Computerization of operation and maintenance for nuclear power plants

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

INTERNATIONAL ATOMIC ENERGY AGENCY
The originating Section of this publication in the IAEA was:

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

COMPUTERIZATION OF OPERATION AND MAINTENANCE FOR NUCLEAR POWER PLANTS
IAEA, VIENNA, 1995
IAEA-TECDOC-808
ISSN 1011-4289
© IAEA, 1995
Printed by the IAEA in Austria
July 1995
PLEASE BE AWARE THAT ALL OF THE MISSING PAGES IN THIS DOCUMENT WERE ORIGINALLY BLANK.
The need to use computers for nuclear power plant design, engineering, operation and maintenance has been growing since the inception of commercial nuclear power electricity generation in the 1960s. The needs have intensified in recent years as the demands of safety and reliability, as well as economic competition have become stronger. As a result, IAEA Member States have requested assistance and advice to guide their use of computers in nuclear power plants.

The rapid advance of computer hardware and software technology in the last two decades has greatly enlarged the potentials of computer applications in all aspects of design and engineering of future plants as well as operation and maintenance of existing plants. The traditional role of computers for mathematical calculations and data manipulation has been expanded to enhance human performance and corporate business by information processing and knowledge-based systems.

This report provides a resource for computerization of activities in plant operation and maintenance. Experience gained from design and implementation of various computer systems around the world is described. The material may be useful as a guide to modification and upgrading of existing plants as well as design and engineering of new plants. It should be particularly of interest to managers and engineers who are engaged in planning, bidding, specifying or designing computer systems for operation and maintenance applications.

The technical document is the result of a series of advisory and consultant meetings held by the IAEA in Vienna in 1991-1994. It was prepared with the participation of experts from Canada, France, Germany, Hungary, Japan, Russian Federation, Sweden, the United Kingdom and the USA. Recognition is given to other contributors in "Contributors to Drafting and Review" in this report.

Special thanks are due to B. Sun of the Electric Power Research Institute, USA, who compiled and edited the document from contributions provided by the working group members, particularly, A. Cook of Canada, D. Spohn of France, W. Bastl of Germany and D. Welbourne of the United Kingdom.

The IAEA officer responsible for preparing this document is A. Kossilov of the Nuclear Power Engineering Section.
EDITORIAL NOTE

In preparing this document for press, staff of the IAEA have made up the pages from the original manuscripts as submitted by the authors. The views expressed do not necessarily reflect those of the governments of the nominating Member States or of the nominating organizations.

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

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

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

The authors are responsible for having obtained the necessary permission for the IAEA to reproduce, translate or use material from sources already protected by copyrights.
CONTENTS

1. OBJECTIVE ................................................ 9

1.1. Operation and maintenance of nuclear power plants .......................................................... 9
1.2. Scope of the report ......................................... 9
1.3. Purpose of the report ...................................... 10

2. OVERVIEW OF COMPUTERIZATION ON NUCLEAR POWER PLANTS ........................................... 10

2.1. Use of computers in nuclear power plants ............................................................................ 10
  2.1.1. Historical evolution ......................................................................................................... 10
  2.1.2. Reasons for applying computers ..................................................................................... 10
2.2. Overview of application areas ............................................................................................... 12
  2.2.1. Computer applications to operations .............................................................................. 12
    2.2.1.1. Data logging .............................................................................................................. 12
    2.2.1.2. Information systems ................................................................................................. 12
    2.2.1.3. Monitoring and diagnostic systems ........................................................................... 13
    2.2.1.4. Digital control and automation ............................................................................... 13
    2.2.1.5. Protection .................................................................................................................. 13
  2.2.2. Computer applications to maintenance ............................................................................. 14
    2.2.2.1. Predictive maintenance and inspection ........................................................................ 14
    2.2.2.2. Maintenance management ......................................................................................... 14
  2.2.3. Engineering and administrative functions .......................................................................... 15
2.3. Human–machine partnership ................................................................................................. 15
  2.3.1. Functions which must be automated by computers ............................................................ 16
  2.3.2. Functions which are better automated by computers ....................................................... 16
  2.3.3. Functions which should be allocated to humans ............................................................... 17
  2.3.4. Balancing factors ............................................................................................................. 17
2.4. Relationship to safety and availability .................................................................................... 18
  2.4.1. System considerations ...................................................................................................... 18
  2.4.2. Regulatory and licensing requirements .............................................................................. 18
  2.4.3. Computers for safety applications .................................................................................... 18
    2.4.3.1. Advantages ................................................................................................................ 18
    2.4.3.2. Challenges ................................................................................................................. 19

3. COMPUTER APPLICATIONS TO OPERATION OF NUCLEAR POWER PLANTS ................ 21

3.1. Introduction ......................................................................................................................... 21
3.2. Monitoring, control and protection architecture ...................................................................... 24
  3.2.1. Monitoring systems ......................................................................................................... 24
    3.2.1.1. Operator information systems for plant monitoring ................................................ 24
    3.2.1.2. Specialized reactor monitoring ............................................................................... 24
  3.2.2. Fault-tolerant control systems .......................................................................................... 24
3.2.3. Integrated control and monitoring ...................................................................................... 26
  3.2.3.1. Objectives .................................................................................................................. 26
  3.2.3.2. Safety and availability ................................................................................................. 28
  3.2.3.3. CONTROBLOC layout in a 1 300 MW nuclear power plant .......................................... 28
3.2.4. Protection systems ............................................................................................................ 30
3.3. Information systems and operator aids ................................................................................... 30
  3.3.1. Information systems in the control room ......................................................................... 30
5.4.2.3. Data dictionary .......................................... 59
5.4.2.4. Data storage ............................................. 59
5.5. Obsolescence and retrofitting ................................. 59
5.6. Implementation issues ........................................ 60
5.6.1. Organization ................................................ 60
5.6.2. Implementation of databases ................................ 60
5.6.3. Training .................................................... 61
5.6.4. Investments required to achieve results .................. 61

6. FUTURE TRENDS AND RECOMMENDATIONS ..................... 61

6.1. On-line and off-line data management ....................... 61
6.2. Diagnosis and prognosis systems ............................ 62
6.3. Computer-assisted operating procedures .................... 62
6.4. Touch screen control ........................................ 62
6.5. Distributed systems ......................................... 63
6.6. Equipment with embedded software .......................... 63
6.7. Communication systems ...................................... 63
6.8. Network management ........................................ 64
6.9. Standardization of information exchange .................... 64
6.10. Data architecture and management for maintenance ....... 64
6.11. Effective verification and validation methods ............. 65
6.12. Configuration management .................................. 65
6.13. Fault-tolerant design ....................................... 66

7. CONCLUSIONS .................................................... 66

REFERENCES ....................................................... 69

ANNEX: REPORTS ON THE USE OF COMPUTERS FOR NUCLEAR POWER
PLANT OPERATIONS AND MAINTENANCE .......................... 75

Data management as a pre-requisite for configuration management .... 77
A. Cook

The contribution of an information management system to Electricité de France
enterprise strategy .................................................. 89
D. Spohn

Diagnosis systems in nuclear power plant developments and applications .... 99
W. Bastl, L. Felkel, D. Wach

Core monitoring system for VVER 440 nuclear power plants .................. 123
F. Adorján, L. Bürger, I. Lux, M. Makai, J. Valkó, J. Végh, I. Hamvas, Z. Kálya

Computer-based operator decision aids ................................ 127
Y. Shinohara

Computer-based support for operation, maintenance and management ........ 141
A. Andersson

Computer employment in protective action control systems for VPBER-600
nuclear power plant .................................................. 153
A. B. Pobedonostsev

The Torness advanced gas cooled reactors direct digital control and data
processing computer system ........................................ 159
D. Welbourne

Enhanced functions of process computer systems for nuclear power plants .... 169
B. Singer, S. Bhatt, B.K.-H. Sun
1. OBJECTIVE

1.1. OPERATION AND MAINTENANCE OF NUCLEAR POWER PLANTS

The advance of computer technology has been significant in recent years. The use of powerful personal computers and workstations is widespread in all sectors of industry. The role of the computer in nuclear power technology includes design, engineering, operation and maintenance and has grown steadily in the last decade. The use of computers has been extended from its traditional contribution of manipulations of large quantities of numerical data and mathematical equations for the design and engineering of nuclear power plants to its more current role of fast and accurate processing of information and applying knowledge-based systems for operation and maintenance of capital investment.

Operation and maintenance are fundamental aspects of a utility corporate business to keep nuclear power plants safe and reliable and to provide economic electric power. The major goals of using computers in operation and maintenance of nuclear power plants are (1) to improve safety and reduce challenges to capital investment; (2) to reduce the cost of operations and maintenance; (3) to enhance power production, and (4) to increase productivity of people.

The functions and tasks of operation and maintenance are closely related to each other. Operational needs include areas of control and protection, and manual actions in a control room that call for continuing and periodic surveillance, testing and maintenance of equipment. The need of maintenance is to keep a plant in an optimal state for safe and economic operations.

In the past decade, there has been a growing need to address obsolescence, improve human performance, and to comply with increasingly stringent regulation requirements. As a result, nuclear power plants have implemented plans to replace ageing analogue systems with digital systems and have developed comprehensive and accessible information database and management systems. These systems support operations and maintenance for an overall improvement in quality assurance and productivity. The advances in information and communication technology have been proved to help utilities operate power plants more efficiently by integrating computer resources and increasing the availability of information to meet NPP staff needs and corporate business strategy.

1.2. SCOPE AND STRUCTURE OF THE REPORT

This TECDOC contains technical and methodological information and recommendations requested from Member States for advice and assistance in the use of computers for operation and maintenance, for backfitting of existing plants and for new power plants.

Section 1 shows the objectives and outlines the goals of the IAEA in sponsoring this report to promote co-operation in the use of good practice in computerization of operation and maintenance activities in nuclear power plants.

Section 2 is an overview. It covers the motivation for the application of computers, the current practice in the use of computers, the advantages and disadvantages, human and machine interaction considerations and safety versus non-safety aspects of computer application.

Section 3 describes computer applications to the operation of nuclear power plants. It covers general aspects of on-line, real-time applications for instrumentation, control and protection systems, as well as operator aids for diagnostics and decision making.

Section 4 depicts the aspects of computer use in maintenance of nuclear plants. It covers the use of a database to support various activities including maintenance administration, outage planning, work authorization, tagging, spare parts management and computer-aided monitoring, inspection and surveillance, etc., and their related design and implementation issues.
Section 5 covers life cycle management of computer systems, with focus on the user aspects of dealing with changes, modifications, verification and validation, quality assurance and overall configuration management of the computer systems.

Section 6 outlines future trends and gives recommendations based on lessons learned from design and implementation, as well as R&D trends.

Section 7 provides a summary of the conclusions of this report. The Annex gives specific examples taken from direct experience of participating countries of computer applications in the field.

1.3. PURPOSE OF THE REPORT

The main purpose of this report is to provide information on practices and methodologies which may be used for computerization of operation and maintenance of NPPs, not only by the plant designers, but also by the utilities and the manufacturers of equipment and systems to meet operational and safety requirements.

This publication also provides information concerning different approaches to the use of computers, the history of operational experience, lessons learned, and a summary of existing computer systems.

The information is an overview and the reader is encouraged to seek additional detail in the referenced documents related to the particular applications that are of interest.

The state-of-the-art and future trends in the use of computers in operations and maintenance, including cost benefits, man-machine interface, life-cycle management, verification and validation, etc., are also considered in view of the fast evolution of the technology.

2. OVERVIEW OF COMPUTERIZATION OF NUCLEAR POWER PLANTS

2.1. USE OF COMPUTERS IN NUCLEAR POWER PLANTS

2.1.1. Historical evolution

In the 1970s, computer applications to operation gained broad recognition. The implementation of several large-scale, advanced control rooms and integrated control systems in the USA were unfortunately terminated due to setbacks of nuclear plant orders in the time period. Nevertheless, the advance of digital systems application in broad areas of operation and maintenance has been continuing around the world.

Digital technology has been increasingly recognized as a valuable tool for support and enhancement of human capability in the areas of monitoring, diagnosis, control, protection, maintenance, surveillance and communication.

2.1.2. Reasons for applying computers

Computers are applied to operation and maintenance of NPPs because they provide, but are not limited to providing, the following main advantages [1-18]:

- Complex protective and interlock functions, with extensive logic or calculations, often using proven PLC units of higher reliability and lower cost than relay systems.
- Automatic control for plant conditions which could not otherwise be possible, giving improved plant performance.
- Complex and rapid calculation facilities to allow on-line assessment of reactor conditions, giving improved safety, power output and economy.
VDU to display of plant conditions, which can reduce control panel size and increase operational effectiveness.
- Automatic records not otherwise possible, which often have a safety role.
- Plant control with reduced cable requirements of cable quantity, size, number of terminations etc, and thereby improved safety and economy.
- Use of proven systems for controlling inventory, purchasing, spares and management of material.
- Use of economic methods of storing and manipulating large quantities of data, either on-line or off-line to the process plant, and providing information to NPP staff.

The needs arise in the on-line, real-time processes of control and protection, alarm detection and display, and in the on-line assessment of processes needed for operation of a power reactor. In addition, they arise equally in the semi on-line operation needed for daily or hourly assessment of operation; for example, monitoring of detailed reactor flux distribution. The need to use computers also arises in the administration of the station to ensure safety, control of staff access and maintenance of spares and inventory.

NPP designers found that they could gain operating advantages if a calculation could produce some output of a value or condition which cannot be directly measured. For example, the NPP designers want displays of in-core flux profiles, interpreted from ex-core measurements. They want protection functions based on maximum heat flux for PWRs. They require safe refuelling operation when fuel movement may involve complex configurations of fuel ponds, transfer paths, bottling units, etc., which need careful interlocking and control.

NPP designers found good reasons for designs with mechanical systems and boilers where complex control algorithms must be followed to prevent metallurgical damage. The hazard requirements may require fail-safe action to be taken by equipment in switchgear rooms if cables are destroyed by fire. Such operations are either very difficult or even impossible unless computers are used. Several international standards have been developed to guide the design of digital systems for nuclear plant applications [19-22].

The penalty of using computers can be a high risk of short-term failure of achievement or even delay in NPP delivery of power. A major problem can be the demonstration that computer systems are satisfactory for safety, since the system may have a direct impact on protection or even provide protection directly. Very high costs can be incurred in demonstrating the safety of a software system and in verification and validation of the final system due to the complexity which was in itself the reason for using computers [23].

A major difficulty with the application of computers is that the requirements of a NPP are always special and specific. Much on-line software must, therefore, be specifically written and the hardware configuration is generally difficult to obtain off the shelf. A major problem with procurement of on-line systems has been and continues to be the need for internal redundancy to ensure high availability of the computer functions. These problems have often prevented the design intentions from being fully achieved, and the economic benefits expected have not always been fulfilled in consequence.

NPP managers were quick to adopt commercially available database management systems, for the control of spares and inventory, for staff access control and records, for management of information, etc. Development has been rapid, and modern power stations are designed with a full project database of all items in the plant, all drawings in CAD format, and all project design documents held and controlled through computer systems. On the other hand, problems have been found in ensuring compatibility of information and its accuracy. The software systems for such total information control are very extensive, and have been found to be difficult to produce in the allocated timescales, and difficult to fill with the vast amount of data accurately.
2.2. OVERVIEW OF APPLICATION AREAS

2.2.1. Computer applications to operations

The use of computers on-site date back almost to the beginning of commercially applied nuclear power. At this time a central computer served as a data logger. With the progress of technology, smaller dedicated computers have been introduced, which now serve for data acquisition, exchange of data throughout the plant, information generation by means of simple logic or more complicated analytical functions, and by providing the desired information to the operator in the control room, usually by means of VDUs.

In parallel, computers began to be used for open and closed loop control and are also applied for the protection of the plant. Early protection applications often were limited to calculating safety-relevant parameters such as departure from nucleate boiling (DNB); later applications included all signal handling, trip detection and redundant majority voting functions.

Theoretically, we can distinguish between computers used:

- for storage of operational data in order to have available historical data for later checkup or comparison, and
- for real-time data management in order to serve all needs of on-line monitoring and automation.

2.2.1.1. Data logging

The first major computer system used in nuclear power stations was the plant process computer which typically processes thousands of analogue and digital signals. These computers provide the plant operators with basic data to facilitate smooth startup and shutdown operations, as well as efficient, steady state operation. They generally provide alarms. The process computer has undergone continuous renovation and replacement as the old 1960 computer systems have become obsolete. In some modern plants, such systems are considered safety related.

2.2.1.2. Information systems

On-line computers are used in control rooms with two main goals - information presentation and information generation [5, 6, 8, 9, 12, 14].

High definition colour VDUs are normally used for information presentation. The information can be shown in the form of system diagrams with inserted parameter values and plant states, trend curves showing the history of important physical parameters, and as listings of plant alarms in groups or according to their priority. The information on one VDU screen will be a selected subset of all information, and therefore is serial rather than parallel in nature. It is therefore important to arrange simple and direct methods of selection at other associated displays, for example, by pan and scroll facilities to display adjacent plant groupings on the process, or by linked navigation facilities using soft keys, mouse or tracker ball facilities. Often, fixed keys give rapid selection of the most frequently used displays and alarm listings.

Some systems have reduced the difficulty of associating information from several displays at once by grouping several VDU screens together in the control panels. One of the more successful methods is to group the method of selection of displays from an overview screen for a plant area (e.g. the reactor primary coolant circuit, or the steam generators) with rapid selection of detailed displays using pre-programmed targets on the overview. By these means, rapid location of the alarms of a plant is possible, and the operators retain a spatial view of the plant through the relationship of the displays to the overviews.
Information generation and concentration are basic to the use of computers. They are therefore used with the VDU to present concentrated or calculated information, selected information and historical trend information. Information functions such as status monitoring, heat and mass flow visualization, critical function monitoring, and success path monitoring can be included. These functions will select information and present it in flexible formats which are designed to include calculations and data selection processes, and present the necessary information for the operator use and support the decisions needed for each task for safety or for the next steps in a plant manoeuvre.

In the course of development, such functions have often been implemented as stand-alone systems or operator aids, driven by operational needs of a specific plant or by licensing requirements. Typical examples are core power mapping systems, load following advisors and safety parameter display systems. Today, these systems are normally integrated into the total station data processing and display system of current process computers as well as in advanced control rooms.

2.2.1.3. Monitoring and diagnostic systems

Monitoring of the mechanical components and systems of the plant is an important application of computers. On-line monitoring and diagnostic systems have been applied to reactor vessel internals, pumps, safety and relief valves and turbine generators. The monitoring techniques include noise analysis, vibration analysis, and loose parts detection. Complicated signal analysis may be involved, e.g. conversion into the frequency domain, application of correlation and pattern recognition methods, etc. Comparison to reference values or "signature" information and trending are important tasks. More recently, expert system methods have been introduced in order to improve the performance of such systems.

The advantages of performance, therefore, cause computers to be increasingly used to enhance monitoring and diagnostic functions, to make the methods applied more user friendly and to achieve the necessary user acceptance.

Since a main goal of the diagnosis systems is the early detection of a developing mechanical deficiency, the importance for maintenance and inspection is obvious. Experience shows that due to findings of the on-line diagnosis systems, the preparation of repair actions can be considerably improved, and maintenance and inspection times can be reduced.

2.2.1.4. Digital control and automation

As utilities in recent years have met problems of obsolescence of analogue technology and unavailability of spares, the existing analogue systems have been gradually replaced by digital controllers. Fault-tolerant digital feedwater and reactor power and power distribution controllers have been successfully designed and implemented for advanced gas cooled reactors, CANDU plants, BWRs and PWRs [24-28].

The designs can provide dual redundancy with rapid bumpless changeover on failure of one channel, bumpless transfer from manual to automatic control, signal validation of sensor inputs, a simple man-machine interface, and control algorithms able to handle wide ranges of plant conditions with the non-linearity features needed for the wide range of plant dynamics. The operating experience of these digital control systems has demonstrated that for some applications they improve operational reliability and avoid reactor trips and outages, their main advantage is however simplification and cost reduction of maintenance and better information and documentation about actual implementation.

2.2.1.5. Protection

The first application of the digital computer in a reactor protection system of a nuclear power station was the installation of the core protection calculator (CPC) in the Arkansas Nuclear One, Unit
2 (ANO-2) plant in the late 1970s [29]. The intensive licensing review process proved to be a challenge to the utility. Extensive efforts, including review and testing, were made by the utility and its supplier to validate and verify the design and performance of the computer system. This effort, as well as the operating experience of the ANO-2 plant since 1979, has demonstrated that computers can be used effectively for safety protection functions. The US NRC published a detailed assessment of one such proposal [30].

A similar computerized version of a local core protection system (using cobalt incore detector signals) was for years installed in the NPP Grafenrheinfeld for studying purposes as a four channel/open-loop arrangement [31-33].

Recently, nuclear plants have begun to implement digital protection systems for replacement of obsolete analogue units. These digital systems include self-diagnostics and self checking features which can substantially reduce testing and surveillance functions by operators. One full computerized safety shutdown system has been installed in the CANDU plant and digital protection systems have been operational in French 1300 MW PWRs. Neutron flux measurement systems with reactor trip functions performed by computer equipment are installed in several Swedish BWR plants (Ringhalls, Forsmark and Barsebäck) and is being installed at present in the Kerncentrale Borssele in the Netherlands (Sinuperm N). A computerised protection system (described in Section 3.5.2.3) is installed at Dungeness B AGR in UK. A computerized protection system has been installed for Sequoyah PWR in the USA and the Sizewell B PWR in the UK. In the boiling water reactor Gundremmingen a subsystem of a limitation system to protect against channel dry out is in operation [34]. The safety implications have been proven to be a major challenge to the applications of computers to protection systems [7, 16, 23].

