessary test effort can then be calculated according to the required overall reliability figures. Figure 3 depicts an example in more detail. Four strata are assumed. The possible damage is considered equal in all cases of failure in any stratum. (If this were not the case, we would chose the size of our strata according to the product of frequency of demand and damage in case of failure.)

![Figure 3: Stratification of input cases](image)

Stratum 1 called with frequency \( f_1 \) during operation:
- trip via one safety parameter, others in normal positions

Stratum 2, frequency \( f_2 \):
- trip via one safety parameter, others in disorder

Stratum 3, frequency \( f_3 \):
- two other
- others in disorder

Stratum 4, frequency \( f_4 \):
- other

The example of figure 3 is taken from reactor safety. It is assumed that the correct execution of all single trip functions has been shown by systematic means. So the related failure probability is zero:

\[ P_{\text{sys part}} = P_{f_1} = 0. \]

The other cases shall be verified probabilistically. The consideration shall lead to an overall failure probability per demand

\[ P_{\text{total}} \leq P, \text{ true with the confidence level } \alpha = x \% \]
Based on subchapter 2.1 we are aiming at some
\[ p_{\text{tested part}} \leq \tilde{p}_i \quad \text{with} \quad \alpha = x \% \]

The result of the total verification effort will be
\[ p_{\text{total}} = \text{Some function} \left( p_{\text{yst part}} + p_{\text{tested part}} \right) \]
\[ = p_{\text{yst part}} \cdot \frac{f_1}{\sum f_1} + p_{\text{tested part}} \cdot \frac{f_2 + f_3 + f_4}{\sum f_1} \leq \tilde{p}, \quad \text{with} \quad \alpha = x \% \]
\[ p_{\text{total}} = 0 + p_{\text{tested part}} \frac{f_2 + f_3 + f_4}{\sum f_1} \leq \tilde{p}, \quad \text{with} \quad \alpha = x \% \]

\[ i \in \{1, 2, 3, 4\} \]

From that the necessary test cases in the individual strata \( n_2, n_3, n_4 \) can be calculated on the basis of the relationships of chapter 2.2 or 2.3.

In the ideal case the number of test runs will be chosen proportionally to the height of the individual strata according to figure 3. Test data selection will be such that each case of the selected strata will have equal chances of being selected.

However, due to technical reasons the test harness may be such that it is too costly to provide all input cases or sequences with the required probability. In this case we may turn to a two stage sampling process.

6. Two stage sampling

In the case of two stage sampling each case has also a known probability of being selected during the whole test, as it is the case with simple sampling. The selection procedure of test cases is different to the aspects treated so far, however: the test selects clusters first and input conditions in these clusters second.

The related mathematics is not very difficult as far as expected values are concerned. For this purpose the test results just have to be extrapolated under consideration of the selection procedure. The formula for the variance, however, is quite complex. This relationship is needed, if the number of necessary test cases is to be evaluated for any practical problem. In /8/ the related formula has been derived. It has been applied to testing of computer behaviour in /3/. The essence is the need of some additional testing effort in order to balance the loss of accuracy due to the two stage sampling process.

7. Conclusion

Probabilistic verification efforts should be used complementarily to systematic approaches; in particular, if no program analysis is feasible on which exhaustive testing could be based. Probabilistic testing is usually very expensive due to the large number of required test cases. It is facilitated, if a test harness exists that makes it easy to apply the test input conditions and to monitor the output of the test object. Random number generation may be required if the numbers of test cases get large.
Probabilistic verification is quite economically to apply if the reliability requirements are small or if one can make use of operating experience. In this second case also high reliability requirements can be fulfilled through probabilistic considerations with modest effort. Probabilistic thinking is more or less indispensable, if the reliability properties of diverse structures shall be demonstrated.

Usually design and evaluation of the results of a probabilistic test requires considerable knowledge about probability theory.

References

/1/ J.Heinhold und K.W.Gaede
Ingenieurstatistik
Oldenbourgverlag München und Wien

/2/ B.W.Gnedenko
Wahrscheinlichkeitsrechung
Akademie Verlag Berlin

/3/ W.Ehrenberger und K.P.Plögert
Einsatz statistischer Methoden zur Gewinnung von Zuverlässigkeitskenngrößen von Prozeßrechnerprogrammen
Bericht KFK-PDV 151, Juni 1978, to be received from the author

/4/ W.Ehrenberger und B.Krzykacz
Probabilistic Testing

Reliability Evaluation of a Safety Related Operating System
in Proceedings of SAFECOMP 85, Pergamon Press

/6/ B.Littlewood
Assessment of Software Reliability
in: Proceedings of the CSR Workshop on Software Reliability - Achievement and Assessment, University of Keele, April 1985, to be ordered from The Centre of Software Reliability, The City University London

/7/ Z.Jelinski and P.B.Moranda
Software Reliability Research
in: Statistical Computer Performance Evaluation
Academic Press New York, 1972