2.2.2. Computer applications to maintenance

2.2.2.1. Predictive maintenance and inspection

The application of computer technology to maintenance and inspection has recently gained increasing attention. On-line monitoring and diagnostic systems have been applied to reactor vessel internals, steam generators, pumps, safety and relief valves, and turbine generators. Digital processing of sensor information has been coupled with adaptive learning techniques for analysis, e.g. the neutron, acoustic, radiographic, ultrasonic, or eddy current signals, and provide a decision support system for predictive maintenance.

Technical specification monitoring systems have been developed which enable plant maintenance personnel to achieve compliance with operational licensing requirements while maintaining flexibility with respect to maintenance schedules and system configuration.

Special computer equipment is also used for performing recurrent tests of the rather sophisticated limitation systems (in semiconductor technology) in Geman PWR NPPs [35].

2.2.2.2. Maintenance management

As utilities implement more and more computer software and hardware, a need has emerged for a comprehensive and accessible information database and management system in nuclear plants. This information database supports maintenance, commitment tracking, personnel management, and radiological control, etc., for overall quality assurance and productivity enhancement. The advances in computer communication technology have been proven to help utilities operate power plants more efficiently by integrating computer resources and increasing the availability of information to meet the needs of NPP staff.
The basic support systems in current use, or being developed, include the following:

- Daily work planning, including maintenance work plans, preventive maintenance program, daily work schedules for crews.
- Outage planning including compiling list of all work, resource analysis and preparation, critical path analysis, scheduling and prioritization of work.
- Material management, including material specification, equipment spare parts lists, material storage and ordering systems.
- Maintenance support, including radiation hazard surveys, qualification requirements for specialized work, calibration records, and management of specialized tools.

There is also a trend in the utility industry to apply knowledge-based expert systems to various engineering, maintenance and operations functions. Expert systems technology has a number of specific capabilities which include: programming flexibility, inference capabilities, explanation facility and knowledge structured according to human models. Expert systems can be used as an aid to help achieve goals set by the electric power utilities. Examples of successful implementations are PWR water chemistry diagnostics, reactor emergency action level classifications, emergency operating procedures tracking, diesel generator diagnostics, and fuel shuffle planning.

A recent advance in this area is the use of expert systems and neural networks in recognizing hand-drawn text and symbols on engineering drawings. Designed to save costs for power plants to maintain design configurations and knowledge and to facilitate design modifications, the pattern recognition techniques convert the scanned binary raster image of a drawing into intelligent, computer-aided design (CAD) objects such as lines, arcs, circles, symbols and text. Development of the semi-automated drawing conversion tool will provide cost effective ways to extract information from engineering drawings to populate CAD and other plant databases.

2.2.3. Engineering and administrative functions

There are a number of engineering and administrative functions that are typically computerized. Although not discussed in detail in this report, examples of such systems include:

- Basic administrative systems for payroll, word processing, budgeting and accounting.
- Basic communication systems such as electronic mail and electronic bulletin boards.
- Fuel and physics systems to manage the insertion of new fuel bundles and storage of irradiated fuel.
- Technical support systems such as computer-assisted drafting, reliability statistics analysis, and performance reporting systems.
- Safety analysis systems, such as are used for reactor physics modelling, thermal and hydraulic analysis, containment pressure analysis, risk analysis and registry of licensing documents.

2.3. HUMAN–MACHINE PARTNERSHIP

Many functions in NPPs are achieved by a combination of human actions and automation. Increasingly, computer-based systems are used to support operations and maintenance personnel in the performance of their tasks. There are many benefits which can accrue from the use of computers but it is important to ensure that the design and implementation of the support system and the human task places the human in the correct role in relation to the machine; that is, in an intellectually superior position, with the computer serving the human. In addition, consideration must be given to computer system integrity, software validation and verification, consequences of error, etc. To achieve a balance between computer and human actions, the design process must consider each operational function in regard to either computer, human operation, or more commonly, in nuclear plants a combination of human and computer. The process is usually known in the ergonomics literature as "allocation of functions" [17, 19].
2.3.1. Functions which must be automated by computers

The first consideration must be to examine any function for which a computer is mandatory. It is desirable that any such task definition would be justifiably based on human factor principles, but this may not always be so where mandatory requirements are based on established custom and practice. The designer must identify all the functions which, by virtue of their nature and their requirements, can only be achieved using a computer. As a general statement, these can be defined as those which exceed the capabilities of human performance. In determining whether a function falls into this category, the design team must consider the long-term demands of the task, the required performance under the worst possible conditions, and the variability of the human operator. Performance factors which will need to be addressed include: required task rate, accuracy, repeatability and, in particular, the consequence of error. Functions which exceed the capacity or capabilities of humans include:

- Processing large quantities of data
- Tasks requiring high accuracy
- Tasks requiring high repeatability
- Tasks requiring rapid performance
- Situations in which the consequences of error are severe
- Situations in which errors cannot readily be retrieved or corrected.

Typical applications in a NPP for which the use of computers will be necessary include: data recording, analysis and archive. Depending on the particular task performance requirements, in all such cases it will be easy to demonstrate that one or more human capabilities would be exceeded if the resulting task were performed manually.

When a decision is being taken to use computers for a function, consideration must be given to supplementary tasks, such as maintenance and testing activities, which are required to allow the computer to perform its role [36]. Further on it has to be considered that human operators may have difficulties in coping with the psychological impact of automation [37].

2.3.2. Functions which are better automated by computers

Certain functions may be identified which, although lying within the capability of human performance, may be better assigned to a computer. These include those functions which are lengthy, require high consistency, high accuracy or involve a degree of risk to an operator. Tasks which would result in boredom or monotony for an operator also fall into this category. The progressive increase in the capability of technology means that computer use can be considered for more and more functions. The cost of such technological solutions is often seen to be falling, and computer use becomes an increasing possibility. The point at which computers are regarded by users as necessary, or become a normal expectation, changes as societal and workplace values change.

An additional benefit of using computers is the potential improvement which they can bring to the design of jobs and working conditions by changing the role humans play in technology-based systems. With careful job design, significant improvements in operator roles can be achieved. There may also be consequential improvements in overall system performance.

Practical examples of computers being introduced to replace tedious or arduous human activities include the use of machines to carry out maintenance or surveillance activities; for example, steam generator examination. Computers are also being used increasingly to carry out lengthy, repetitive testing such as that for safety and protection systems. Not only does this improve the role of the operator, but it also brings improvements in the consistency of testing and may allow it to be carried out more frequently.
2.3.3. Functions which should be allocated to humans

Functions which require heuristic or inferential knowledge, flexibility, etc., will need to be assigned to humans. In addition, there may be practical or technical constraints which make computers impractical and thus require human operation. In many cases, it will be possible to justify assignment of such functions to the human. However, there is a risk that functions will be so assigned simply because computers would be difficult to use or uneconomical in some way. Regrettably, a function may be assigned to a human simply because there is a lack of a precise specification or some difficulty in producing one. It may prove possible to produce a workable system in this way but there is a risk that the result produced is an unsuitable or inappropriate set of tasks for the human.

A particular set of functions which is currently left with the human operator is that which occurs in extreme fault or accident situations where human flexibility and high level skills are essential and the unexpected nature of the task makes specifying appropriate computer functions difficult or impossible.

2.3.4. Balancing factors

The following qualitative factors will govern the relative weighting used in allocating functions between humans and computers.

1. **Existing practices:** The extent of using computers depends on operational practices and the level of technological and experiential support that is available. For example, staff trained in computer maintenance may be required before a high degree of computer use is possible.

2. **Operational and design experience:** Experience is often critical in establishing the confidence and justification for further use of computers. For example, if an organization has successfully implemented computer functions which have resulted in fewer spurious plant shutdowns, that utility is more likely to consider using more computers.

3. **Regulatory factors:** Regulating bodies establish specific rules which may restrict or, conversely, require the use of computers.

4. **Feasibility:** Sometimes using a computer is not possible for practical reasons. For example, installation downtime may preclude modification in an existing plant.

5. **Cost:** There are very few cases where other factors will totally outweigh costs. A cost benefit must exist to justify most proposals to use computers.

6. **Technical climate:** Increasing capabilities of technology may facilitate the use of computers while unavailability of technology may limit what can be achieved by computers.

7. **Policy matters:** An organization may develop policies that encourage or discourage using computers. For example, the decision to standardize on a type of plant design may determine the level of computer use.

8. **Cultural and social aspects:** The modified role of the operator in a highly automated plant may represent a social problem that can lead to loss of motivation and significantly decreased performance.
The various factors which exist may differ between applications and may be affected by whether a new design or a modification to an existing process through retrofit is being considered. In the retrofit case, the implementation of computers has less flexibility, owing to existing plant designs, operating practices, the need for replication, etc.

2.4. RELATIONSHIP TO SAFETY AND AVAILABILITY

2.4.1. System considerations

A computer system for operation and maintenance (O&M) of a power station will be installed because it improves safety, plant availability or economy of operation. The relationship of the computer to these factors must be carefully considered during system design. When a computer is intended in a NPP to improve safety, its impact on availability must be considered, and vice-versa. A specific factor which has been of importance is the need for internal redundancy of the computer system to ensure continuity of operation of the functions during single failures of computer modules. Often, proprietary equipment able to provide comprehensive control and display facilities for process plants may be available only on a single channel basis, and this can make it unusable for a NPP both on availability and safety grounds.

When an on-line computer system is intended in a NPP, its role in the maintenance or provision of safety must be considered with care, as for any item of I&C. Its role in the safety of the station should be assessed using the criteria given in IEC1226 [38] and its basic reliability, redundancy, environmental durability, quality assurance (QA), and other requirements determined in accordance with that document.

2.4.2. Regulatory and licensing requirements

Special care must be given to the requirements of licensing and regulatory bodies in regard to software systems. Safety and protection systems can be considered as a special case of control systems. They have additional regulatory and technical requirements imposed on them [39-41]. Requirements for good practice for such systems is given in IEC 880 - "Software for Computers in the Safety Systems of NPP" [21], and a supplement under preparation by IEC/SC45A on recent developments, increasing the scope of the recommendations to cover all computer systems important to safety, as defined in IAEA-50-SG-D3 & D8 [42,43]. Additional requirements such as the use of formal mathematical methods in design, very comprehensive and independent V&V, testing on-site, etc may also be applied to safety systems in some countries.

The duty of licensing and regulatory staff includes consideration of factors which may not have been thought of by the designers. It must, therefore, be always remembered that a computer system may be found to have a role in safety which had not been clearly foreseen, and, therefore, the best practice will be necessary in design, installation and operation even of computers which provide an operating aid or support function.

2.4.3. Computers for safety applications

2.4.3.1. Advantages

Specific reasons for considering computers for applications important to safety include:

1. The ability to process large volumes of complex information rapidly.
2. The ability to process the data, and to display information rapidly to the operators.
3. The ability to present complex information in a form which can be easily interpreted.
4. The ability to validate the process information by automatic checks during the input process and by software which compares similar or related signals.

5. The ability to obey complex algorithms or calculations in determining the plant state and safety.

6. The possibility of saving space for equipment cabinets or cables in the station layout.

7. The minimization of electrical penetrations from reactor containment structures by the use of multiplexed signal transmission.

8. The provision of safety information from the safety system via separate routes both to a Main Control Room (MCR) and to emergency or support control points, such that all information can be shown and recorded, and remains available if the MCR must be evacuated.

9. The retention of data on previous events, fault transients or trips (as a post-event record or a reference "signature") for later analysis.

10. The ability of computer equipment to self-test and thereby to provide modules with fail-safe characteristics.

2.4.3.2. Challenges

Challenges which have been encountered in applying software systems to applications important to safety include:

1. The computer application may be thought to reduce operator "on-the-job" involvement. Management action for training and for ensuring job satisfaction will be needed.

2. The redundancy of the computer system must be considered carefully and the actual in-service reliability of computer modules should be determined during design. Redundant, hot-standby systems can achieve outage levels below 1 to 10 hours/year. This requires very careful design.

3. The use of a computer for a function important to safety must include consideration of common mode failure of the computers. If a monitoring function is provided by two separate channels of a computer system, consideration should be given, for example, to separate power sources, separate environmental control systems, and separate equipment rooms and cable routes. Furthermore, consideration must be given to the need for some form of backup and diverse method of providing the function if the system does suffer a common mode failure of software or hardware.

4. Programmable devices are in themselves complex, and may be modified by the manufacturer without notification. Analysis to determine failure modes, and careful QA audit trails will be needed for a safety system application, although less stringent measures may be acceptable for less critical functions.

5. The overall system design of a computer system important to safety should consider carefully the division and partitioning of the system between safety critical and safety related sections, both for the hardware and the software and the data within the systems.

6. The division of the system should take into account the need to assemble the system on site in a structured and systematic manner, and to build up operator familiarization effectively.

7. The use of a computer system to functions important to safety will depend on and interact with the reactor system characteristics. This will be found to affect the functional requirements in many ways. Interaction can be expected from:
(a) The internal characteristics of the reactor and its self-regulation and self-limiting characteristics over its whole operating parameter range.

(b) The equipment installed on the plant, and the plant itself, in regard to normal and failure modes of self-actuating passive devices, active devices, the characteristics of pneumatic valves and actuators, the operation of regulation systems, etc.

(c) Special requirements for reactor manoeuvrability conditions.

8. The computer systems partitioning and internal intercommunication must be considered carefully in relation to the transmission of faulty data, defective programs or incorrect control commands and the like. The safety system itself is subject to requirements of electrical isolation from other, non-safety systems. It must also be subject to comparable and stringent isolation from data, program, commands and information which is not of the safety system.

9. The computer software will consist of program code modules and data, which specifies how the code is to act. The identification of the data and of its inclusion in the software is often difficult, and often a cause of error. Great care must be exercised, and careful management procedures followed, when data is prepared or changed.

10. The complexity of a safety functional requirement may be a major reason for choosing a computer implementation. The result is, therefore, certain to be complex and may involve large quantities of computer code and data which may take a long time to produce, install and test. The challenge is therefore to identify simple safety functions, and to develop code able to perform it without unnecessary complexity.

11. The use of computers for functions important to safety must include a careful assessment of the potential impact of a software failure. No method exists to guarantee no software errors will remain after final installation. Therefore, if redundant safety plants are each controlled by separate software systems which use the same software modules, all redundant safety plant items could fail to act due to a single software error. The station system design, therefore, requires consideration to ensure some complementary control or alternative safety plant can be claimed to maintain safety if such an event occurred.

12. The quantification of the reliability of software-based systems remains a difficult area. The level of complexity and the maturity of development and checking practices of analogue based systems has allowed the assumption to be made that the reliability of the system can be quantified as the random failure rate of the hardware, provided accepted development practices have been rigorously followed. The current position is that software failure is dominated by design errors, not be random failures, and consequently the analogue route is not open. The challenge is to produce a means of quantifying design failures for the software implementation process or to develop the arguments for showing the current analogue practice of using random failure rates can be justified for computer-based systems.

13. The through-life maintenance of computer-based systems can pose problems of differing nature to those encountered for analogue systems, the most common of which is time scales. Analogue systems are generally installed for periods of 20 to 30 years and because of the relatively stable manner in which the technology evolves, maintenance only becomes a problem towards the end of life as component manufacture ceases and stocks run out. The threat to maintenance of computer-based systems comes from two sources, first for control and display systems the software life is short. The systems are usually built around some proprietary kernel and support is only available for the most recent kernel. This can force very frequent upgrades, these upgrades can in turn force the need for hardware upgrade as the later versions of the software seek to exploit the latest hardware almost annually and appear to have a shelf life of only a few years. Critical systems that avoid proprietary software including operating systems
would appear to face less of a problem as once in service they generally remain unaltered. Here the threat is genuine hardware obsolescence which may occur on a long time scale (about 10 years) but shorter than for analogue hardware. There can also be a threat arising from the development environment and hence the maintenance environment, which is usually software dependent, becoming unmaintainable.

14. A particular requirement of regulatory authorities is for very high confidence in the correct statement of requirements, and in its successful, error free implementation. To meet this, special analysis and review may be required and this may be very costly and demanding. The challenge is to meet this in an economic, timely and efficient manner.

15. Safety-related systems will require internal checks to prevent control system demands, alarm settings, etc. from being set to unacceptable values, but may permit some inward data and program flow. In all cases, stringent measures to prevent corruption from unauthorized communication and spurious connections must be enforced by system design, management procedures, internal software checks and lockouts and other appropriate measures.

3. COMPUTER APPLICATIONS TO OPERATION OF NUCLEAR POWER PLANTS

3.1. INTRODUCTION

When discussing the use of computers in the operation of a NPP, a very broad scale of both the computing devices and the activities they are meant for must be considered [44-47]. The operational activities are closely related to maintenance as described in Section 4. A computerized function is considered as a part of the operation of a NPP if:

- It has an interaction with the operational personnel or is on-line to the plant instrumentation and control equipment;
- It is real time or quasi real time;
- It is directly related to the systems and to the processes of the NPP.

The basic functions usually provided for a nuclear power plant by on-line computer systems are plant monitoring and recording, and the display of information and alarms.

On a typical reactor plant, between 3000 and 7000 analogue signals from instruments measuring temperature, pressure, flow and other special parameters will exist. In addition, between 10 000 and 20 000 state signals will be used. These state signals provide information on switchgear states, valve states, and alarm states and may include the states of control room switches [1,3].

The main use of the computer system is to read in these signals at intervals, typically one second, and to form an internal data base representing the plant condition.

That internal database is then available for software to perform checks of analogue signals for high, low and other alarms, and checks of state signals for alarms. In the alarm check process, the computer system provides recorded time of detection on printed logs and on magnetic media for off-line analysis. VDUs allow the alarms to be displayed to the operators, with clear language titles, the instrument or plant contact identity, and other information.

The internal database can be used to operate VDUs to show the current plant state. A typical installation may have 200 to 500 display formats, which group signals and present their values and states with suitable titles for each plant item, or plant system. Special displays can be designed appropriate to specific operations, for example, attaining reactor criticality or controlled steam raising operations. A typical installation will allow the operator to select any display to any VDU in the control room. The display will appear within 1 or 2 seconds with current plant conditions shown and
refreshed at regular intervals of 2 seconds or less. Normally, any of these displays can be printed to record the conditions seen, and printed logs showing the current state are available [48].

The use of modern high definition, graphic and colour VDUs gives many possibilities for displays with mimic presentation of the plant, dynamic symbols to show valve open/closed states, coloured histogram presentation of level, etc. Great care must be taken in the design of these displays to ensure consistency of style and representation of all plant information, and the design should allow for comprehensive review of the displays, a strong human factors input, and the views of the operating staff [49]. The VDUs can show the output of calculations; for example, to derive reactor flux profiles, or to identify the highest and lowest core exit temperature.

By storing sections of the database at regular intervals, histories of signals can be produced. These can then be displayed on VDUs to show trends as graphs of chosen signals.

Generally, graphs of turbine temperature, vibration and other conditions are of special value, as are graphs of feedwater and steam conditions. This information is normally available as a special log, retained or printed out at a turbine trip for identification of any turbine problems. Great care is needed in design to limit this information to that which is truly needed, and to avoid excessive numbers of records being produced.

The database available within the computer system which represents the plant condition allows records and logs to be produced both as printed records, and magnetic records. Special care is needed in designing these logs, in making a distinction between a log of the current state, a log which gives a historical record of signals (for example, the values taken every 30 minutes for an eight-hour shift), and a log which includes calculations such as average over time or integration of values such as leak rates over time. The logs provided on a station typically include shift handover information logs, daily efficiency logs, routine logs at intervals of one hour or one day, and various post-trip logs for diagnosis of reactor and turbine problems. A log of special importance is that which records the inputs, conditions, and actions of the reactor protection system so that the reasons for any trip may be determined. The use of off-line VDUs can allow rapid inspection and checks of logs made in magnetic form.

Typical computer functions are listed in Table I. This table shows a great variety of computerized functions exists in various NPPs. This chapter discusses these functions according to the following classification:

- Information and operator aid systems
- Computerized control and automation
- Computerized protection systems.

It is worth mentioning, however, that the separation and order of the subject, as above, reflects the level of computerization of the activity at hand. Thus, while some sort of information and operator aid computer system exist at almost every NPP, the application of computers to closed loop control is more recent and the application to the protection system has been done only to very recent plants and current designs of light water and CANDU reactor plants [50]. Particularly for the protection systems, safety implications and regulatory concerns have been major challenges to implementation [2, 16, 23, 41].

When discussing the interaction with computerized services in a NPP, the integration of the distributed information and control systems through networking is a major concern. On the other hand, distributed systems are usually involved in data acquisition and control and are connected and integrated with other systems in higher hierarchical positions. In other words, the distributed units perform the primary, "in-field" task, the integrated system, like an envelope, covers the interconnection between the various processes, possibly including also maintenance and design analysis.
<table>
<thead>
<tr>
<th>TABLE I. TYPICAL COMPUTER FUNCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic functions</strong></td>
</tr>
<tr>
<td>- Process communications</td>
</tr>
<tr>
<td>- Human-computer communication</td>
</tr>
<tr>
<td>- Sequence of event recorder</td>
</tr>
<tr>
<td>- Transient recording</td>
</tr>
<tr>
<td>- Alarm annunciation</td>
</tr>
<tr>
<td>- Persistent alarm handling</td>
</tr>
<tr>
<td>- Data logging</td>
</tr>
<tr>
<td>- Postmortem review</td>
</tr>
<tr>
<td>- Limit checking</td>
</tr>
<tr>
<td>- Communication with in-core fuel management computer system</td>
</tr>
<tr>
<td>- Self checking</td>
</tr>
<tr>
<td><strong>General functions</strong></td>
</tr>
<tr>
<td>- Issuing of production report</td>
</tr>
<tr>
<td>- Measurement of operation time</td>
</tr>
<tr>
<td>- Transient recording</td>
</tr>
<tr>
<td>- Supervision of safety functions</td>
</tr>
<tr>
<td>- Supervision of plant status</td>
</tr>
<tr>
<td>- Safety system testing</td>
</tr>
<tr>
<td>- Redundant input validity checking and mean value calculations</td>
</tr>
<tr>
<td>- Automatic surveillance testing</td>
</tr>
<tr>
<td><strong>Core supervision functions</strong></td>
</tr>
<tr>
<td>- Neutron flux calculation and display</td>
</tr>
<tr>
<td>- Neutron flux sensor supervision</td>
</tr>
<tr>
<td>- Core performance calculation and presentation</td>
</tr>
<tr>
<td>- In-core neutron flux sensor calibration</td>
</tr>
<tr>
<td><strong>Reactor supervision functions</strong></td>
</tr>
<tr>
<td>- Calculation of reactor thermal power</td>
</tr>
<tr>
<td>- Presentation of operating point</td>
</tr>
<tr>
<td>- Reactor coolant water quality monitoring</td>
</tr>
<tr>
<td>- Calculation and surveillance of reactor vessel heating</td>
</tr>
<tr>
<td><strong>Automatic control functions</strong></td>
</tr>
<tr>
<td>- Control of startup flux</td>
</tr>
<tr>
<td>- Control rod manoeuvre (fine motion control)</td>
</tr>
<tr>
<td>- Control of feedwater flow</td>
</tr>
<tr>
<td>- Control of reactor temperature and pressure</td>
</tr>
<tr>
<td>- Boiler or steam generator level control</td>
</tr>
<tr>
<td>- Control of feedwater pumps</td>
</tr>
<tr>
<td><strong>Protection functions</strong></td>
</tr>
<tr>
<td>- Reactor trip detection</td>
</tr>
<tr>
<td>- Reactor trip actuation</td>
</tr>
<tr>
<td>- Actuation of emergency safeguard systems</td>
</tr>
<tr>
<td><strong>Turbine governor and supervision functions</strong></td>
</tr>
<tr>
<td>- Main-turbine supervision and governor control</td>
</tr>
<tr>
<td>- Turbine condenser performance monitoring</td>
</tr>
</tbody>
</table>
3.2. MONITORING, CONTROL AND PROTECTION ARCHITECTURE

3.2.1. Monitoring systems

3.2.1.1. Operator information systems for plant monitoring

Modern monitoring systems depend on the operation of full colour VDUs, with full graphic facilities [12, 19, 48, 52]. The process plant information is held as a real-time database which can be accessed by all VDU stations. The typical architecture includes full redundancy of all data transfer paths, multiple VDU work stations, and redundant gateways from data gathering networks or specialized data sources such as the protection system. Redundant backing disc storage is included, together with redundant central processors for system coordination and database management. The operation of the processors will be on a hot stand-by basis. A representative configuration is in Figure 1. Such systems require large, special project teams to coordinate the design and implementation in all its aspects. Extensive use of off-the-shelf hardware will be needed for interfaces with other systems, operation of hot-standby computers and other factors. A major technical point is the requirement for a high bandwidth on the interconnecting LAN or highway. Although extensive standard system software may be available for such systems, they often require some system software development, and will require application software development which may be extensive.

The preparation, verification and validation of the data for each processing operation, each signal, and all VDUs and records is a very extensive task which is special to the particular NPP. Data may be required for about 6000 analogue signals, 20 000 digital signals and 500 VDU designs, and the magnitude of this task requires detailed and careful management.

3.2.1.2. Specialized reactor monitoring

For individual monitoring systems retrofitted in existing plants, the network architecture is much simpler than the plant-wide operator information system, as presented in the last section. These individual operator aid monitoring systems are implemented, often in a modular and piecemeal fashion, for specific requirements and needs which are often driven by regulations.

Representative monitoring systems for reactors consist of redundant minicomputers with proprietary or specially designed interfaces to signal measurement and input digitization equipment. Redundant backing disc stores may be provided, and output will be to dedicated VDUs and printers. The systems may be able to provide very high availability even without redundancy. Such systems can, today, be configured from off-the-shelf items with special-to-project software operating under control of a proprietary operating system. A representative architecture is given in Figure 2.

3.2.2. Fault-tolerant control systems

Modern control systems typically have dedicated minicomputers or microcomputers, with a program for the automatic control functions and the operation of the input/output equipment permanently in read-only-memory (ROM), or other permanent memory. Standard input digitization cards and contact signal input sensing cards will be operated by the microprocessor. Standard digital-to-analogue converter units or other interface modules will be used.

To maintain availability, the minicomputers will be redundant, and they will both have full access to all inputs and outputs. An arbitration unit will be used to assign which computer is on-line and which is on standby.

Normally, the control system will send information on its actions to the monitoring computer system. In early systems the control functions and monitoring functions were often in a single computer system.
Such systems normally are implemented using a proprietary control language, giving the control
engineer direct access to operations for proportional, integral and derivative action, for hysteresis and
for actuator monitoring. It may be possible to configure the control design using an interactive CAD
approach. Special software to interface with other systems may be needed, and for on-line/standby
operation. A representative configuration is shown in Figure 3.

FIG. 1. Representative configuration of an operator information system for plant monitoring.
3.2.3. Integrated control and monitoring

A representative system which integrates control and monitoring is the CONTROBLOC system, installed on the EdF 1 300 MW nuclear power plants in France. The system receives control room controls and information from sensors and actuators, performs the control logic and interlock functions, and operates station equipment and electrical switchgear accordingly. The system provides closed loop control as well as information display on VDUs.

3.2.3.1. Objectives

The system objective is to provide high reliability control and plant signal monitoring, while reducing the physical size of the control equipment by using microprocessor technology. To achieve this in a satisfactory way, it is necessary to select some specific targets. The selection of these preferred targets must take into account the field of application of the electronic system.
For example, an extensive hardware redundancy will increase availability, but will decrease reliability. Similarly, performing a frequent and detailed hardware integrity diagnosis, especially on the passive components, gives the risk of too tight overlapping of the action and survey loops, and of too frequent program interrupts. This will prejudice safe operation. Consequently, priority has been given to the four following design objectives:

- Safety and availability of automatic controls.
- Adaptability to subsequent changes of process operation. Capability of performing new control functions without changing the system architecture. CONTROBLOC is designed to be a versatile system.
- Staff not acquainted with electronics and data processing techniques shall be able to configure, program, test, maintain, repair and modify the CONTROBLOC cabinets.
3.2.3.2. Safety and availability

A high safety level means design for a risk of spurious or unsafe actuation commands which is "as low as practicable." Consequently, arrangements have been provided in the implementation and the operation of the system including:

- Continuous checking of the validity of the data to be processed;
- Use of "2 scanning cycle" check procedures for the process data acquisition and transmission of orders or information;
- Issue of actuation commands is prevented if a fault is detected within CONTROBLOC.

Galvanic isolation of the inputs and outputs is another important feature of CONTROBLOC safety. The inputs and outputs of a CONTROBLOC cabinet behave as effective barriers between the electronic modules which use low level signals and the hostile plant environment.

The requirements for adaptability for subsequent developments of process operation and the capability of performing new control functions are easily satisfied on account of the use of EPROM memories which store user programs. The many microprocessors which are used in the CONTROBLOC have the capacity to perform the wide range of logic and analogue calculations which would be necessary if plant automation were increased.

The implementation or modification of a system by staff unskilled in electronics and data processing techniques is a very stringent design requirement. The need to allow hardware configuration to be defined by unskilled personnel has caused the CONTROBLOC system designers to organize it around a structure (cabinets, racks, power supplies, etc.) able to receive functional modules mounted on printed circuit boards. CONTROBLOC has a high modularity. Each logic module has a specific function and is operated by a dedicated program. Consequently all internal connections of a cabinet are systematically made the same during design and hardwired on printed circuit boards.

In order to program the EPROM memories easily, a CAD system is used to create the electrical diagrams. These diagrams are automatically translated into logical equations and, after verification, are transferred onto EPROM's.

Application programs can be modified, and during modifications, a CONTROBLOC cabinet continues running. Due to the internal redundancy of the electronic unit, it is possible to separate the unit to be modified to carry out the program modifications and to test the modifications on the cabinet itself.

3.2.3.3. CONTROBLOC layout in a 1 300 MW nuclear power plant

A 1 300 MW PWR nuclear power unit has about 1 000 remote controlled actuators, 2 000 logic and position sensors, 600 control devices, 3 000 alarms, 600 analogue signals and has to deal with almost 6,000 data items to be transmitted to the unit computer. Figure 4 shows a schematic layout of the CONTROBLOC function.

80 to 100 CONTROBLOC cabinets are required to process the relevant data. These cabinets come from three families:

1. Automation cabinets

These cabinets receive logic data from the plant or the control room; they generate orders for actuators and alarms for the main control room and the unit computer. All actuators controlled by these CONTROBLOC cabinets are operated and supervised from a main, centralized control room, except those located in the nuclear auxiliary building (for the first 1,300 MW unit) and
in the demineralized water control station, which are operated locally and supervised from the main control room.

2. Common data cabinet

Some data concerning either status conditions of the nuclear plant or controls (e.g., acknowledgement of alarm horn or alarm lights) must be distributed to a large number of automation cabinets. This data is acquired or processed by three cabinets designated "common

FIG. 4. A schematic layout of the CONTROBLOC function in French 1300 MWe PWRs.
data cabinets" and transmitted through multiplexed links to all automation cabinets, which all receive the same data three times. The receiving cabinets then process this data in two out of three modes. Triple transmission of common data has been retained to allow the system to tolerate the loss of a cabinet or a multiplexed link.

3. Alarm management units

The alarms requesting immediate operator action are indicated by lamps connected, wire by wire, to the automation cabinets while others are displayed on VDU displays. The switching of alarms generated by a given automation cabinet to a given VDU is performed by a set of two CONTROBLOC cabinets, one devoted to the train A alarms, the second devoted to train B.

Seven polychrome VDUs are mounted in the main control room; six display all alarms included in the plant. The seventh VDU, used only as an alternative, displays alarms of safety B train systems.

3.2.4. Protection systems

The protection applications of computers is evolving, and no representative architecture can readily be identified. Some generic features can be identified as follows: [23, 24, 52, 53].

1. Protection of the reactor requires redundancy, and generally, a two-out-of-four approach is needed.
2. Dedicated input systems, separated into four channels (for a 2/4 system), are required.
3. The highest industrial quality hardware is needed.
4. The application of fail-to-safe design principles is often required in individual nations.
5. Self-testing on-line is normally included.
6. Automatic off-line testers for all basic functions are normally included, with appropriate safeguards on operation.
7. Specialized software is required, held in ROM or similar permanent memory.

A representative three-channel configuration is shown in Figure 5.

3.3. INFORMATION SYSTEMS AND OPERATOR AIDS

3.3.1. Information systems in the control room

The design and technology of NPP control rooms have been developed on the basis of the rich experience with the control rooms in conventional power stations [13, 19].

Considering recent NPPs, VDUs are commonly used in the control room for monitoring data in conjunction with the conventional panels [51, 54]. This may be characterized as a hybrid information system where the operators are using the traditional and the new information tools as well [55]. In reality, the solutions arise from using VDUs as additional information sources as compared to fully integrated designs where the plant must be shut down if the VDUs fail. Alternatively, a strictly limited set of independent instruments and alarms may be provided, sufficient only to allow a safe shutdown operation if all VDUs and computer services fail for longer than a defined period, typically of a few minutes.
Process computers have been used for a long time in order to provide monitoring and surveillance of the plants, e.g. to print important alarms and disturbance messages or to provide various types of calculations such as flux distribution or core power. With the advances in computer technology on the one hand, and with the new information requirements (as described above) on the other hand, today integral concepts are more and more introduced, which try to meet information needs of operating, maintaining and managing of the plant as well.
3.3.1.1. Information presentation methodology

In early applications, only one or two VDUs, together with other instruments and alarms, were used. The VDU can relate directly to the working controls. If it fails, the conventional instrument can generally be used. However, the VDU must be operated on a page-by-page basis.

Recent approaches apply grouped VDUs and this offers several advantages [56]:

1. A single process can be simultaneously displayed in a number of different ways. This makes the information more accessible, thereby facilitating understanding of the actions of complex I&C systems.

2. This multiple-screen presentation of the same function increases the fault tolerance of overall information output as, on the basis of experience, it is relatively easy to identify single failures within the information as a whole. This allows the capability of the human brain to identify any contradiction.

3. The most important information can be moved to the centre. Information to be observed only sporadically can be positioned at "parking spots" around this central information. A "quasi-window technique" allows overview formats to be displayed at the same time as detailed subformats. The large size of the displays permits multi-person viewing at the same time.

4. Those visual display units which are not used in undisturbed operating conditions, can automatically display menus of suggested formats as pointers to "off-design behaviour" in the event of sudden disturbances.

A whole range of different features can be provided to allow rapid and easy access to the entire range of stored information. These include single formats as well as direct selection of sets of formats and direct access to neighbouring information and to hierarchical, extra information via the formats themselves. Of particular importance is a large range of possible types of presentations, and well-designed controls for selecting information.

Experience shows that there is a limited number of fundamentally important formats ("key formats") which are required in most situations. Such single formats form a part of or supplement to the multi-screen format sets and give the required information a particular transparent form. To ensure that the displays are designed effectively, the design team should include direct representation of the ultimate operating staff and also should directly include designers with human factors and ergonomic experience [51].

3.3.1.2. Experience with VDU systems in control rooms

When discussing the VDU information technique, it is important to note that they do not simply replace conventional means but rather enable new ways for basic improvement of plant monitoring. In general, there are two types of presentations:

- System overviews with a hierarchical structure leading the user to more and more detailed information down to the component level.
- Task/function oriented displays which provide comprehensive information about the status and dynamic behaviour of the processes to be observed, e.g. by means of diagrams.

Both types of presentations open up a new dimension of information. The first one enables rapid and easy access to information when tracing back a problem through the system involved. The second one provides a closer contact between the operator and the overall plant behaviour and provides a more direct contact with the processes (e.g. control actions and their influence on the
process) which could not be achieved by the former information means. More recently it is supplemented by a display presenting advice on how to cope with a faulty situation.

Operators must be able to track operation of the plant, and likewise, all situation and event sequences for plant faults so that they are always completely informed of all processes involved. This enables them to take manual actions where appropriate, for areas where this is admissible and to supplement the automatic counter measures. Shift supervisors and specialists require additional, widespread and varied information.

In case of system operation with safety relevance, the operator has to rely on the information provided on the VDU. In some countries, information must be shown with colour to enhance clarity, and with a symbol or other indication that a change has taken place in the state or value of a plant signal. This is done both to provide indications with safe properties, and also to ensure colour vision impairment is not challenged. Where information is presented which is derived from redundant sensors, it is normal nuclear plant practice to provide VDU screens with all values arranged together, to allow comparisons to be made, and also to provide screens which show only the averaged value, with dynamic rejection of faulty signals using an appropriate validation algorithm. Where redundant contact sensors are provided, algorithms have been used, and are being developed, which will detect discrepancy between the states and, where appropriate, will prevent unsafe action then being demanded by the operator. An appropriate algorithm is described in Ref. [85].

There are certainly various stages concerning the application of VDU systems in the control room. At present, VDU information is often used in addition to traditional information. Although this seems to be a natural first step, very often there are complaints with respect to even more information overload for the operator.

First experiences in Germany have been reported by the utility BAG [57]. The most important outcomes are given below.

(1) Automation

The degree of automation is ultimately determined by the safety requirements, operational needs, and the natural limits of human capability. From the point of view of human factors engineering and systems ergonomics, concerns are often expressed with respect to decoupling of the operators from the process. The experiences reported show the opposite:

- The additional VDU information system provides an essential means for fully understanding complex process situations; it forms the basis for integrating the operator into the world of process automation.
- The extensive process automation represents a considerable amount of the I&C knowledge complex. This knowledge has to be trained and adapted and comprises more than 50% of the operators' teaching and training experience.

(2) Parallel and serial information presentation

Traditional control rooms provide a good overview because of parallel stationary presentation areas of distinct information type. This may be lost by the window-type of information presentation as given by VDUs. The findings have been:

- The VDU system showed the ability to replace the overview function mentioned above to a large extent by means of overview pictures;
- Since VDUs have been grouped into units (e.g. six VDUs in two levels on the console, for each of the turbine and the reactor operator) disadvantages of serial presentation are highly compensated. Several windows to the process are available at the same time. The mental
Requirement for picture and diagram selection was relatively low due to hierarchical structures and menu selection.

(3) **Plausibility checking**

Plausibility checking of highly-condensed information is often considered a major problem when using new information systems. It is assumed that this may lead to decision lags:

- According to the reported experience, plausibility control with the VDU system provides many more possibilities than with the traditional system. It is believed that the high potential of plausibility control is far from being exhausted.
- Future systems can be extended to even wider plausibility control by comparing measured signals with values calculated by on-line computation (analytical redundancy). It is recommended that the design should provide measured values instead of calculated as a prime information source for the operator. When grouping or calculating information, care must be taken to ensure that the algorithms operate satisfactorily if a signal is defective or a scanner subunit is out of action.

(4) **Participation of the operators in design and training**

The participation of the operators in designing the information presentation is essential for later acceptance. Training means for the new VDU system have to be provided:

- Operators have been integrated into the design process at an early stage. Even after putting the system into operation, the team consisting of engineers from the vendor and the utility remained working.
- This team still formulates improvements and new requirements. A trend to ask for even more information about automatic action and their influence on the process can be observed.
- The expectation with respect to the operators’ acceptance of the VDU system has been fulfilled.
- Training of the operators must consider the new information system.
- A specific simulator (called a function trainer) is used in order to provide operators’ training in addition to the on-site training.

(5) **Verification and validation**

Although the VDU system is used as an additive system, major V&V actions had to be performed within the licensing procedure. This was due to the fact that safety-relevant information is also given by the VDUs.

- Since national NPP standards for this subject are not yet available, a guideline has to be developed based on present national and international experience.
- In the past, application of validation to existing systems has led to considerable additional expense and licensing delays. Software V&V procedures should be considered carefully, and determined so far as practicable, in the beginning of planning.
- Software costs present a more and more dominant percentage of the total system costs of the first unit; more than 70% has been attributed to software in some cases, with rising tendency.
- Hence, the portability of software is an essential requirement of the utilities, especially considering the short innovation time of hardware. During the life time of the NPP, the hardware will need to be changed several times.

(6) **Hybrid information system**

In order to facilitate introduction of the new VDUs, the intermediate step of a hybrid solution has been adopted in some countries (i.e. the VDUs additive to a complete conventional control room), with three main points in mind – to ease adoption by the operators, to learn lessons and to
gain experience without impacting production and to better overcome licensing problems. Experience showed:

- The hybrid solution did not lead to undue operator load.
- The design solution found provides an optimal combination of traditional and advanced information systems.
- V&V and licensing can be gradually developed from operational systems to safety systems (e.g. SPDS).

### 3.3.2. Operator aids

In regard to operator aids, it is common practice for information features to be introduced as additional sources to those already available in the control room [14]. They date back to the TMI-2 accident, where serious information deficiencies were observed, as a consequence of which the idea of symptom-oriented procedures came up. These procedures were meant to be as simple as possible and clearly directed towards a few definite safety goals, which have to be met in case of accident situations (e.g. adequate cooling of the reactor core, primary circuit integrity). The information system to comply with this procedure was the SPDS (Safety Parameter Display System) [5,6,8,58]. Its purpose was to indicate deviation of the defined Safety Parameters and to provide the subsets of important measurement values in order to assist the operator in reaching the safety goals [59,60]. The world-wide impact of the TMI-2 accident has resulted in the widespread adoption of similar SPDS functions in other countries. The installation of computers and colorgraphic workstations is matched by the development of sophisticated application software modules, such as signal validation software to be used as a preprocessor for the SPDS and emergency procedure monitoring, to integrate the rule-based control functions with the SPDS.

From then on, further development has been driven mainly by two factors: the desire to provide additional help to the operator which goes beyond pure information; and second, the experience that operator aids which are practically never used for accident situations creates training and acceptance problems. Concerning the first factor, additional features like success path monitoring or status monitoring of safety-relevant equipment have been provided. The second factor caused extension into the normal operation regime; consequently, the operator aid system was used in the normal working environment and acceptance was achieved. Further, once this important problem had been solved, it was no longer necessary to switch from one information means to the other dependent on the operational regime [9].

Besides this main line of development, special aids have been developed and successfully used for operating purposes only. Among them are advisors for load following control, secondary feedwater control during part load operation, or assessment of Xenon poison and reactivity margins [45, 46].