/8/ H.Stenger
Stichprobentheorie
Physika Verlag Würzburg und Wien

/9/ W.J.Quirk
Verification and Validation of Real Time Software
Springer Verlag Heidelberg, 1985
<table>
<thead>
<tr>
<th>Country</th>
<th>Name</th>
<th>Organization/Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argentina</td>
<td>Mr. Touzet</td>
<td>CNEA, Echeverria 2296 2º &quot;A&quot; 1428 Buenos Aires, Argentina</td>
</tr>
<tr>
<td>Belgium</td>
<td>Mr. De Feu</td>
<td>Département Sûreté Nucléaire, Association Vincotte, Avenue du Roi 157, B-1060 Brussels, Belgium</td>
</tr>
<tr>
<td>Canada</td>
<td>Mr. G.J.K. Asmis</td>
<td>Atomic Energy Control Board A.E.C.B., P.O.Box 1046, Station &quot;B&quot;, Ottawa Canada KIP 5S9</td>
</tr>
<tr>
<td></td>
<td>Mr. W.R. Whittall</td>
<td>Atomic Energy of Canada Ltd., CANDU Operations, 2251 Speaksman Drive, Mississauga, Ontario, Canada L5K 1B2</td>
</tr>
<tr>
<td>Czechoslovakia</td>
<td>Mr. P. Krs</td>
<td>Czechoslovak Atomic Energy Commission, Slezská 9, Prague, 129 00, CSSR</td>
</tr>
<tr>
<td>Finland</td>
<td>Mr. T.T. Manninen</td>
<td>Imatran Voima Oy, P.O.Box 112, SF-01601 Vantaa, Finland</td>
</tr>
<tr>
<td>France</td>
<td>Mr. J.F. Aschenbrenner</td>
<td>Electricité de France (EDF), 12-14, avenue Dutriévoz, 69628-Villeurbanne CEDEX, France</td>
</tr>
<tr>
<td></td>
<td>Mr. J. Boulch</td>
<td>Institut de protection et de sûreté nucléaire, CEN Fontenay-aux-Roses, BP NO. 6, 92265 Fontenay-aux-Roses Cedex, France</td>
</tr>
<tr>
<td></td>
<td>Mr. Ph. Marq</td>
<td>Service Electricité, Region d'équipement alpes Marseille, 140, ave. Viton, B.P. 560, 13401 Marseille Cedex 9, France</td>
</tr>
</tbody>
</table>
GERMANY
Mr. Hampel
Technische Hochschule Zittau
Theodor Körner Allee 16
Zittau, DDR-8800

INDIA
Mr. G. Govindarajan
Reactor Control Division
Bhabha Atomic Research Centre
Bomby - 85
India 400085

ISRAEL
Mr. S. Carmona
Soreq Nuclear Research Center IAEC
Yavne 76060
Israel

Mr. David Segal
Israel Atomic Energy Commission
P.O.Box 7061
Tel-Aviv 61070
Israel

POLAND
Mr. A. Mikulski
Institute of Atomic Energy
Department E-4
05-400 Otwock-Swierk
Poland

SPAIN
Mr. F.A. Santos
Central Nuclear de Valdecaballeros
Goya, 4 - 28001 Madrid
Spain

SWEDEN
Mr. L. Fredlund
Swedish State Power Board
Statens Vattenfallsverk Ringhals NPP
S-43022 Väröbacka
Sweden

Mr. E.F. Larsen
Vämeteknik TVS
Sydkraft AB
Carl Gustafs Väg 4
21701 Malmö
Sweden

UNITED KINGDOM
Mr. E.F. Potter
Nuclear Installations Inspectorate
St. Peter's House
Balliol Road, Bootel
Merseyside L20 3LZ U.K.

Mr. N. Wainwright
(Chairman)
Nuclear Installations Inspectorate
Room 501, St. Peters House
Balliol Road, Bootel
Merseyside L20 3LZ U.K.
UNITED KINGDOM (cont.)
Mr. D.J. Pavey  National Power (CEGB)
              Barnwood, Glouster, U.K.

UNION OF SOVIET
SOCIALIST REPUBLICS
Mr. V. A. Eremenko  Gosatomenergonadzor
                    Science and Engineering Centre
                    for Nuclear Power Safety
                    34, Taganskaya St.
                    109147 Moscow, USSR

Mr. V. Meshkov  R&D Institute of Instrumentation
                Engineering

Mr. N.A. Sazonov  c/o USSR State Committee on
                   Utilization of Atomic Energy (SCUAE)
                   Department of International Scientific
                   & Technical Cooperation
                   109180 Moscow
                   Staromonetny pwe, 26 USSR

YUGOSLAVIA
Mr. D. Mandic  NE Krsko
              Vrbina 12, 68270 Krsko
              Yugoslavia

Mr. M. Smolej  NE Krsko
              Vrbina 12, 68270 Krsko
              Yugoslavia

Mr. A. Stritar  Inst. Jozef Stefan
               Jamova 39
               61111 Ljubljana
               Yugoslavia

SCIENTIFIC SECRETARIES
Mr. M. Dusic  NENS/SAS - IAEA

Mr. A. Kossilov  NENP - IAEA

IAEA PARTICIPANTS
Ms. E. Swaton  NENS/SAS - IAEA

Mr. B. Tomic  NENS/SAS - IAEA
OBERVERS

Mr. W. Ehrenberger
Fachhochschule Fulda
Fachbereich Informatik
Marquardstrasse 35
D-6400 Fulda

Mr. Spriet
French Mission, Vienna