### 3.3.2.1. Diagnosis and prognosis

The enhancement of man-machine interface by means of VDUs accompanied by new forms of information presentation is just one step. With the rising power of process computer technology, the tool was there to produce on-line high level information and to improve and condense information at the same time. Among the new features, diagnosis and prognosis play an increasingly important role. This is because knowing about plant deficiencies at an early stage provides the maximum time for adequate measures. Corresponding to the operational needs, two main areas can be distinguished:

- aids to diagnosis arising during abnormal deviations of the plant process and for prognosis of the further development of these deviations;
- aids to diagnosis of the onset of mechanical deficiencies and for prognosis of further development of these deficiencies.
Processes

The origin of process diagnosis and prognosis dates back to disturbance analysis systems which have been investigated and developed since the 1970s. The basic idea of these systems was to assist the operator [61,62]:

- in tracing back a disturbance of the plant (which as a rule is indicated by alarm messages accompanied by a bulk of analogue readings) to its origin, the cause of the disturbance;
- by providing information about potential developments of the disturbance; and
- by providing recommendations for adequate countermeasures.

All these developments were considerably hindered by access problems to the sensor signals, poor dynamics of digitized values (available via the plant process computer) and last but not least, by the effort needed for system and process analysis. Yet, successful working of prototypes could be demonstrated, partly in on–line experiments [63]. Subsequently, these systems were further developed and led to integral concepts within the framework of advanced I&C and enhanced control rooms.

Today, the main goal of those systems has switched to diagnose a process in terms of initial deviations from the normal state, i.e. to inform the operator about a developing disturbance before reaching the traditional alarm levels. This calls for intensive analysis of the dynamic process and systems behaviour so that the temporal development of the measured variables and their mutual interrelation can be reliably interpreted. Possible presentation to the operator can be achieved, e.g. by a transient diagram [64]. This diagram shows the distance between actual process variables and the defined limit values as well as denoting the time available until a limit value is reached in the course of transients. In the specific case, the graphical representation has been developed to monitor transients regarding the three ways of heat transport on the secondary side of a PWR (turbine/condenser, steam generator, relief/safety valves). For this purpose, distances and time residuals are computed and ordered for those process variables that have some effect on the current heat transfer path once they have crossed a threshold and are approaching the trip level. This gives the operator information about competing or mutually influencing factors of a jeopardy regarding the respective heat transfer paths. Twenty relevant variables have been selected. Beginning with the actual value (fixed marker line), the transient is mapped 30 minutes into the past and an extrapolation of 15 minutes into the future is performed.

Enhanced diagnosis abilities are available now in various new information concepts, e.g. in the advanced control room designs in France, Japan, and Germany [49]. Experience is young, but operators adopt the new information possibilities and, after the adaptation phase, recognize the advance in information and prefer the new system as compared to the old one.

(2) Mechanical systems and components

Similar to the systems discussed above, a lot of development work had been done to provide diagnosis and prognosis features for the mechanical health of the plant. In the past there was little or no direct information on this for the operator. Rather, he had to draw his own conclusions from the process behaviour supplemented by just a few sensors indicating the status of active components (e.g. turbine vibration). Since the 1970s, more detailed investigations have been performed in France, Germany and the USA on diagnosis for loose parts vibration of reactor vessel internals and leakage in the primary circuit. Indirect measuring methods and subsequent diagnostics techniques have been developed based upon acoustic, vibration and process signal noise analysis [65].

Typical of the methods applied is the use of stochastic signal information. Therefore, considerable effort had to be placed on signal analysis and interpretation as compared to the usual reactor instrumentation. Depending on the problem, either analysis in the time or frequency domain
is applied. Very often essential information is drawn from the interrelation between different signals (correlation analysis, pattern analysis). Especially for successful application of vibration diagnosis, extensive knowledge of the vibrational behaviour of the observed mechanical systems is necessary. Therefore, adequate pre-operational vibration tests which may require additional sensors and theoretical model studies had to be performed. Also, databanks storing relevant events are necessary in order to allow for comparison.

Meanwhile, loose parts monitoring systems are installed in nearly all light water reactors [66]. Regular vibration and leak detection analysis are applied to most of the PWRs. Loose parts in the reactor vessel or steam generator can cause structure damage, especially when they remain undetected for a longer time. Excessive mechanical vibration fatigue effects may cause breaks or loosening of screwed connections. The detection of these deficiencies is important from the operation and safety point of view.

3.3.2.2. Experience

As indicated above, operator aids provide special information or guidance to the operators. Typically they are realized as stand alone systems, or where sufficient on-line computer power is available, the additional information features are integrated in existing control rooms [67]. In recent designs, which are based on flexible, distributed, computerized I&C, these aids have been considerably extended and, from the beginning, integrated in the overall information concept [4]. Design aspects of these integrated systems are:

- task-oriented information, if feasible automatically following the actual plant situation;
- transparency of information, i.e. the operator receives full information on how and why the information systems derived its conclusions; and
- assurance of information validity and consistency, e.g. by on-line signal validation.

The experience with the operator aids used up to now are positive. They have achieved their main task, i.e. to save time in understanding complex situations and processes and to act in time. As a result, human error has been reduced. Flexibility for adaptation to task extension and upgrading is obvious. Problems still exist with integration in the overall information system and with verification and validation (V&V), not only due to computer hardware and software reliability, but also due to V&V of the underlying information condensation, which tends to become more and more complex.

Good experience has been gained with diagnosis systems for mechanical components in many countries operating nuclear power plants. Among important findings are excessive core barrel vibrations due to relaxation of the clamping conditions, loosening of the secondary core support in the reactor vessel, loosened internals in the steam generator, etc. Loose parts monitoring has been successfully applied in French and German plants. There is no doubt the systems have paid off [68].

In spite of successful operation, further development is necessary. One of the most important problems which still exists is the operation and use of the systems on site. Typically, measurement results are stored and investigated by specialists in analysis centres. This certainly leads to decoupling of the operating staff from the systems and often results in acceptance problems. The future tendency is to perform more analysis work in an automated manner on site and to generate condensed information which is easier understood by the staff.

One example pointing in this direction is a German condition monitoring system called COMOS [44]. It is used for on-line vibration analysis, and allows automatic simultaneous monitoring of up to 32 signals. In the spectra of each signal, up to ten frequency bands with adjustable band width can be determined. Margins are set individually around learned reference states. The trends of the different features are displayed graphically. They can easily be followed by the operators; set points can be introduced and used in the control room for triggering an alarm.
As a consequence of this on-site analysis feature, COMOS can also be used to monitor possible fast escalating deficiencies, e.g., when using it for pump shaft vibration monitoring. This is described in the annex.

By means of a new information correlation matrix, rules for vibrational relations in various signals and frequency bands can be programmed to realize diagnosis and prognosis properties. Step by step the comprehensive and still growing knowledge-base can be implemented in the on-line monitoring, so that in the future a diagnosis and prognosis system for vibration and anomaly monitoring will be available. The system is installed in 7 German PWRs with a successful operation experience of 20 reactor years.

This is just one example of how even complex systems can be successfully applied on site. With the new powerful I&C systems now available on site, which typically have available a considerable computation capacity, similar developments in other diagnosis and prognosis applications will become available in the future.

3.4. CONTROL AND AUTOMATION

3.4.1. Automatic control functions

Analogue control modules were used on early nuclear power plants. However, they are now not generally available due to commercial obsolescence. Since the early 1970s, the availability of computer modules able to be configured for a three-element (proportional-integral-derivative) control has allowed their use for the simpler control functions not related to safety.

This use has grown, and more complex, non-linear control functions have been progressively included in nuclear power stations. A wide range of standard firmware modules are now available for such applications. Computers have been used for distributed digital control (DDC) with great success in some countries since the 1970s. The advantages of using DDCs are flexibility of control strategy and it allows integration of control parameter schedules, giving wide control ranges. The extensive non-linearities of behaviour of the plant can be covered in this way, for example, the transfer from startup feedwater control to the main feedwater control mode at a power of about 10% [69,70].

An advantage of computers for gas cooled reactors has been the ability to provide DDC for the separate automatic control of up to 40 control rods used for control of channel gas outlet temperatures. A typical application is described in detail in the annex for the United Kingdom Advanced Gas-Cooled Reactor at Torness. The control functions needed to maintain station conditions of coolant temperature, steam generator level, feedwater flow etc., are recognized as having a role in safety since they maintain the reference conditions used by all safety analysis studies. They may have trip function in control of heat removal. The use of computers for such control functions, therefore, may involve justification of their performance as suitable for a safety-related function.

An interesting and important development in the application of computers is the operation of actuators controlled by the station control functions. The control of turbine power on a modern plant will involve the use of a microprocessor turbine governor controller whose setting is altered by the station power control loop. The operation of control rods for recent PWR designs involves a microprocessor controlled rod movement and sequencing system. Control of reactor coolant temperature, therefore, involves transmitting demands to this control rod microprocessor system.

3.4.2. Sequence and interlock control

A successful application of computer control on most modern nuclear plants has been the automatic run-up of the turbine, its synchronization and its initial block loading. This is normally a
system provided by the turbine manufacturer and its use is necessary to ensure satisfactory operation of the turbine for all temperature conditions.

Turbine run-up control has a wider character than a pure sequence since closed loop speed and acceleration control is used within the run-up sequence.

Control of refuelling is a standard application, in which a computer or a Programmable Logic Controller (PLC) is used to position the fuelling machine, operate its hoist and grab, and move the fuel to its fuel pond storage location. On some fuelling systems control applications, interlocks to prevent moving the fuelling machine during its operation, to prevent movement to specific locations, and to ensure the fuel assembly is submersed, are required. This can be implemented through PLCs; however, great care is needed. If a potential activity release could be caused by a PLC malfunction, a detailed safety justification of the computer may be needed.

The use of computers to assist operators by automation of startup of nuclear plants is less widespread than for other classes of power generation, since nuclear plants are generally operated for base-load generation over long periods. However, often the closed loop controllers are designed with schedules to allow automation of aspects of startup over a wide range.

On two advanced gas-cooled reactors built during the 1970s in the UK (Hartlepool and Heysham 1), a complete automatic startup system has been integrated with the station automatic control functions. On these stations, startup from below critical to about 30% power is normally under computer control, followed by full transfer to DDC of the station power and reactor conditions. The startup brings the reactor from zero power to criticality, then increases temperature and power, controls the boiling in the once-through boilers, and initiates turbine rundown and loading, in several phases. The system is used as a matter of routine on all startups.

For automatic control, the configuration of the computer system to ensure availability is important. Dual computer units, with automatic changeover, were used on earlier stations with DDC. All control functions were generally integrated in one mini-computer system. Modern micro-computers systems have distributed the functions, with a dual micro-computer subsystem for each control loop [70]. The computer system typically includes a local area network (LAN), or a set of direct data links, to take messages from the control computer to the display and alarm computer. The LAN will normally require redundancy, to ensure high availability, and this will allow a full check of all messages sent.

Interlocks on the operation of plants may be needed to ensure, for example, correct valve positions and lubrication when a pump is started, to prevent high pressure fluid entering low pressure pipework, or to prevent radioactive fluid contaminating clean fluid. Such operations have normally been done by conventional wiring of limit switches and position switches in the control switchgear, or by the use of equivalent solid state logic. PLCs or computers programmed with standard logic functions can achieve these interlock functions, and this application of computer equipment is increasing. A wide range of industrial PLCs suitable for these functions is commercially available.

3.4.3. Integrated control and multiplexing

An application of computers which is becoming increasingly important is the multiplexing of control room controls. A computer system controls a local area network (LAN), to which are connected input/output multiplexing units which read control room switches, and operate plant actuators and switchgear. The multiplexing equipment can be physically distributed. Cubicles in the control room area communicate control demands by optic fibre or coaxial cables to cubicles in the electrical switchgear rooms or at plants [71, 72].
The advantages of this approach are that:

1. very extensive cable savings are possible;
2. safety can be improved, since the potential for incorrect action caused by a cable fire can be eliminated; and
3. total electrical isolation of plants from the control room is possible by use of optic fibres.

If a control multiplexing system also monitors plant signals, and is used to provide information to the alarm and display system, the displays can include full information on control switch states. A further advantage is that automatic records can be made directly from the actions taken in the control room for analysis after an incident.

The computers used for such multiplexing normally are internally redundant, with a redundant LAN system. The very high possible availability allows the same network of multiplexers and computers to be used for automatic control and interlocks, giving integrated data collection and automation. To allow for the fire separation needed on a nuclear station, two or more separate multiplexing systems are needed, with the equipment and LAN cables of the two systems separated and electrically isolated from each other.

An important extension of the use of multiplexing is the use of touch-screen control. In this approach, VDU screens are selected by the operators. These screens show control areas. Touching specific areas of the screen will activate 'open', 'close' or 'start', 'stop' actions, with confirmation of the selection by touching a further area of the screen.

If a multiplexing system is used for control, it is important to assess its significance to safety. If safeguard plants are controlled which are also operated by the reactor protection system, the multiplexing equipment may form part of the safety system and the special factors concerned, which are discussed in Section 3.5, must be considered. It is also important to consider carefully during design, the separation of control and data which is important to safety from other controls and data. Software and hardware isolation is needed to a suitable extent such that corruption of safety system control or data cannot take place.

3.5. PROTECTION SYSTEMS

3.5.1. Introduction

Reactor protection and safety actuation systems have been developed on the basis of analogue modules to detect unsafe conditions, and logic modules to vote on those conditions [73]. Many early systems depended on industrial trip amplifiers and relays to perform voting on a one-out-of-two, two-out-of-three, or two-out-of-four basis.

The need to demonstrate safety resulted in the use of high quality special designs of analogue and logic modules. The high availability required and the need for reduction of spurious trips has led to a general present day requirement for two-out-of-four, and in special cases, three-out-of-four voting. Solid state equipment is standard, and some countries require equipment which has been designed to be fail-safe.

To allow the highest possible reliability to be claimed, some countries have included a method of diverse automatic shutdown, using relays or some alternative equipment, in addition to a solid state protection and safety actuation system.

The increasing complexity of the protection requirements has resulted in several nations considering the use of software-based protection systems. These have generally been based on the use of standard microprocessors and computer input/output cards.
The confidence needed before a designer or utility has been prepared to consider computers for protection has only been possible because of the successful experience of computers for data display and control applications. In spite of this, major problems remain in the application of computers for safety functions.

3.5.2. Representative systems

In spite of obvious advantages when using computerized protection systems (e.g. calculation of more complex parameters, adaptation to plant changes), the required reliability level and V&V problems have caused considerable delays in applications. Today, fully developed systems are in operation on some PWRs, CANDU and other reactors. In the following, examples of digital protection systems are briefly described.

3.5.2.1. Integrated digital protection system

The 'integrated digital protection system (SPIN) for 1 300 MWe nuclear power plants of EDF is intended to produce an emergency shutdown of the reactor on detection of critical parameters outside normal operating limits and to initiate suitable safeguard actions in the event of an incident or accident situation.

SPIN receives electrical signals (analog, logic or digital) representing the boiler quantities monitored (physical parameters, neutron flux parameters, position of control rods, etc.) and outputs control signals to emergency shutdown circuit breakers and safeguard actuators. It comprises four redundant Acquisition and Processing Units for Protection (UATP) and two redundant safeguard logic units (ULS) to which an automatic tester is added for periodic tests, as shown in Figure 6.

1) Acquisition and processing unit for protection (UATP)

The UATP, as shown in Figure 7, performs all the processing required to generate the protection function tripping commands, i.e.:

- Acquires the sensor outputs,
- Processes these signals,
- Compares the computation results with the reference levels to obtain tripping information per parameter,
- Exchanges this tripping information between the UATPs,
- Performs logic processing on two out of four (2/4) of the information for each parameter,
- Generates tripping commands either directly to the emergency shutdown switches or to the ULSs for safeguard actions.

This processing is performed by 8-bit microprocessors. The UATPs are microprocessor-structured and comprise two types of independent units:

- Seven functional units (UF) which perform all of the digital and logic processing relative to monitoring of one or several parameters.
- Six exchange units (UE) controlling the multiplexed links for partial trip information exchanges between the UATPs or transmission of information to the outside of the protection system, in particular, for centralized signalling and information processing.

Each Functional Unit and Exchange Unit can operate independently and is entirely asynchronous with respect to the others. The information exchange between the UFIs and the UEs takes place through a shared memory network.
FIG. 6. Architecture of the French integrated digital protection system (SPIN) for 1300 MWe PWRs.
(2) Safeguard logic unit (ULS)

Each ULS, as shown in Figure 6, is associated with a set of safeguard actuators. It acquires
the trip commands from the four UATPs (safety injection, containment isolation, etc.) and combines
these for 2/4. It then performs various logic processing relative, in particular, to acknowledgement
of manual controls.

Functional units

Exchange units

- UATP inhibition logic

- Hardwired logic

Digital signals

Logic signals

FIG. 7. Structure of protection acquisition and processing unit (UATP) in French 1300 MWe
PWRs.
Finally, it generates individual commands for the safeguard actuators. The cables of the UATP and ULS are separated to maintain the integrity of the four protection channels. To avoid unintentional tripping in the event of failure of the equipment on one hand, and to allow periodic operating tests on the other, each ULS has two identical logic subassemblies whose output is 2/2 combined, prior to controlling the actuators.

(3) Tester

The periodic tests of the SPIN required by administration rules are performed, using an automatic tester. This tester, built around a minicomputer, is normally disconnected. To perform the periodic tests on a UATP, the tester is connected to the UATP whose input is then controlled by the tester.

The tester applies a series of input configurations and checks that the UATP processing results match the expected values. The tester can also perform a periodic test on a ULS logic subassembly. The periodic tests on the safeguard actuators require special precautions and are performed manually for this reason.

3.5.2.2. Integrated protection system

A computer-based reactor protection system called the 'integrated protection system', has been developed by Westinghouse in the USA. It is used as the primary protection system (PPS) for Sizewell B PWRs in the UK [23,24,53]. The PPS provides reactor protection for all design basis faults. For all frequent faults of the design basis, an additional solid state protection function is provided by the secondary protection system [73] to ensure that the overall probability of failure to provide protection is sufficiently small. This provides diversity of protection as well as redundancy. The structure of the PPS is based on four redundant channels, with two out of four voting for reactor trip, and for reactor engineered safety features (ESF) operations. The voting is performed for each parameter individually, within each of the four protection channels. The architecture within a channel keeps a partial separation between two groups of trip/ESF parameters, so that protection is still normally possible if one main processor within the channel has failed.

The primary protection system is provided with a comprehensive automatic testing unit, one for each channel. Interlocks and automatic time lockouts restrict the use of the automatic tester to one protection channel at a time. During that time, the input signals are disconnected and the inputs taken from outputs of the automatic tester. The automatic tester then checks to see that each parameter will provide a satisfactory trip or ESF operation.

The hardware and software of the primary protection system is extensive. The hardware is based on Intel and Westinghouse units. The software has been subjected to extensive and comprehensive internal V&V by the supplier, and to review on a line-by-line basis by NNC for Nuclear Electric [74]. In addition to this review, the hardware and software has been subjected to an Independent Design Assessment by a specialist unit within Nuclear Electric. No use was made of Formal Mathematical Methods during design, but the functional documentation and detailed logic were reviewed in detail to ensure satisfactory interpretation into the software functions. To ensure the software is fully accurate, the independent design assessment process included the use of a software code analysis tool, MALPAS [75], which is used to confirm all potential logic actions of the code. An extensive set of test runs was done on a statistical basis against simulated operational transients using a one-channel prototype [76].

3.5.2.3. An inherently safe automation trip system

The 'inherently safe automation trip (ISAT) is a computer system developed by the UK Atomic Energy Authority for the Dounreay Prototype Fast Reactor. It provides fast response protection from fuel subassembly outlet sodium temperatures. Comprehensive dynamic operation provides a fully fail
safe computer approach. The principle behind the ISAT is to use test signals interleaved with the plant signals, passed through the computer system to exercise the trip algorithm to give a known pattern of states, "healthy" from the plant and "trip" from the test signals. This pattern will change if the plant becomes unsafe or equipment fails. The pattern is matched with a reference pattern in a hardwired pattern recognition unit to detect unsafe plant or equipment failure states. The dynamic logic is continued through to the actuators since the output of the pattern recognition unit is itself dynamic. In normal operation the pattern recognition unit steps through the sequence of correct patterns, first obtaining a mismatch with the input pattern which causes the next expected pattern to be brought up to obtain a match. The approach is described in detail in Ref. [52].

This system has been installed on the Dungeness B advanced gas-cooled reactor (AGR) to provide reactor protection from channel gas outlet temperature conditions. Two thermocouples from each of 408 channels are each monitored by two subsystems, and a two-out-of-four trip on high temperature is produced by the ISAT system. A demonstration for the PWR protection functions of departure from nucleate boiling (DNB) and linear power has also been developed.

3.5.3. Experience

The major benefits of a computer system for providing protection compared to other methods may be stated as:

(a) Improved operating margins due to accuracy of protective functions, which may include computation of rate changes, calculations of power, or approach to boiling conditions, and logic of greater scope and complexity than was previously possible.

(b) Increased safety due to the hardware self-testing ability of the software, which can reduce fail danger possibilities significantly.

(c) Increased plant availability and fewer spurious trips due to the higher reliability of computer equipment compared to analogue equipment.

(d) The ability to include modifications of system data and software allows simpler and more effective inclusion of modifications.

(e) The computers can transmit detailed information from the protection system to the station display and recording computers, to give both input signals, internal states and actions taken.

(f) The systems can readily be designed to include automatic testers, with printed records, which allows higher quality maintenance to be achieved with less down-time.

The experience with computerized protection systems has been mixed. On the one hand, they have operated reliably and have done their job well. On the other hand, problems have been encountered in a number of areas [77,78] and have caused some countries to suspend work. A major problem has been the reluctance of Regulation Authorities to accept software systems [39,41]. The safety assessment methods used generally require reliability to be estimated and a typical random failure probability for a high quality hardware system of $10^{-5}$ failures/demands, depending on analysis methods and the treatment of dependent failures. However, software faults are systematic in nature and therefore can cause common mode failure. It is necessary to show reliability and dependability of the software to comparable levels of performance to the hardware.

A software fault can be introduced during the specification, design or implementation phase of the software, i.e. a fault is manifested deterministically in the code. When this code is executed the fault may be encountered, depending on the choice of input data for that specific execution (run). A software failure occurs only if the fault is encountered. Encountering a fault is a random event in
most cases, as a single execution normally uses only a small part of the input space.

It is generally agreed that software has no random failure property. Its common mode failures can be considered to be due to the number of errors in the design or in the final code. However, a level of better than one fault in 10,000 lines of code can only be achieved by the most careful quality assurance (QA), independence of verification staff, independence of validation staff, and the most careful documentation, coding and site testing [23,74].

The requirements for documentation and the technical factors to be considered in the production of the code are defined by the Standard IEC880 - Software for Computers in the Safety Systems of Nuclear Power Stations [21]. Although this standard provides an important reference point, it does not discuss in detail subjects such as the validity of the language used, code analysis tools, the use of software preparation and configuration control tools, the data used to define software functions, or the use of Formal Mathematical Methods. All of these aspects have been found to bear strongly on the software freedom from potential error, and must be taken into account for any software important to safety.

IEC880 stresses the importance of independence in the verification and validation (V&V) process, and goes into detail on the degree of verification needed. It is generally recognized that the cost of removing an error is up to 100 times less if it is detected during design rather than on site. There is, therefore, a strong incentive both for economy and for safety in establishing an effective clearance of each reported error early in the design and implementation process. Some of the steps necessary for qualification of software for use in safety systems are outlined in Section 5.4.3.2.

The methods of on-site demonstration of correct functional performance used for data display and logging systems have generally involved signal injection, confirmation of each display, and checking of each action. For a reactor protection function, these methods must be used with care in order to give a 100% coverage for tests of all input signals and all output functions. The specific logic operation followed for each trip and safeguard action requires testing and demonstration, both by signal injection after installation, and also with the final plant during commissioning. Part of this process, following the experience with past data processing and distributed digital control (DDC) systems, must include some form of endurance test in which the system is exposed to the behaviour of the actual plant prior to operation. Simulations of random plant transients may be needed for the highest confidence in the correctness of the software [76].

4. COMPUTER APPLICATION TO MAINTENANCE OF NUCLEAR POWER PLANTS

4.1. INTRODUCTION

Computers are used as a "tool" to assist with the management of information, and thereby enhance the maintenance of NPPs. A structured storage of history and knowledge builds up an information resource enabling the administrative organization to be more effective, providing the staff with access to common information directly. Data needed for computer applications for maintenance comes (in part) from the process computers. It is essential that the information system computers are not allowed to corrupt the performance of the process computers.

"Maintenance management" covers all aspects of maintenance, from the point where needs for maintenance work are identified, to control of the work, to final close-out storing of records (history) and analysis of the maintenance acts or events [79].

"Equipment performance applications" covers on-line monitoring of vibration, chemistry and inspection records, etc., which are used to determine the need for maintenance. In addition, such monitoring covers heat exchanger leakage and fouling, temperature, and flow variations, etc. Note that operators can use similar information (as in Section 4.1.5) for critical equipment to decide if a
NPP should be shut down (or must be shut down) e.g. vibration limits on a primary circulation pump.

4.2. MAINTENANCE MANAGEMENT

This section gives a general description of possible and existing integrated computer support for maintenance in the following manner:

- by defining and describing the basic functions of a computer support system as an integrated part of maintenance management;
- by giving examples on how it affects the organization, and the information exchanged between the organizational departments for maintenance, operation and administration.
- providing in Figure 8 an example of an information system structure.

4.2.1. Basic maintenance files

The basic maintenance files that are required are:

- Equipment files, work orders, preventive maintenance program, history, outage programs (pad locking, the umbrella function), work permits, technical specifications and maintenance procedures.
- A complete listing of all the equipment in the NPP, with each device having a unique device code. The device codes typically identify the unit number (if the NPP has more than one unit), the system that the device is part of, the type of device (pump, valve, etc.), and a unique device number.
- A cross reference from the equipment code to the material code, where the material code leads to the description of the assemblies and sub-assemblies installed in the NPP.
- Instrument calibration setpoints and calibration history.
- Detailed reports of all abnormal events that have occurred, including records of system transients, analysis of the events, recommendations and actions taken.

4.2.2. Maintenance administration/routines

Corrective maintenance and preventive maintenance programs require support from basic files including files for history, procedures and calibration setpoints.

When work is to be done on a device, a work order is initiated and the computer is used to store and process the information, and to provide a cross reference to the correct spare parts and procedures for the maintenance of the device.

When corrective maintenance work is to be done, a work order is also opened. A computer provides for rapid access to the history files for the devices. In many cases, the history files will enable staff to make more efficient preparations for the work to be done. Rapid access to the correct procedures and calibration data can also be provided. This is especially important as procedures and calibration settings may have been revised, and the up-to-date information must be made available immediately and must be used.

Computers also allow staff to search quickly for other work that can be done on the device (e.g. preventive maintenance), and to achieve more work under one work permit. The capability is also provided for operations and maintenance staff to follow work orders from the beginning to the end, allowing a better organization of the tasks to achieve improved productivity in completion of maintenance activities.
4.2.3. Outage planning

There is a close association and interaction between maintenance (work order), engineering (modification of projects) and operation (isolations, tagging).

Outages of a NPP present an opportunity to do maintenance work, but they also represent a loss in production of electricity. Therefore, it is essential to achieve as much work as possible, and to complete all mandatory work within as short an outage period as possible.
Computers provide staff with the capability to list all work that needs to be done (corrective and preventive maintenance, and changes to be made) and to acquire all material and equipment required. They are also used to perform resource level analysis, and to optimize the scheduling of work to fully utilize the opportunity for work to be done in association with predetermined functional equipment groups (or umbrellas) of isolated equipment.

These functional equipment groups are selected so that they can be isolated without contravention of the policies and procedures for safe operation of the NPP. Each functional equipment group can have a pre-prepared isolation (tagout) procedure, and all work that can be done on any equipment within the group is scheduled to be done at one time. Such work would include all corrective maintenance, preventive maintenance, and changes to be made.

Computers are used to assist preparation and control of the isolation (tagout) sequences which must be performed before authorization can be given to commence maintenance work. If major pieces of equipment in the NPP are identified with a barcode as a tag, a barcode reader can be used to confirm that the correct device is being opened or closed. The computer can also record the state of each device used for isolation, marking this information on the plant and instrumentation diagrams. Figure 9 is an example of the information modules used in outage planning.

---

![Diagram showing information modules for outage planning](https://example.com/diagram.jpg)

**FIG. 9.** General arrangement of information modules for outage planning. Ringhals Information System (RIS), Vattenfall, Sweden.
4.2.4. Materials management

It is essential to meet the specific demands of a nuclear power plant to use the correct spare parts at all times.

Computer systems are used to link the equipment device codes with the spare parts list, to maintain up-to-date specifications for the spare parts, to manage the purchasing and storage activities of spare parts, and to create records on the use of spare parts.

It is necessary to use the correct spare parts to ensure that the NPP continues to meet the design specifications and requirements. It is necessary to have the correct spare parts available at the right time to permit work to be completed on schedule.

Each piece of equipment in a NPP should have a unique equipment code identifier. This code must be linked to the design specifications for that piece of equipment. There must also be a cross reference to the material code, where this code defines the actual physical device that has been installed. It is essential that the technical characteristics of the actual device (defined as a subset of the material code), equal or exceed the requirements of the design specification (defined as a subset of the equipment code). Figure 10 is an example of the information modules used in material administration.

4.2.5. Maintenance support functions

Computers are also used to provide a maintenance support function by giving staff quick access to information they need. This information is in areas such as: current radiation doses for staff; radiation hazards and levels in the NPP; qualification requirements for specialized work; qualifications records of available staff; cross reference to supporting documentation. By making this information

![Diagram of information modules for materials administration](image)

*FIG. 10. General arrangement of information modules for materials administration. Ringals Information System (RIS), Vattenfall, Sweden.*
available to all staff at the time they need it, there is greater assurance that maintenance work is done effectively and efficiently.

4.2.6. Other administrative functions

There are a number of administrative functions that are computerized and form a subset of maintenance management.

Personnel-related systems deal with shift schedules, minimum approved complement scheduling, qualification of staff, personal accounting during emergencies, approval of training and vacation periods, etc.

The management of the documentation defining the operating and maintenance procedures is of great importance to the continued safe operation of a NPP. The content of these procedures must be consistent with licensing and regulatory documents, and they must accurately describe the systems and devices actually installed in the NPP. The procedures published for use by staff must be current, correct, and authorized for use. To continually maintain these documents to the quality described above requires considerable effort, well coordinated and properly executed business processes, and generally involves the use of computers.

Document management systems provide on-line search and retrieval systems for documents (e.g. procedures and reference material).

Dose management systems maintain the official dose records of staff and combine these with recent "estimated doses" to provide up-to-date dose information for staff when preparing to do newwork. Entry control systems are used to control and monitor the entry of personnel into a NPP, whether they be regular staff, visitors or contractors.

4.3. EQUIPMENT PERFORMANCE APPLICATIONS

Computers have been increasingly recognized as tools for improvement of maintenance capabilities, practices, methods and procedures to supplement the traditional manual intensive maintenance activities. The goal of the improvement is to reduce the number of unplanned outages, shorten outage length, reduce the cost of repairs, improve plant availability and reduce plant maintenance costs.

Computers are also used to perform reliability cantered maintenance processes to evaluate plant systems for maintenance planning. The key steps of the process are: to define the system boundary, partition the system into subsystems (i.e., typically group functionally alike equipment), define the important system functions, perform a failure modes & effects analysis or fault tree, and develop preventive maintenance tasks for functionally critical components.

Recent utility implementation of predictive maintenance techniques particularly rely on monitoring and diagnosis of plant equipment performance status. The monitoring of equipment status is often related to operations, as described in Section 3. To emphasize maintenance applications, the computer-aided monitoring and diagnosis functions are categorized as follows:

- Computer-aided monitoring includes loose parts monitoring, rotating equipment monitoring, thermal performance monitoring, heat rate monitoring, water chemistry monitoring, corrosion and erosion monitoring, piping components fatigue monitoring, vessel integrity monitoring, emergency diesel generator diagnostics, and motor operated valve monitoring, etc.
- Computer-aided inspection covers areas of reactor vessel inspection, primary piping, welding inspection, nondestructive examination, piping inspection, steam generator tube inspection, valve inspection and service tools, etc.
Computer-aided surveillance and testing consists of activities such as computerized procedures, self-checking and automated testing of reactor protection systems, on-line signal validation for reduction of instrument calibrations, etc.

4.4. ADVANTAGES AND BENEFITS

The main attributes of a computerized information system that benefits the maintenance of NPPs are:

- The ability to have a master database that contains correct and up-to-date data for use by staff throughout the NPP.
- The ability to have synchronized databases that can be updated by staff who are authorized to do so, and to have the updated data immediately available to staff throughout the NPP.
- The ability to have "right information in the right place at the right time" providing staff with an essential resource to enable them to perform work effectively and efficiently.

It is essential to have the "right information" stored in databases. This implies having all the required information and having all the information correct. This is not achieved easily; it requires considerable effort to put information into databases, and to ensure the information is correct.

Information in the "right place" implies accessibility to the databases from any work location in the NPP. This is achievable with the use of computer communication systems, e.g. local area networks.

Information at the "right time" implies accessibility to the data bases at any time of the day, whenever staff need the information to assist (or enable) the performance of work.

A significant benefit to the "right information at the right place at the right time" is that the time intervals between steps in a work process can be reduced significantly. These "time intervals" represent slack time (dead-time), and if they are reduced, will have a direct impact on the amount of work achievable in a given period of time.

Of course the most significant benefit is having correct and appropriate information (the "right information"). This has a direct bearing on the ability of staff to perform quality work, using the correct materials, procedures, calibration settings, and so on. The following section lists specific examples of benefits.

4.4.1. Quality

The quality of work performed can be enhanced.

- Nuclear safety and industrial safety can be enhanced because equipment isolation permits (tagouts) can be managed effectively; radiation dose records are up-to-date and available where needed, and radiation hazard information is available as work is being planned.

- Environmental protection is enhanced because analysis of leakages (and effect on the environment) can be done immediately, in real-time as an event is unfolding; and plume analysis can be done in real-time, allowing for the correct counter-measures to be put into effect.

- Configuration management capability is enhanced because up-to-date engineering data & drawings are always available to all staff; correct spare parts are specified and provided; correct procedures are available; records are properly filed for future reference.

- Procedure compliance is enhanced because authorized procedures are always available; there is an assurance that correct procedures are used; up-to-date documents are maintained for calibration information; and documents for QA records, tests and previous maintenance are
readily available.
- Fuel management is enhanced because fuelling is completed according to specifications for reactor core physics and fuel limitations, and irradiated fuel records can be managed effectively.

4.4.2. Production

The production of electricity from NPPs can be enhanced.
- The duration of outages can be reduced by identifying and acquiring all resources needed (including spare parts, tools, procedures, etc) before the start of the outage; and by performing critical path planning before and during an outage.
- The risk of forced outages can be reduced when preventive maintenance is performed correctly and on time.

4.4.3. Cost

The cost of producing electricity can be reduced.
- The inventory of spare parts can be managed to provide the correct spare parts, when they are needed, while controlling the total inventory at an acceptable level.
- Productivity improvements can be achieved by developing information systems which reduce the difficulties in getting work done. For example, improvements can be made to the timely availability of the right material, tools, procedures and information to the worker at the workplace.
- The throughput of work done can be increased by reducing the dead-time (idle time) between the steps in a business process, and to reduce the time spent waiting to receive the correct part or procedure. Computers can, for example, eliminate the delays encountered by moving paper documents from place to place and they permit workers to rapidly search for and find information that is stored in the information system.

5. MANAGEMENT OF COMPUTERIZED INFORMATION SYSTEM

5.1. MANAGEMENT OF HARDWARE, SOFTWARE AND DATA

To achieve good management of a computerized information system throughout its complete life cycle, it is necessary to develop a strategic plan, consistent with the objectives of the utility and considering management of information as a corporate asset. This plan must be based on analysis of the role that information technology can play to help close the gap between the actual and desired level of performance. Information technology should not be considered by itself but in conjunction with the other resources of management (human, financial, organizational). From the results of this analysis, precise goals for the information system design and operation should be built into the strategic plan [15].

An information system gives users a representation of the physical plant which helps them to operate based on the information derived from the system. Therefore, it is of the highest importance to maintain consistency between the information system data and physical reality.

An information system has many connections with business organizations. Ongoing evaluation of how the work proceeds is necessary, not only before the startup of the system, but throughout its life cycle. It is necessary to monitor the evolution of work places and of exchanges between work groups during the complete life of the system in order to maintain consistency with the working conditions. The startup of the system is only a beginning and not the end.
The maintenance management system, tightly connected to other systems (financial, human resources, technical and process, etc.), is one of the main tools of management. Information system has to be maintained and must be prevented from being degraded. Information is a corporate resource, and has to be managed as such. The responsibility for the information should be defined clearly and its effectiveness on the results should be evaluated.

5.2. CHANGE CONTROL

The essence of change control is that all changes are made in a planned and controlled manner, are properly tested, and are only considered complete after all the documentation of the system has been updated. A necessary prerequisite for change control is to have documentation which correctly describes the installed base of the hardware and software components of the computer system. This documentation must be kept up-to-date as changes are made. The change control procedure must ensure that changes are implemented in a planned manner, and that thorough testing takes place to ensure that the systems perform correctly after the changes have been made. Back-out procedures should be ready in case undesired results occur. While the principles of the change control process are simple and clear, execution of all the necessary steps requires a great deal of effort, determination, and thorough follow up to ensure full compliance.

When modifications are made to on-line software, a rigorous assessment of each change should be made before implementation. The change should be tested off-line, so far as is practicable, and shown to meet specified requirements by written tests. Written authorization should be required before on-line operation takes place with the software change loaded in the target computer hardware, and a probationary period of running should be agreed. This should take place during stable and non-critical plant conditions. Written test procedures to confirm the on-line viability of the change are recommended, and a permanent inclusion of the change must be formally authorized. Where modifications to software with a major significance to safety are involved, more extensive procedures are usual, involving off-site checks of the need for the change and its correctness. The verification and validation of the change must be assured to the same degree as the original software, although site conditions may require that different detailed processes take place.

5.3. QUALITY ASSURANCE FOR COMPUTER SYSTEMS

5.3.1. Quality assurance requirements

The general requirements for quality assurance (QA) on nuclear plants are well documented in IAEA Code of Practice No. 50-C-QA (Rev. 1), Code on the Safety of Nuclear Power Plants: Quality Assurance [80]. These principles are supplemented for software in IAEA Technical Reports Series No. 282, Manual on Quality Assurance for Computer Software Related to the Safety of Nuclear Power Plants [10].

For management information systems, the QA requirements of IAEA Technical Reports Series No. 282 cannot be followed in all cases, since extensive commercial software systems must be used. The following section outlines the processes of QA of current good practice.

5.3.2. Commercial systems

The necessary QA processes for accepting and using proprietary software from a manufacturer depend on:

(1) The use of a well-proven software system, of wide application, and with minimum change, which should be specifically agreed.
(2) The use of established international or national QA standards or policies, e.g. IAEA Technical Report Series No. 282 [10]. QA policies or routines developed by the utility or the vendor could also be used if they are in accordance with established QA standards.

(3) The establishment of careful procedures for error handling and error correction.

These error handling processes depend on processes of verification, at detailed and at global levels. Specific data entry should be confirmed, and data produced should be tracked and controlled by established issue, change and reissue procedures. Again, these will generally be consistent with the changed control requirements of the IAEA.

The ultimate responsibility for the operational use of the information system has to rest on the user. The information system will provide a service, which will be as accurate and reliable as is practicable, but may for all that have residual errors. Specific responsibilities of the human user will include responsibilities of plant safety and availability, and part of that must include responsibility for confirming, to a reasonable extent, that information which is used is correct.

5.3.3. Verification and validation

A basic requirement for computer systems is that system documentation is verified at each stage of production. Each document which defines the design should be produced by a top-down process, in which the functional and design requirements are defined in progressively greater detail. Each document should then be verified to confirm that it correctly represents the requirements of the source document. For the highest requirement of safety, the verification should be independent, and formally conducted using check lists and documents with recorded resolutions of any discrepancies.

After completion of the design breakdown, in the form of detailed specifications of hardware and computer codes, system validation is needed to confirm that the integrated hardware and software perform correctly. The definition of functions given in the original requirement for the system must be taken, and interpreted into the form of detailed functional tests, test instruction, and expected test results. The computer system must then be systematically tested to those requirements, and the results recorded and analyzed. Any discrepancies of performance should be formally recorded and corrected through change notices, in accordance with the QA procedures. Extensive and detailed guidance on the verification and validation (V&V) of computer systems is given in IEEE1012, IEC987 and IEC880 [21,22,81].

5.3.4. Qualification of hardware and software

5.3.4.1. Hardware qualification

The hardware qualification of a computer system for a nuclear power plant will depend on its application, and whether it is formally classed as "important to safety". Off-line information and support systems can normally be procured as off-the-shelf items, operating from standard tolerance electrical supplies, and housed in offices or a computer centre on site. On-line systems connected to the process will require a definition of limits of power supplies, frequency and voltage, and of ambient temperature and ambient humidity, and will require a demonstration or certification that operation is achieved satisfactorily in the limiting conditions. A safety computer system will require formal Equipment Qualification (EQ) to IEC 780 [82] and IEC 980 [83] for environmental and seismic performance, sufficient for its duty. If computer system components, such as remote multiplexers, are required to operate within the containment, demanding temperature and humidity conditions must be shown to be acceptable for periods sufficient for the safety duty. A general guide to accepted practice is given in IEC 987 [22]. General practice for hardware qualification of on-line systems will require some or all of:
(1) Type testing of each class of module to its full operating extremes and full performance in works.

(2) Production testing of modules to production acceptance criteria.

(3) Subsystem or unit tests, and system integration tests to criteria appropriate to a factory assembly platform.

(4) For critical systems, a formal factory acceptance test, which may require a period of continuous satisfactory operation under controlled conditions for periods of about a week to a month.

(5) For critical systems, testing may be required in the factory at the environmental extremes (0°C to 55°C ambient, 0% to 95% relative humidity are representative), and may require special supplementary tests for Radio Frequency Interference.

(6) Installation on site should normally be followed by customer acceptance testing, which repeats the factory tests but from site supplies and under the plant administration procedures.

(7) After installation, a period of several months of trouble-free operation should be required, during which time plant signals are progressively connected and demonstrated to the utility.

(8) The completed installation should be shown to operate satisfactorily by witnessed demonstrations of its functions and some form of endurance test.

(9) The satisfactory integration of the computer into the total nuclear plant I&C will require commissioning tests with plant. During these tests, plant process systems will be operated, alarms will be monitored, and automatic control and protection functions operated in all foreseen modes, to written test procedures.

5.3.4.2. Software qualification

Software qualification is a growing issue within the process industry. Verification and Validation (V&V) and testing are growing rapidly in formality and rigour, and are being extended to all levels of software design and the total software life cycle [77,78].

The major problem of software qualification for any application is the attainment of confidence in the failure free performance of the software. This is at its most demanding for applications important to safety. At the present time, techniques are developing rapidly.

Early systems often were assembled in the factory, but rigorous testing was not always possible due to late production of software. The system installed on site often required on-site development of software. Before operation with station plant could be accepted by the utility, a software soak test and demonstration of all facilities was used to give confidence.

Present day systems can often be assembled using system software which has been previously used. Where this is possible, the application software and data can be rapidly produced, and a factory test can be used to demonstrate correct functions of display, logging, recording etc. Nevertheless, utilities should insist on full on-site soak testing and witnessed demonstrations of all facilities before operating with plant.

All modern software for an on-line nuclear station should be independently verified in some way. If this is done, and careful top-down documentation is prepared, very few faults will remain. Such software will operate without failure for periods of over a year, from practical experience. This level of assurance is not sufficient, however, for applications to reactor safety.
For a software application to reactor safety, in addition to the above methods, regulatory authorities may require confidence to be considerably enhanced [39,40]. The measures which are being used for this include:

(1) The animation of the written specification, during development, to confirm the specification is correctly written and correctly understood.

(2) The expansion of the specification in a Formal Mathematical Notation (e.g. VDM, or Z) [84, 85].

(3) The formal demonstration or proof that the code corresponds exactly to the formal expression of (2).

(4) Full factory and on-site testing, in accordance with normal past practice.

(5) An independent assessment and certification that the software design, implementation and documentation is satisfactory.

(6) An analysis of the code, using an automatic tool (e.g. MALPAS, SPADE), [75, 86] to demonstrate that the logic required matches the logic which the code implements.

(7) A back- compilation, to take the machine-code instructions and generate source language statements, which must then be shown to match the source code.

(8) Pseudo-random testing of an integrated hardware/software system, to inject representative transients and to confirm correct responses are made.

Not all the above measures will necessarily be required for any particular application; however, for the highest level of assurance and modification, the majority may be [23, 40].

5.3.5. Documentation

The documentation needed for a computer system is defined in IEC 987 [22] and IEC 880 [21], for on-line systems. Design documentation should be produced for the functional requirements, the design specification of all hardware and software modules, the detailed module circuits and layout, and the detailed code for systems important to safety. This information should be fully available in the systems handbooks and manuals, which should also include full details needed for obtaining spares, and organizing repair or replacement of defective components and modules.

The provision of full documentation to the end user for proprietary systems, systems bought off-the-shelf, and systems important to safety is desirable for the hardware, but may be commercially difficult or impossible to arrange where extensive standard software packages are used. The manufacturer or his agent must be competent to repair failed modules, provide spares and give help on software operation problems, and must be known to the end user.

Specific information, as project documents, is needed to show installation details and arrangements, cable routing, power supplies etc.

5.4. CONFIGURATION MANAGEMENT AND CHANGE CONTROL

5.4.1. Architecture management and change control

5.4.1. Objectives

The use of computers arises generally in separate fields to solve separate problems. However,
the overall architecture necessary should:

- give end users a common view of the information system
- allow communication between the different systems
- give to every user valid and consistent data.

5.4.1.2. Architecture constraints for designers

To define an architecture according to the previous objectives, leads the designer to study carefully the following topics:

- Workstations - For technical and financial reasons it is not yet possible to define a unique workstation for all users. Nevertheless, it is necessary to define for each family of end users, a standard workstation and a standard communication interface between applications and users. The applications developed recently show that passive terminals are being replaced more and more by intelligent workstations. A good feature is to use the computational capacity of the workstations to enhance the capacity of the man-machine interface for applications of local interest.

- Networks - It is necessary to implement an effective and realistic separation between process-oriented network and support-oriented network. The exchanges of information between the two networks must be carefully controlled by a "high security" gateway, e.g. working in a single direction, from the process-oriented network to the support-oriented network. According to the nature of the applications, computers and departmental networks are connected to the appropriate network.

- Data - Data quality is essential in a computerized system. This requires data standardization and data management processes to be set up.

The systems developed in the last few years, especially in the maintenance field, show that collecting, checking, and entering data on computer systems represent a large amount of work. This represents a large part of the total cost of the system. Generally, a new system gives management an opportunity to increase the quality of the existing data in documents or drawings.

5.4.1.3. Organization

The complexity and variety of systems on one hand, and the strategic importance of information systems on the other hand, gives reasons to modify the existing organization in order to be able to control the entire information system. Generally, modifications are made at three levels:

- Decision level - One person of the top level management team is in charge of information systems.
- Consulting level - A committee or a consultancy group, gathering representatives of different users, helps the manager in charge of information systems.
- Executive level - The consistency of information systems is ensured by a person or a team working full time on this subject.

5.4.2. Standards

Standards must be used to preserve the ability of systems to communicate and exchange information. The use of standards also facilitates evolution of hardware and software and helps preserve the previous investment of the company from obsolescence. The problems are not the same for systems using general purpose computers and for systems nearer the process and directly linked to it. In the first case, the standards can easily be at the base of developments. However, for the second case, standards are not at present available for such systems whose role requires them to reflect the current state of the plant.
5.4.2.1. Functional standards

Exchange of information needs a common meaning for the entities manipulated by different components of the information system. The same object has often several possible representations. It is necessary to ensure consistency of all the representations. Internal standards have to be defined by the company, with respect to national and international standards when they exist.

5.4.2.2. Communication standards

An information system is based on communication. It is important to preserve the integrity of the system during the complete life cycle. For this reason, the designers must respect standards for communication with the objective of minimizing the effects of hardware and software evolution.

Standards concerning the data transmission domain are well known. Communication of information between subsystems is not completely standardized today, but standards will begin to appear. It is recommended that the state-of-the-art in this domain is followed. Utilities have an interest in defining internal procedures for this class of communication. A rigorous structure for the management of the exchange of data will provide a degree of protection from the unavoidable changes of hardware and software in the future.

5.4.2.3. Data dictionary

A data dictionary which defines the meaning and the types of data, their exact format and ranges of validity, is necessary for any application of computers to information systems. Data dictionaries may be specific to the supplier of the software, and will not necessarily be of a compatible standard with other suppliers. If, however, standards do not exist, it is important to use market standards, but only if they have a reasonable chance of enduring.

5.4.2.4. Data storage

Physical storage follows current standards and is mainly the responsibility of the information system designers. For storage of documents, new standards are now being developed and appearing and can be used with benefit.

5.5. OBSOLESCENCE AND RETROFITTING

As many plant systems and equipment become aged, the issue of obsolescence has become one of the most important concerns in operation and maintenance, particularly those related to instrumentation, control, and computer systems. Certain aspects of obsolescence may have the potential for causing reactor outages or keeping them from regaining power level promptly. Other aspects of obsolescence could involve long delays in procurement due to re-qualification or licensing activities. The need to address obsolescence unavoidably leads to upgrading or replacement of the obsolete systems or equipment by retrofitting (sometimes referred to as backfit). Although there are many and various reasons for retrofitting, retrofitting and obsolescence are directly related because retrofitting considerations often constrain or dictate the modification and upgrade process.

In the area of computer technology for operation and maintenance, the obsolescence and retrofitting are related as follows:

- Installation is driven by the requirement or need to improve operator-machine interface
- An upgrade or extension of existing computer-based systems is needed
- Existing systems that are obsolete must be replaced
- Previous analogue systems need to be augmented or replaced
- Experience and problems encountered with retrofitting show the following concerns:
- Retrofitting is very complex to perform in operating plants
- It is difficult to work in parallel with the operation of a plant
- Short changeover times are usually mandated to reduce outage durations and costs
- Commissioning and testing must be thorough, but be completed expeditiously
- Training and operator qualification must be done thoroughly
- Communication techniques and open standards tend to develop over time
- Verification and validation is necessary but costly
- Operator acceptance may be difficult to achieve
- Regulatory acceptance may be difficult to secure.

Lessons learned from the experience lead to the following considerations:

- In retrofitting, the utilities will be likely to use stepwise design changes to directly solve specific obsolescence problems. This makes it important for utilities to develop an integrated strategy to deal with many and different parts of retrofitting.
- There is a need for developing understanding of the economic benefit to be derived from making plantwide retrofitting improvements using modern computer technology. This will strengthen utility interest and incentive in planning long-term upgrades.
- In addressing obsolescence issues effectively, the identification of replacement and interchangeability with modern computer technology alternatives is needed.

In addition, designing future computer systems to minimize the effects of obsolescence on both software and hardware are key elements for system designers. The design for obsolescence should consider the following factors: configuration and architecture, hardware choices, partitioning or use of building blocks, software methodology, requirements and specifications, documentation for programs and users, computer language selections, and modularity design, etc.

5.6. IMPLEMENTATION ISSUES

Implementation of an information system is a major and demanding operation. An information system will be efficient only if operators can be confident in the correctness of information in use and if concerned people are currently trained at the same time to operate with the system. Quality of the databases and of the training are, with organization problems, the main points to study before implementation of an information system.

5.6.1. Organization

Introduction of a new information system often has consequences on organizations. It is important to integrate the organization structure and the work processes in the workplace with the new information flow. A difficult but necessary task is the measurement of the consequences of introduction of the system on people in the plant. In general, information systems modify in a significant way relations between workers and groups. It would be a serious error for management to neglect this asset when an information system is implemented and it could be the origin of serious disappointment.

5.6.2. Implementation of databases

In general, data which exists in different databases will not normally be consistent unless a specific effort is made to ensure the databases are designed to be consistent.

Verification, and in some cases certification of the data included in the databases needs a large amount of work. For example, in the French nuclear system, the activities to collect, verify and record the data of the maintenance information system is evaluated as 2 000 man-days per unit. However, work is not often finished in this first step. Management of the plant should then be very
careful to maintain the database consistent with the state of the plant. All modifications have to be reflected on the database and the initial quality has to be preserved. Maintenance of database needs organization and resource.

5.6.3. Training

The best systems would be completely ineffective if users did not know how to use them. Training requires the mobilization of a lot of resources. Modern information systems represent a very large field of activity, products are complex and they include many subsystems. It is sometimes difficult for a user to find the most appropriate way to achieve a given objective. Initial formation relating to the French experience represents about 1 300 man-days of training per unit. However training is not fully achieved with startup of the system. Supplementary training is always necessary, first for new operators but also for those having a first level training. Training has to be included in the general training for maintenance and operations staff. In the French experience described, the amount of supplementary training reaches 300 man-days per unit each year.

5.6.4. Investments required to achieve results

A computer system cannot solve the existing problems of an organization. It is not possible to buy and import a ready-made system that will immediately achieve results. It is always necessary to audit the structures and to analyze the work procedures, modify software and enter data before startup. This study should include all of the users at all hierarchical levels and should report conclusions and recommendations for acceptance and subsequent implementation.

6. FUTURE TRENDS AND RECOMMENDATIONS

There is a continuing trend in the nuclear power industry to apply computer technology, including expert systems, to various engineering, maintenance and operations functions. Expert systems technology has a number of unique capabilities which makes it a resource for the utilities. These include programming flexibility, inference capabilities, explanation facility and knowledge structured according to human models.

The next generation of nuclear power programs has placed significant emphasis on the appropriate use of modern technology for the man-machine interface system. Considerable experience has been accumulated regarding operation and maintenance of existing designs. This experience provides opportunities to improve fundamentally the safety and operability characteristics of nuclear plants. Breakthroughs in information and communication technology provide a real opportunity and challenge to exploit these capabilities in a manner that will provide benefits to operation and maintenance. Specific future trends and recommendations are described in the following sections.

6.1. ON-LINE AND OFF-LINE DATA MANAGEMENT

The data which is required in on-line systems for display, control and protection to define the details of each signal, and the data which is received in off-line systems for information support and management of the plant is very extensive, complex and critical. Some of the data has a central place in safety; for example, the procurement details of a safety plant item or the trip levels included in a protection system. The advantages of full resolution of the problems of on-line and off-line data management will be improved management control of the plant, and higher confidence in the correctness and accuracy of the function of the computers on the plant.

It is recommended that careful attention is given to ensuring full compatibility of databases, correct gathering of the data initially and satisfactory verification and control of the data itself.
6.2. DIAGNOSIS AND PROGNOSIS SYSTEMS

Diagnosis and prognosis systems for operator aid calls for a broad and detailed knowledge of the dynamic behaviour of processes and systems, experience with disturbance sequences and failure mechanisms, ideas and rules about recovery methods, and operating procedures, etc. Those systems need dialogue functions with easy access to the stored knowledge and the ability to explain to the user how solutions and answers have been achieved. In this context, Knowledge Based Systems have found great attention [11]. One of the most important enhancements to diagnosis and prognosis systems is to ensure reliable and accurate signal input into the systems. Analytical redundancy will be an important tool to back up or replace or even enable the necessary cross checks of primary information.

This implies a recommendation for development of on-line simulation models with the ability for separation of process anomalies and sensor faults and, consequently, has to be seen tightly aligned to the diagnosis process. Techniques for modelling individual processes should be further developed. Qualitative simulation will be a key to achieving simpler and more robust simulation models.

Filter techniques to connect the models to the process have to be industrialized. In the field of prognosis, predictive filters will be applied, and coupling of simulation with cause-consequence-diagrams will be investigated in order to realize extrapolation of event sequences. Also, neural networks will be considered as tools for fast recognition of learned scenarios from signal patterns as they appear.

6.3. COMPUTER-ASSISTED OPERATING PROCEDURES

Computer-assisted operating procedures will minimize the need for paper procedures. The operators will use VDU screens that present integrated text, graphics and checklists. 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 may be "context sensitive" in that the computer will edit and simplify them, based on 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, but the status of the pump would be shown because it is key to the success path of the procedure). Examples are an on-line emergency operating procedure (EOP) system implemented at the Canadian Point Lepreau CANDU plant, an expert system which codifies EOP logic rules and links them with plant database for use by training but not for operation [87]. In general, current usage of computer-assisted procedures is minimal and in its infancy, but is a major target for future development.

The recommendation is therefore that computer-assisted operating procedures should be developed as research projects and prototypes, and feasibility tested on suitable full-scale applications where these may be possible.

6.4. TOUCH SCREEN CONTROL

Touch screen control is developing rapidly in nuclear power. Typical methods being implemented, or intended, involve an overview display with a moveable cursor. The operator selects a plant area with the cursor. A VDU display is presented with details of that plant. Areas on that display, or alternatively a separate display VDU, then show control functions (such as open, close or raise, lower). Touching those areas, or selection using a cursor, with a confirmation action then causes the plant action to be taken.

Touch screen control has very great advantages of reduction of control room cables, and enhanced flexibility of control. The regulatory acceptance may be difficult, since clear assurance
must be gained that a selected function is correctly selected and correctly performed, if safety plant
is involved. The economic and technical advantages are such that touch screen control is certain to
increase.

The recommendation is therefore that touch screen systems are approached with care, and that
consideration is given to the problems of system integrity.

6.5. DISTRIBUTED SYSTEMS

The use of distributed on-line systems, with input and output equipment local to plant and
connected by local area network methods will increase. Several subsystems will exist on a plant, each
of which will integrate data collection, control room controls, switchgear and plant control, and
automatic closed loop control functions. Separate systems will be needed for safety functions as well
as non-safety functions. They will operate autonomously, and provide their information to other
systems for on-line display and operator support, and for off-line engineering analysis.

The advantage of such systems is the reduction in cables and the provision of comprehensive
information while preserving total electrical and physical isolation with optic fibre. Problems will
exist in safety justification and in assessment of common mode risks if software errors could cause
several such systems to fail.

A firm recommendation arises from the field of distributed systems when Local Area Networks
(LANs) are used. For information interchange between partners connected to a LAN the kind of
communication protocol is of essential importance. For all communication, given deadlines for
successful communication should be met. This requires the implementation of a deterministic LAN
protocol if possible. An example which has been used with success on the Sizewell B plant is a
deterministic version of the well-known Ethernet system. This is defined in IEEE802.3D [88].

6.6. EQUIPMENT WITH EMBEDDED SOFTWARE

Manufacturers of different types of equipment, e.g. sensors, transmitters and more complex
subsystems such as power inverters, are increasingly using digital computer technology in order to
improve the functionality and efficiency of their products. This development implies that software
will be embedded in the product.

The implementation of computer technology in such items opens up the possibility for data
communication with higher level systems. This could reduce the cabling and the need for complex
data acquisition systems.

The increased functionality is advantageous but attention must also be paid to the licensing and
qualification considerations that may arise due to the embedded software. This is especially important
for retrofits and replacement of old or obsolete equipment.

6.7. COMMUNICATION SYSTEMS

Communication systems play a key role in rapid development, integration, and efficient use of
digital systems. A digital system in a power plant may include single-loop controllers, programmable
logic controllers (PLCs), distributed controllers, plant monitoring and data acquisition systems, and
engineering, maintenance, and operator workstations. A communication system that connects these
systems has a significant impact on the present and future operation of a plant. For reliability and
operability reasons, a communication system may consist of several networks.

The recommendation arising is that, to take advantage of powerful applications such as
diagnostics for plant operators, these networks should be integrated. These networks can best be
integrated by having them meet an open standard adopted by nuclear power plant owners. The most widely recognized open standard is the International Standards Organization Open Systems Interconnections.

6.8. NETWORK MANAGEMENT

In the future, the computer systems will evolve to a highly decentralized system, cooperating on a powerful multi-media network system. Networks will in the future, transfer many types of data coming from various databases, not only from classical alpha numerical or graphical databases, but also from voice or video databases. One of the main problems will be network management. Today, network management is a growing function in utilities. In a few years it will have first place in the information system management. Network management will realize the functions allowing the users to obtain, at any time, the services they need: access to the servers, implementation of security requirements, and control of performance, etc.

Today, these functions are mainly based on human procedures. It is recommended that the designer notes carefully the expectation that, in future, they will be automated, and that designs should make full use of this. The automatic network manager will be able to choose the appropriate support at each time with respect to security conditions, performance needs, availability of servers and materials on the network.

6.9. STANDARDIZATION OF INFORMATION EXCHANGE

Networks will be the backbone of the information system. On the networks, servers custom-designed for specific functions would deliver service to the users. It will soon be possible to achieve the vision that all staff in NPPs will, by themselves, be able to access the information they need to do their work when and where they need it.

The technology is available today and is becoming more economical. The concept is that staff will have access, from any location, to information on parts, procedures, calibration data, etc. The information they access will be up-to-date and correct at all times.

Communication between the servers and the users will need a high level of reliability and availability. The users must be protected from the change of technology in computer hardware and software or in transmission procedures. The general use of standards is a major need for the electronic data processing community, but it is of special interest to the nuclear industry where the needs of reliability and availability are extremely important.

The recommendation arising is that, to reach this goal, it is desirable to adopt the existing standards, e.g. IEEE or OSI standards. Where these standards do not cover the requirement, it is good practice to use the commonly accepted industry standards and this can give the designers and the users a good assurance of durability.

6.10. DATA ARCHITECTURE AND MANAGEMENT FOR MAINTENANCE

There is a trend towards defining and developing a total data architecture for the complete data requirements for NPPs. Such an architecture would define all the data entities and their relationships to each other [89, 90]. With this it will be possible to identify the master data for each data set, and to assign responsibilities for management and control of the data.

The recommendation is therefore that all information systems should use data from master data sets to eliminate inconsistencies. It will then be possible to ensure the configuration management is achieved throughout the life cycle of the NPP.
6.11. EFFECTIVE VERIFICATION AND VALIDATION METHODS

The increased use of digital technology in nuclear power plants brings with it concerns about the reliability of the associated software, which will perform many functions previously fixed in hardware logic as well as add requested and desired capabilities. Software failures can affect plant safety, reliability and availability. Verification and validation of computer systems will enhance the acceptance of digital systems by users, managers and regulators through increased confidence in the software. Recent experience of implementation of computer systems for safety applications in Canada and France shows that verification and validation can be costly and delay the schedule of plant commissioning.

The recommendation is that practical and cost-effective verification and validation methods and tools are developed to help assure the quality of software and to facilitate wide implementation of digital systems. Software design and development methods and tools need also to be developed to improve software quality and to allow the reuse of software modules in other applications, and to facilitate the development of tools to support automated software development, verification and validation.

6.12. CONFIGURATION MANAGEMENT

The essence of configuration management is that there should be a plant information base (drawings, specification, etc.) that correctly represents the approved design basis, and correctly represents the physical plant itself (pumps, valves, wiring, etc.) and its functionality, and the converse must also be true at all times during the life of the plant.

The information base must be the same as the physical plant and its functionality must be the same as the information base. During the life of the plant as changes are made, as maintenance is performed, as equipment becomes obsolete and is replaced, this equality relationship must be preserved [51].

To achieve this is a daunting task. Computers can assist with management of the databases, but the information in the databases is only as good as the information which is put into them. Full achievement of configuration management requires management resolution, adequate support systems and procedures, and a disciplined approach by all staff of the NPP.

A major contribution to computer technology is the capability of having a master dataset (e.g. of equipment lists, spare part specifications, etc.) that is used consistently by all staff in all aspects of their work. This master dataset would enable consistency to be achieved between the components of the documentation (drawings, procedures, spare part lists, specifications, etc.) and enable all documentation to be modified as changes are made in the plant.

At present, most NPPs have documentation systems contained in paper and electronic (computerized) media, and frequently each dataset might be stored in more than one database. It is difficult and time consuming to update all databases and documents for each change, and to keep them all up to date. New computer technology can be used to overcome these difficulties, and systems are being developed for new NPPs.

In the future, it will be necessary to guarantee that at least for safety systems, information and documents are correct and consistent at all times.

At the present time, no system exists that is able to assure the consistency of all the information. This function is performed by the management of the company or of the plant. However, some systems specializing in certain fields such as control and automation are beginning to appear. For example, in the 1300MW French plant, one system is able to automatically generate the logical equations from the electrical diagrams designed by a CAD system. This type of solution may be
extended to other fields, when the system is defined during the engineering phases of the plant. Until systems are able to treat the entire problem, it will be necessary to convince management of the value of applying resources to achieve specific improvement using existing systems. Before introducing a new computerized system in the plant, it is necessary to examine it in a general perspective to determine what it is able to achieve for the desired state of configuration management.

6.13. FAULT-TOLERANT DESIGN

Fault-tolerance is a system approach for designing hardware and software to satisfy the requirement of high reliability and availability. For digital systems such as digital controllers, fault tolerance means that the system is designed to protect against single failures. In other words, the system is able to identify faults as they occur, isolate the faults, and continue to operate. To achieve fault-tolerance, the system is designed with redundancy, including for examples, input and output modules, central processing units, power supplies and cooling mechanisms.

Fault-tolerant design for hardware has become a common practice for high reliability on-line digital controllers and process monitoring computers. On-line digital protection systems have an equal or greater requirement for fault-tolerance and often must be designed to be fail safe.

Since the failure modes for software are different from hardware, fault-tolerant design for software needs to consider the failures caused by common modes effects which may be introduced during designing or programming. While the assurance of fault-free software is difficult to achieve, regardless of formal verification and validation, software fault–tolerance may require the consideration of functional diversity. This means that duplicate software would be designed, programmed, verified, and validated independently and separately. Alternately, fault-tolerant software may require a backup system or a fail-safe option so that if the software fails, it will fail to a safe state as the overall system requires. This kind of approach is expected to be extremely costly.

The recommendation is therefore that active research is undertaken to identify the practicality of software fault tolerant designs, so that arguments of diversity can be used to pre-empt some of the problems of software reliability justification. It is anticipated that in the future application of digital systems, more and more V&V procedures will be required for software to reach a level of reliability and availability for which they were not previously expected to achieve. The ability for software to be qualified would certainly be a main constraint in the near future.

7. CONCLUSIONS

The nuclear power industry has often been in the forefront of the process control application of computers, and this has been the case for application to operation and maintenance. However, the power and speed of computers have only recently become economical and sufficient for some operations which require frequent updating to match plant conditions. The speed and power now give a firm base for the expansion of computers into many fields on nuclear plants. These include both systems on-line to the plant and reflecting plant state directly, and off-line and reflecting plant state indirectly, using links to other systems and used to support operation and maintenance.

The application areas of significance include:

- On-line support to the operators through man–machine interfaces to show plant states
- On-line control, sometimes of safety significance
- On-line protection and interlock applications, important to safety
- Systems for condition monitoring, prognosis and diagnosis, on-line to specific plant equipment
- Off-line systems, providing information for planning, support, management and operation history information needed for efficient plant operation and maintenance.
A summary of experience, problems and advantages shows:

1. The use of computer systems for on-line display of plant state to the operators is now common, and retrofit systems with improved performance are being implemented. The flexibility of colour VDUs and the use of structured hierarchies of displays have overcome most of the problems of early systems. The use of such systems has major advantages of providing information on the complete plant, with the added ability to present summary and calculated information to operators. Integration of such features as operating procedures into the Video Display Units is possible.

2. Fault tolerant digital control systems have significant advantages, and have been successfully applied to many nuclear plants. These controllers use redundant microprocessors and signal validation methods, and provide wide range algorithms with more optimized performance and higher reliability than the previous analogue controllers. They have been shown to reduce plant outages and trips, and reduce safety challenges to the plant. Their use will grow, but this may be inhibited for safety applications by regulatory problems.

3. Computers are being used increasingly to provide integrated and multiplexed operation of control room controls, with connection to the plant equipment using predefined and protected local area network systems. This provides significant advantages of cable reduction, space reduction and improvement of safety. All plant interlocks can be implemented into the control and automation of the production of control logic for switchgear is possible. Touch-screen controls in the control room can be integrated into the system. This will be a significant area of growth.

4. Computer-based systems for protection have been implemented successfully in several countries, but often at costs far higher than expected. The extensive verification and validation required for assurance of software accuracy and integrity has been found to cost more than anticipated. The lessons learned have general application in the production of very high quality software. The other difficulties have not generally been those of computer technology, but of regulation and licensing. The operational integrity must be demonstrated and assured to very high levels, using demanding methods. These methods, such as formal verification and validation, formal definition of requirements, modelling, code proof, code analysis and dynamic testing, are now becoming more fully supported by software tools, and the costs will fall. The need to address obsolescence of existing protection equipment, the attraction of better protection algorithms and the improved protection which is possible using computers will increase protection applications worldwide.

5. The use of proven software in a new application gives problems of assurance of performance. The availability of documentation and of the operating history of software is essential to its reuse. A commercial software system may have many millions of lines of code, and known unresolved software problems, yet it can often be used with full confidence for management information in many organizations. No practicable means of analysis exists to show such software is suitable for an application in safety or protection, yet such systems may be used for planning outages, spares and stock control and many other applications important to safety, and such uses will increase. The successful and economic use of such software is an essential part of the growth of computer applications.

6. The flexibility of computers for information processing has resulted in their application for diagnosis and prognosis purposes. Expert system methods including advanced man-machine interfaces with dialogue functions enable the implementation of complex diagnosis and prognosis tasks in an operational environment. The introduction of process related operator aids such as disturbance analysis, success path monitoring or computerized operation instructions and handbooks are still in an early stage. However, the use of computers for condition monitoring has resulted in widespread vibration and special monitoring on reactors
and turbines. Operations such as motor start logging, loose parts monitoring, mechanical vessel thermal cycle monitoring, etc., are now routine on many plants. Operation strategies will include more comprehensively the concept of predictive maintenance based on such systems, and this can be expected to improve availability and extend plant life.

7. The use of computers for management of spares gives tangible and intangible benefits. Tangible benefits include the reduction of inventory levels by eliminating obsolete material, by taking account of detailed use and supply patterns, and by reducing order and delivery delays. Intangible benefits include improved assurance that spares are correct, and that safety equipment spares have the correct equipment qualification and quality assurance pedigree.

8. The use of computers for improved management of maintenance outage is significant. The use of "umbrella" concepts allows maintenance of associated plants to be grouped. The planned delivery of the correct replacement parts and planned work schedules for specialist staff can reduce outage time. These methods can be integrated with the use of proven computer-based planning tools extended by the addition of on-line update of progress. Such methods improve significantly the records of maintenance made and provided to plant management. This use will grow, but can depend critically on good design of the databases involved, and their compatibility.

9. The management of computer systems will reflect the corporate strategy and attitude to computers. Unless this is carefully thought through, the necessary support to the plant computer management may be lacking, and the system will be less successful than it might be. Key measurements of success are the cost of power produced, the improvement in availability and in safety, and the quality of the work on site. The balance of costs and benefits is difficult to quantify in many cases, and may only be possible by consideration of the practicality of performing some operations without the use of computers.

10. The regulation authorities will require records and documentation of the processes which involve computers, as well as the justification of the computer use as safe where any function important to safety is involved. This can be onerous. In some cases the volume of documentation involved is so great that only a computer system can provide it with confidence.

In summary, the use of computers will increase in all fields, but needs special skills, which are often scarce. Careful planning, system design, detailed design and software production must be followed by verification and validation. The system must have adequate long-term support from suppliers to cover maintenance, modifications, enhancement and replacement. The proper use of computer systems for operation and maintenance will bring significant advantages of safety and economy. The use of computers has great importance both for existing plant upgrades, and for the new designs of reactor anticipated before the turn of the century. All vendors and utilities must take into account the challenge of user acceptance, of implementation and of regulation and licensing if these intentions are to succeed.
REFERENCES


[57] HEINBUCH, H., Erkenntnisse aus dem Betrieb mit bildschirmgestützter Informationsdarstellung und resultierende Anforderungen an zukünftige Warten in Kernkraftwerken (Results from the operation with VDU information in the control room and resulting requirements for future control rooms in NPPs), Fachsitzung "Mensch-Maschine-Kommunikation", Jahrestagung Kerntechnik (1991).


[77] ARCHINOFF, G. H. et al. Verification of the Shutdown System Software at the Darlington Nuclear Generation Station, presented at the UK Institute of Nuclear Engineers International Conference on Control and Instrumentation in Nuclear Installations, May 8-10, 1990, Glasgow, UK.


[81] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, Standard IEEE 1012.


Annex

REPORTS ON THE USE OF COMPUTER FOR NUCLEAR POWER PLANT OPERATIONS AND MAINTENANCE
DATA MANAGEMENT AS A PREREQUISITE FOR CONFIGURATION MANAGEMENT

A. COOK
Bruce Nuclear Power Development,
Ontario Hydro, Canada

Abstract

This paper starts by discussing some real problems that are occurring with data that is being copied and modified. An example is given which involves "Equipment Codes". Root Causes of the problem are identified. Then, Principles and Analogies are developed that help with the understanding of the need for Data Administration. This is followed by development of Data Management Concepts, and an examination of the foundation required for Document Management, and for Document Integrity. The link is then made to Configuration Management. Under "Suggested Solutions", a number of practical steps are outlined, completion of which would lead eventually to sound Data Management which would in turn make it possible to achieve Configuration Management.

1. BACKGROUND

1. I will use as an example, the data concerning Equipment Codes and Material Codes.

2. We completed the Bruce Information Management System (BIMS) Project at the Bruce Nuclear Power Development (BNPD) in December 1991.

We loaded data into data bases for Equipment Spare Parts (ESP), Material Management System (MMS), and Work Management System (WMS).

   ESP/WMS * - equipment codes
   MMS * - material codes

... following an intensive program of data conversion, data clean-up, and data entry where needed.

... and did this for all Departments at BNPD (Bruce NGS A, Bruce NGS B, Bruce Heavy Water Plant (BHWP), and BNPD Services.

3. Part of the BIMS Project was to install a Site-wide data communication network, complete with about 29 Servers and to which about 1800 PC's are connected.

4. The BIMS systems uses a propriety database, IDMS*, but Users have found it does not meet their needs and expectations.

Certain groups of Users have used the network/PC technology to "download" Equipment Code data into PC/Server based databases and are working with this data (eg., adding to it).

5. At this point in time, we have a number of data sets on Equipment Codes, no one of which is truly the Master Data Set.

* Refer to Section 9, Definition of Acronyms.
2. SOME PROBLEMS

We have (1) Data Admin problems, but more importantly, we have (2) Nuclear Business problems.

1. Data Admin Problems
   1. Multiple data sets.
   2. "Master Data Sets" not properly defined and maintained.
   3. Data integrity problems.

2. Nuclear Business Problems
   1. Cost - eg., cost of multiple data bases and platforms to support them.
   2. Productivity - eg., effort being diverted to get the data a User needs.
   3. Configuration Management - eg., we could lose control of the data which is basic to Configuration Management - equipment codes and correctly linked material codes.

Example:

There is no single Equipment Code (EC) set for a Station which has been designated and maintained as "complete & correct".

Therefore, we have multiple "Station EC Sets" none of which are complete & correct, meaning:

... when attributes change eg., functional requirements
or when associations change eg., material/equipment associations
or when changes are made eg., additions/deletions/ modifications
then multiple data sets should be changed, but this is not always done.

eg., Pressure switch on Heat Transport System
   - was recalibrated to meet an AECB commitment
   - later it was returned to the original calibration during a routine call-up (using "old" set-point data)
   - this led to a contravention of a Regulatory commitment

3. ROOT CAUSES (OF PROBLEMS)

First, some symptoms

The Equipment Code data is the base on which many systems depend.
Let's call a complete set of Equipment Codes for one Station, a "Station EC Set".
We typically have a Station EC Set built into a number of Application Systems:

1. Work Management System
2. Material Management System
3. Equipment Spare Parts System
4. Flowsheets
5. Operating Manuals
6. Training Manuals

and we will be building them into

5. Configuration Management Systems
6. Environmental Qualification (EQ) System

We typically have parts of the complete sets built into

- valve list
- air supply lists
- instrument lists
- electrical lists
- calibration records
- etc.

1. The Station EC Sets, for the various Application Systems, run on or appear in:

- a number of databases and document systems:
  - IDMS database (on mainframe)
  - Q&A database (on PC's)
  - Interleaf (on workstations)
  - CAD (for Flowsheets)
  - Oracle (on mainframe, Servers and PC's)
  - Foxpro (on PC's)
  - Sybase (on Servers and PC's)

2. ... are supported by a number of IT platforms:

- mainframes
- servers
- workstations
- PC's

3. ... and run under a number of operating systems:

- MVS
- DOS
- OS/2
- Unix

4. ... all of which (or most of which) can now transfer data via Networks (WAN's, SAN's & LAN's)*.

* See Section 9, Acronyms.
ROOT CAUSE

We have provided for the creation of data, and the interchange of data, by providing the technology (e.g., workstations and networks) and application systems, but have largely ignored the "management of the data itself".

This is largely because our justification and approval processes focus on acquiring technology and applications systems. We specify the requirements for technology and applications, but we do not (in general) specify data management requirements.

We have few controls (if any) on the selection of data bases and design of applications, or on how data is administered, or on how data is structured.

Why are we in this Situation?

1. Urgency ("solutions are needed now!")
2. Individual Budgets ("we will do what we need to do, and we have the money!")
3. Easy availability of software
4. No rules governing the work of Consultants
5. No enforced Policies and Procedures for Data Management
6. No Data structure defined for a Division, Branch, or Corporation
7. Etc.

4. SOME PRINCIPLES (AND ANALOGIES)

1. Highway Analogy

   Compare: Highways vs Networks
   "a high degree of Regulation and Discipline leads to freedom to travel Safely on Highways"

   Versus "a high degree of compliance with Policies & Procedures, and User Discipline, leads to freedom to send and receive information across the data networks reliably, and when needed"

2. Yellow Pages

   Compare: Yellow Pages vs Meta data. "Yellow Pages help you find "IT", whatever "IT" happens to be!"

   Versus "A Data Directory will allow the User to find where the data he/she needs, is stored".

3. Warehouses

   Compare: Warehouses vs Data Warehouses. "Warehouses manage material for orderly receipt and delivery and protection".

   Versus "Data warehouses manage Data for orderly receipt, delivery, and protection".
4. Construction Projects

Compare: Construction vs Reports. "People can build to their own design, on their own lot, using Yellow Pages to find material in Warehouses and have it delivered via Highways".

Versus "Users can construct Reports on their own workstation to meet their own needs, using Data Directories to find Data stored in Data Warehouses, and have it delivered via the data network"

5. Positions & Persons

Consider an organizational Chart, and the Staffing of a Department.

![Diagram of organizational position and person comparison]

- Title
- Name

FUNCTIONAL SPECIFICATIONS

- Job Document
- Selection Criteria
- Resume
- Interview

ATTRIBUTES (CAPABILITY)

A "Position" describes an organizational need and opportunity for a contribution to be made to the Goal of the Department.

A "Person" is a person - with education, experience, capability, etc.

Ideally, a person is selected for, and appointed to, a Position when his/her Attributes match the Functional Requirements of the Position.

POSITION

PERSON

A Position is a Position.
A Person is a Person.
A Position has Function Specifications.
A Person has Attributes.
Ideally, the Attributes will "match" the Function Specifications, leading to the required performance.

But a Position is not a Person, or vice versa.
6. Equipment Codes and Material Codes

There is a direct analogy between Organizational Positions and Equipment Codes, and between Persons and Material Codes.

<table>
<thead>
<tr>
<th>Example</th>
<th>Position</th>
<th>Incumbent</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A)</td>
<td>Org. Position</td>
<td>Person</td>
</tr>
<tr>
<td>(B)</td>
<td>Equipment Code</td>
<td>Material Code</td>
</tr>
</tbody>
</table>

The Equipment Code is the "position", which has Functional Specifications.

The Equipment Code is not the Part.

The Material Code is the "part", which has Attributes.

The Material Code is not the Position. We need to know which "part" is in which "Position", and that the Attributes match the Functional Specifications.

7. Data Positions and Data Values

There is also a direct analogy between Organizational Positions and Data Positions, and between Persons and Data Values.

Example | Position          | Incumbent          |
---------|-------------------|--------------------|
         | Data Position     | Data Value         |
         | - in the application system | - numerical or alpha value |
         | - physical position |
The Data Position specifies the "Position" of the data, complete with all Data Definitions.

The Data Value is the data residing in the Data Position (the Data Value is analogous to the "Person" or the "Part", previously discussed).

5. DATA MANAGEMENT CONCEPTS

1. "BUSINESS INFORMATION" versus "Information Technology".

"Information Technology" represents the technical world of PC's and workstations, operating systems, data base programs, networks, and the like.

"Business Information" represents the information needed to run a Business, i.e., the information needed to support operations, decision making, and for reports, etc.

More and more Business Information is being moved from the paper world to the world of Information Technology.

However, the Policies and Procedures that were developed to verify and protect paper-based Business Information, should be applied when this runs on Information Technology.

2. "MEDIA INDEPENDENCE", with respect to Policies and Procedures for managing data.

"Media Independence" for Policies and Procedures captures the point the Business Information needs to be treated properly (verified, protected, etc.) independent of whether the media handling it is paper or Information Technology.

3. There must be only one Master Data Position, which contains the Master Data Value.

4. There can be copy Data Positions, containing copy Data Values but ... a Copied Data Value equals a Master Data Value "only at the instant of being copied", and is subsequently stale-dated.

RULE: "Change the Master, then re-copy"

PRINCIPLE: "If the Copy is wrong, then the real problem is that the Master is wrong".

5. Data Dictionaries" define the Data Specifications for the Data Positions.

6. Data Maps

"Data Maps" define where the data is stored, especially where the Master Data Positions are.

7. Data Structure

"Data Structure" defines the data entities and associations, and how the data families are assembled.
6. DOCUMENT MANAGEMENT

Consider ...

<table>
<thead>
<tr>
<th>Books &amp; Magazines</th>
<th>Standards</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Characters</td>
<td>alphabet</td>
<td>characters</td>
</tr>
<tr>
<td></td>
<td>numbers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>symbols</td>
<td></td>
</tr>
<tr>
<td>words</td>
<td>dictionaries</td>
<td>strings</td>
</tr>
<tr>
<td>paragraphs</td>
<td>&quot;Rules&quot; for</td>
<td>blocks</td>
</tr>
<tr>
<td></td>
<td>good construction</td>
<td></td>
</tr>
<tr>
<td>books</td>
<td>meet Reader's needs</td>
<td>documents</td>
</tr>
<tr>
<td>libraries</td>
<td>classification systems</td>
<td>storage</td>
</tr>
</tbody>
</table>

"Books" are an assembly of words and paragraphs.

Definitions ...

"A Document is an assembly of strings and blocks".

"For Document Integrity, each string and block must be declared to be either a Master Data Value, or a Copy Data Value, and be managed as such".

"Document Management is the proper management of all Master Data Positions (and Values), for strings and blocks, and Copy Data Positions (& Values), and management of all the Master-to-Copy relationships".

This is illustrated in the following diagram for Document Integrity and Document Management:
B1, B2, B3 are Blocks
SI is a String

is a Master Data Position

is a Copy Data Position

B2 is a Master Data Value
(B2) is a Copy Data Value

The "Operating Manual Doc. #1" in the example is an assembly of strings (SI) and blocks (B1, B2, B3).

In the Doc. #1 document, block B2 is a Copy Data Position, and this contains a Copy Data Value, (B2). The author of Doc. #1 must not ("cannot") change the data value (B2) - the author must copy this from the "AECB" Commitment Doc".

Similarly, the data value (SI), for a string, is copied. However, Block B3 represents a Master Data Position, and contains the Master Data Value B3. In the example, two other documents use copy Data Values, i.e., (B3)'s, and the authors of these two documents must not change the data values of (B3).

"Document Management" comes from managing the strings and blocks, and their associations (i.e., which is the Master and where are the copies? and for each copy, where is the Master and where are the other Copies?).

"Document Integrity" comes from managing the Data Values, so that the Master Data Values are correct, and copy Data Values are always copied from the Master.

Principles ...

"Data Management" is a pre-requisite for "Document Management".

We should start with the basics, i.e., Data Management.

Application software should be judged (assessed) and acquired only if it will help us perform the essential basic tasks of Data Management.

7. CONFIGURATION MANAGEMENT

Consider ...

"Information" is an image of "Reality"

... the drawing is an image of the object (eg., of a pump)

... the performance data is an image of the performance (eg., of a pump's performance)

... etc.

"Configuration Management" is achieved only when Information correctly represents Reality, and reality matches the correct Information".
This is illustrated in the following example:

```
<table>
<thead>
<tr>
<th>Equipment Code</th>
<th>Material Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC</td>
<td>MC</td>
</tr>
</tbody>
</table>
```

1. The Information on the Position and on the function must be correct.
2. The Information on the Part and on the Attribute must be correct.
3. The Attribute must match the Function.
4. The right Part must be in the right Position.
5. The information on the association between the Position and the Part must be correct.

These are the five basic requirements for Configuration Management.

Without Data Management we cannot have Document Management.

Without Document Management we cannot have Configuration Management.

Without Configuration Management we cannot have ... (you fill in the blanks!).

Remember the old saying:

"for want of a nail - - - - - a kingdom was lost".

8. SUGGESTED SOLUTIONS

1. We have to develop and implement Policies & Procedures to define:

   Master Data Sets

   Each to be defined by

   - Master Data Position
   - and Master Data Value
These could initially be in an Application System of choice (arbitrarily chosen).

2. Develop rules for management of Master Data Sets.

3. Develop rules for Copied Data Sets

   Where a Copied Data Set comprises a
   - Copied Data Position
   - and a Copied Data Value

4. Develop Data Directories (Yellow Pages)

5. Develop Data Dictionaries (Data Specifications)

6. Develop Data Architecture

7. Establish the capability to distributed Databases on Open Systems

8. Develop a Data Management Vision, and a Plan to get us moving together towards achievement of the Vision.

9. DEFINITION OF ACRONYMS

   ESP            Equipment Spare Parts
   WMS            Work Management System
   MMS            Material Management System
   BIMS           Bruce Information Management System
   IDMS           Data base by Cullinet, now Computer Associates, on Mainframe computer
   WAN            Wide Area Network
   SAN            Site Area Network
   LAN            Local Area Network

REFERENCES


THE CONTRIBUTION OF AN INFORMATION MANAGEMENT SYSTEM TO ELECTRICITE DE FRANCE CORPORATE STRATEGY

D. SPOHN
Production Transport,
Electricité de France, France

Abstract

The nuclear power plant information system is a chief point in the management of operation and maintenance of the French nuclear plants. In the first part, different issues are examined. These include: (1) creation of the model and standardization, (2) transparency and security of the information, and (3) system operability. Second, the different functions of the information system are presented: The operation subsystem which provides operating personnel with information designed to assist them in their decisions; The maintenance subsystem which is at the center of the information system; The equipment management system designed to provide plants with the material resources; The financial and human resources management system linked to corresponding corporate system. Finally, the main components of the technical architecture are presented to address the different networks, the evolution of workstations, the servers, and the software architecture.

After two years under operation, an information system implemented at EdF has gained the full acceptance of the users and has demonstrated its efficiency not only at a qualitative level but also from an economic point of view.

1. THE NUCLEAR POWER PLANT INFORMATION SYSTEM AND STRATEGY

Electricité de France is currently confronted with far-reaching changes in the European electricity generating system. The company must mobilize its full abilities to react and adapt to the changing environment. Most importantly, EdF must prove its ability to anticipate, in order to offer customers products that are both competitive and of impeccable quality.

Optimum operation of the nuclear installed base is central to meeting this challenge. The strategy defined to achieving this goal is based on three components which provide a framework and a system of reference for assessment of actions to be taken and which guide decisions.

These three strategic components are:

- Improve safety
- Control production costs
- Transform employees into true partners committed to achieving shared objectives

This system of reference totally alters the way in which operating problems are approached. An analysis of the multiple facets of systems is progressively replacing approaches which, in the best of cases, emphasized the craft, or job category, or the immediate result of a task. Or, in extreme cases, work was reduced to more or less pertinent application of procedures or simply established routines.

It is pointless to deny the importance of technical aspects in operating a nuclear power plant but this plant also plays an economic role: People work there and it has an impact on the environment. All of these facets must be considered when actions are taken, however minor they might seem. The importance accorded to each element, of course, varies but no elements can be simply ignored out of hand.
This approach to nuclear power plant operation makes information an essential resource and one which contributes to the success or failure of the company's policies. A global analysis of a given action requires access to all the information required, as well as the ability to efficiently work with this information. Information ceases to be an instrument of power and once again becomes the object of communication.

For a number of years, EDF has applied significant resources to developing its information systems, particularly at its nuclear power plants. In the past, this might have been considered an acknowledgment of passing trends. Today, however, the weight of competition, sociological changes, in particular, the rise of environmental awareness, coupled with shifts in the economic and social context, have totally revamped conventional ways of managing a company. Within this context, the information system becomes a strategic management tool.

The information system is based on the way in which the nuclear power base is modeled. The model is static to represent permanent components or those with a certain degree of performance (such as equipment or structures), and it is dynamic in order to represent and retain transitions. The quality of the model in large part determines the place accorded to the information system in the management process.

Before taking a more detailed look at the structure and content of the system, there are a number of issues which should first be examined.

1.1 The Model and Standardization

The first issue concerns the notion of model. Creating a model to represent a complex system of fifty nuclear power units is an extremely difficult task. Furthermore, the systems-oriented concept chosen requires that a given entity be identified without any ambiguity, whatever the perspective from which it is observed, and that it retain its identity if the perspective changes. Yet, for historical reasons, each job category has driven changes in its organization according to specific rules. Consequently, it becomes difficult to recognize the unity of an object that is handled by different job categories (finances, technical or management, for example).

This problem is aggravated for a system of nuclear power plants since difficulties encountered at the level of a single unit become impossible when the scope is widened to more than one plant. Modeling supposes that the elements in the model have been standardized. Ensuring that such standardization is respected is an organizational problem, as is the management of the information system in general. Unless it is based on rigorously applied standards, the model loses its common language and thus its meaning. It also loses its value if it is not made pertinent and if it does not reflect the evolution of the plants.

1.2 Transparency and Security

The second issue is that of transparency. The information system enables any authorized person to access a wide range of data and procedures, the integrity of which is vital to EDF. Over ten thousand persons have an operational interface with the system, representing a significant risk of accidental (or voluntary destruction).

Since it is out of the question to limit the visibility each person has of the system, since one of the objectives is on the contrary to offer a broader view, transparency is limited only by the authorization accorded to each person. The information system itself and the organization established must, therefore, integrate effective responses to problems of security.
1.3 System Operability

The last but perhaps most important issue involves the size of the information system and its operability. In other words, is it possible to effectively operate a system which is supposed to model each nuclear power unit down to an extremely precise level of detail (approximately 250,000 functional positions per unit, and is it possible for this system to organize experience feedback for fifty units in operation and integrate twenty thousand persons in the information system process?

The solution lies in the type of relations established between the system and the people who use it. If this interface requires strict and sometimes constraining procedures, these procedures should not arise from the techniques employed. Rather, they must reflect the rules and policies required of nuclear operators; otherwise, the system must always provide broad areas of unhampered access within which people can exploit their skills and the information available to a maximum degree in order to achieve the objectives assigned to them.

The solution selected is based on the following simple principles.

1. A set of compulsory "basic laws" designed to maintain the consistency of dialogue from one unit to another and to guarantee respect for policies set at the national level. This set of laws includes the following: Standards used to designate and describe equipment; standards used to define the form and content of documents, and standard accounting principles.

2. Accurately defined and stable procedures which establish liaison with other systems or subsystems that cover specific needs.

3. Responsibility for the information system or its constituents is assigned to the people responsible for the corresponding missions. The information concerning operating policy and applicable to the entire installed base is managed at the national level. On the other hand, each plant is responsible for the information concerning it. Likewise, each person or group of persons is free to use the information to which they have access, so long as communication procedures are respected.

Application of these principles is delicate, and is rendered even more complicated since it takes into account existing information "capital." However, these principles have made it possible for the system to gain acceptance. (The first version has been operational at all sites since mid-1991).

2. FUNCTIONS OF THE INFORMATION MANAGEMENT SYSTEM

The information management system for EdF's nuclear power plants consists of four subsystems, each corresponding to one of the central missions of a nuclear operator: operation, maintenance, financial and human resources management and equipment management.

2.1 Operation Subsystem

The operating subsystem does not have any direct action on the industrial process. It provides operating personnel with information designed to assist them in their decisions. This system, thus, constitutes an operating aid, even though certain data comes directly from the installation; in particular, data which specifies the status of the unit at a given moment.

Among the key functions of this subsystem are:

- Tagging and return to service of equipment to ensure the safety of personnel and equipment
Control conformity to technical specifications following any change in status or modification of configuration

Perform periodic tests, analyze results and keep records

Requalification of installations before returning equipment to service following maintenance work

Fuel management during reactor unloading and refueling

Management of radioactive waste

Management of effluents and their discharge into the environment under normal or accident situations.

All these functions fall within the scope of plant operation, but most do not involve action by operating personnel. In particular, it is evident that tagout or requalification operations also involves maintenance personnel.

One of the first observations made when the system came on stream was that a new type of dialogue was established between categories of personnel with different perspectives, such as operating and maintenance staff. However, this is but one example, and the impact on relations between people, whether they belong to the same functional category or not, has been very strong indeed. The use of an information system reflects a commitment to strengthen horizontal relations between different areas, different jobs and between people. In this example, the system enables people working at different jobs to benefit from complementary aspects without losing the specific nature of their craft.

2.2 Maintenance Subsystem

The first objective of the maintenance subsystem is to manage maintenance operations. This encompasses both operations designed to rectify malfunctions or repair anomalies, and systematic actions taken as part of programs linked to operating periods or the value of certain indicators.

The maintenance subsystem is one of the keystones of the information system. The quality of maintenance and of the analyses performed both upstream and downstream from maintenance actions determine the level of safety and unit capability factor. This subsystem makes it possible to schedule operations and control that they are correctly executed. It constitutes a precious source of information for experience feedback regarding both equipment and procedures.

Among the functions performed by the maintenance subsystem are

- Monitoring of maintenance operations, from issuing of servicing requests (generally by the operating team or automatically issued as part of preventive maintenance), through preparation and execution of tasks and archiving of analyses of work done.

- Costing of servicing work. This cost analysis is performed when technical or organizational options are proposed and continues throughout execution. Accounting actions required are generally performed within different time frames than technical actions, and are integrated in the financial management system. Consistency between the two subsystems is a problem for which the only satisfactory solution is a high degree of standardization of communication procedures and adapted standardization of the entities covered by the system.

- Strict control of procedures must be monitored throughout the work. This includes control of hold points, certifications, checklists, documentation, etc.
Storage of data on operations and analyses performed during work and management of the archiving and information retrieval system.

Another maintenance-related function (even though there are good reasons to consider it as a separate area) is documentation. This function is designed to provide clear, and up-to-date documents to all personnel who need them. The function performs document archiving and updating in conjunction with equipment backfitting or changes in procedures.

The documentation function is employed for a number of activities, particularly at the operational level. Even though it is included in the maintenance subsystem, it must provide people who perform other work with the features they require.

To operate correctly, the maintenance subsystem requires a model of the plant that is complete, accurate and regularly updated. Creating and maintaining such a model is a considerable task, since even though most of the information needed is available, gathering, checking and putting it into usable format can prove extremely costly.

At a minimum, this model must include:

- A detailed description of unit equipment
- A parts list
- All operating procedures for equipment servicing
- Description of rooms and areas where work is performed (in particular, dosimetric characteristics)
- All installation plants and diagrams
- A model of technical specifications.

While this list is not exhaustive, it clearly shows the scope of the problem.

As a key resource for experience feedback, the maintenance subsystem also makes it necessary to define a common language used to integrate information from different sites and to incorporate approved terms whenever applicable. This means that strict rules must be followed in representing the objects treated by the system. These rules cover both the way in which entities are represented and the way in which they are interrelated.

This does not mean, however, that standardization should lead to inflexibility. In particular, the system must be able to easily integrate the specific structure of a given unit. Various ways of organizing work may coexist at the same site and especially from one site to another. These differences are the result of historical factors, the local context and even the individual people working at a site. If they make an effective contribution to meeting the objectives of the overall nuclear power system, there is no reason to favor any one of them. On the other hand, the precision of an information system, and in this instance of the maintenance subsystem, requires that the organization be defined without any ambiguity. If this is not the case, any system malfunction will simply underline the weaknesses of the organization.

The maintenance subsystem is linked to all the other components since management of maintenance requires full knowledge of the status of the unit.

This information covers availability of equipment which is to undergo servicing, availability of the appropriate staff and replacement parts, impact on technical specifications, maintenance costs,
impact on dosimetry, etc. This once again underscores the importance of the comprehensive systems approach described above. An operation cannot be isolated within the scope of a given job category since it involves cooperation among numerous specialists. The information system must, therefore, provide support for dialogue among these different professionals.

2.3 Resources Management Subsystem

The resources management subsystem is designed to provide plants with the material resources (spare parts, special tooling, etc.) and external human resources they need, when they need them at optimum cost. At the same time, it must ensure consistency with the company’s industrial strategy.

This subsystem comprises conventional inventory management functions. For EdF, this management is complicated by the fact that inventory may be spread over several sites. Furthermore, there is centralized management of extremely costly equipment or equipment requiring highly specialized skills.

In addition to conventional functions designed to optimize inventories, the subsystem performs tracking operations related to industrial policy. For example, it controls the conformity of orders to directives applicable to suppliers, costs and types of contracts. It also enables analysis of results achieved by quality control of services and comparison with results at the safety, availability and cost levels.

These tasks are situated on the border between two areas, across which the information system helps establish links. On one side are technicians, whose language is that of equipment or physical skills, and on the other are accountants and financial specialists, whose language is money and interest rates. In each of these worlds, every object has a specific meaning and these meanings could end up being different if certain precautions are not taken.

To establish the desired unity, attention must be refocused on the initial objective. Neither physical actions nor financial actions have inherent value; their meaning results from the fact that they combine to achieve the objectives of safety and optimum costs and from the commitment of people to achieving these goals. The resources management subsystem makes a substantial contribution to enabling a horizontal overview of the operations carried out at a plant. This is one of the reasons for which it is also one of the most difficult subsystems to define and implement.

2.4 Financial and Human Resources Management Subsystem

The financial management subsystem manages the flow of financial exchanges, checks that they are correct and integrates them within the accounting system. It interfaces with the systems which perform these same functions at the EdF corporate level.

The system receives economic data from the other subsystems and integrates it in the accounting system. It is thus able to generate reliable information for employees to enable them to assess the financial value of their actions. To do this, it employs cost allocation rules and checks that these rules are correctly applied. These rules are part of a common language and are used to determine the cost of each action taken. Economic and financial management is, therefore, no longer an instrument only available to accountants, but becomes an indispensable source of information for everyone.

Management of human resources is associated, albeit somewhat artificially, with financial management. This association has both historic roots, but also results from the financial impact of human resources management in the strict sense of the term. In particular, the subsystem performs payroll tasks and management of benefits.
Human resources management has another objective too, which is to guarantee the best possible match between the tasks to be performed and the human resources available. Human resources information encompasses skills, availability, certification and dosimetry for each employee.

The main functions performed by this subsystem are:

- Guarantee that personnel with the skills and certification required are available for a specific task
- Optimize the use of skills during a given period
- Guarantee that dosimetric risks are compatible with the total radiation exposure of each employee
- Manage recording of dosimetry data and calculation of collective radiation exposure data
- Manage access to different areas of the site

These functions are linked to operating activities. There are also others related to long-term skills management such as management of personnel training. Hence, the goal is to enable personnel to adapt to new equipment or procedures and acquire additional knowledge within the scope of individual training plans.

Within the scope of human resources management, training is not an end in itself. Rather, it is part of efforts to foster social and professional development, which is one of the core elements of overall corporate strategy for the nuclear power generating system. The human resources management subsystem has thus been designed to support achievement of the corresponding objectives.

3. TECHNICAL ARCHITECTURE OF THE INFORMATION SYSTEM

The actual information technology resources used for the system play a vital role in managing such a vast flow of information. At the same time, a distinction must be made between the means and the end. The information system contributes to management of the company, while the computer is simply a tool on which the system operates. It is obvious that the power of modern information technology resources enable ambitious objectives in terms of managing vast exchanges of information. These resources also increase the importance of information systems in the way a company is run. Automated procedures, however, must never be considered a substitute for strategy.

There are three main components in the technical resources which support EdF's nuclear power plant information system.

3.1 The Network

The main technical component is a data communications network that links all the entities in the nuclear power plant system.

This network has a dual structure.

There is a wide area network (WAN) which links all EdF units. This network conforms to all open system interconnect (OSI) standards when these standards have been approved. When there are no official standards, it conforms to widely accepted market standards. The network, which is managed by EdF, uses the public data network as its "backbone."
The second level is a local area network (LAN) within each nuclear site. These LANs enable exchange of information between people at the same site at very high data rates. They use the Ethernet protocol, but can also adapt to other protocols or higher data rates if necessary. Gateways link each LAN to the corporate data network.

The network enables any person to access any of the resources connected to the network. While this potential is undeniably one of the main strengths of the system, it is also the source of risks that are far from negligible. Network administration and access entitlement, in particular, becomes a vital task. Any failure in network administration can lead to serious system problems. Special teams at both the site and national level handle network administration. Their mission is to guarantee optimum operation and respect for operating procedures.

In its present configuration, the network is dedicated solely to data transmission. It has the capability to evolve to include other applications, however, including multimedia applications.

### 3.2 Workstations

The workstation is the means by which each person can directly access the information system. The basic workstation consists of a personal computer with an MS-DOS operating system and, to a growing extent, Windows 3 display. This station performs a number of functions:

- Emulation of the protocols used by the mainframes connected to the network to provide access to transactional applications which require substantial processing power
- Communication with servers on line in the local area networks
- Desktop-based applications that enable the user to exploit the information supplied by the system (or from other sources)
- Integration within a department level LAN for use of a database specific to a given team.

Over eight thousand workstations are currently running and connected to the network, accessible by practically all personnel at all nuclear power plants.

### 3.3 Servers

The last technical component comprises the data servers or applications used. There are several different types:

- Large processing systems which run databases and applications requiring large data-handling capacity. These systems have a processing power of approximately 300 imps and generally run around the clock, seven days a week.
- Local servers running under IWIX, which support local databases. This category covers documentation servers, dedicate planning terminals, etc. Like the preceding category, they can be accessed from any of the workstations and are available around the clock.
- Local OS-2 (or comparable) servers to serve the needs of small teams with specific objectives.
3.4 Software Architecture

Like the hardware architecture, the software architecture of the EdF system is varied. Whenever possible, it uses off-the-shelf software or programs which can be quickly adapted to avoid any inflexibility resulting from technical options.

While this is relatively easy at the personal computer level, it is more difficult for the mainframe software, even though standard products have been selected over custom developments whenever possible.

The most difficult problem is exchanging data between systems.

If a global architecture for management of data exchange is not employed, there is a serious risk of proliferation of interapplication data transfer applications, to the point that the system would rapidly become unusable. This risk is further amplified when older applications are retained and when they are situated at points where large amounts of information converge. This is the case with EdF’s accounting system, for example.

This problem has not yet found a fully satisfactory solution, but the fact that the system is based on a global design has led to definition of logical data structure and application architecture. This architecture makes it possible to progressively integrate specific data exchange interfaces and migrate towards client-server type architecture.

4. CONCLUSION

The information system for EdF’s nuclear power plants has become a key, indeed indispensable, management resource. However, this tool is far from complete, and will, in fact, by its very nature never be totally "finished." It evolves along with the installed base and with the company’s objectives and it will continue to adapt to its technical environment.

At the same time, in keeping with corporate policy, it must be possible to assess the real contribution of this system to achieving objectives. This aspect, establishing significant indicators to measure the "profitability" of an information system, is rarely considered. Yet, the substantial investments required to design, develop, operate and maintain such systems should, no doubt, be justified. Such indicators will help keep the system focused on its objectives, reveal its weaknesses and adapt the system to external changes.

After two years of onsite functioning, the information system has gained the full acceptance of its users. The first effects of the system have also been felt: it helps drive the systematic professionalism needed for continuous improvement of the quality of technical and management actions. Its direct impact on costs is difficult to determine so long as the indicators have not been established. However, insofar as the system already makes it possible to determine costs and associate these costs with corresponding actions, it contributes to overall cost control.

Assessment of the efficiency of this system is currently being examined. The results of this study should show that the system not only makes a broad contribution at the qualitative level, it also makes an efficient economic contribution.
DIAGNOSIS SYSTEMS IN NUCLEAR POWER PLANT DEVELOPMENTS AND APPLICATIONS

W. BASTL, L. FELKEL, D. WACH
Institut für Sicherheitstechnologie GmbH (IST),
Garching, Germany

Abstract

With the progress in on-line digital data processing and the availability of powerful process computer systems a new dimension of plant monitoring has been opened. Besides introducing information presentation by color screens and its consequence for control room design, new types of condensed information has been made available by using the potential of computers, e.g. status surveillance, computerized operational manuals, success path monitoring. One of the important items necessary for these new systems are methodologies to recognize the deviations from normal operation or normal behavior of components in an early stage. While on-line early failure detection in the beginning have been developed as separate systems (e.g. process disturbance analysis, vibration monitoring), it has been recognized later that they play a key role in plant monitoring and therefore have to be integrated in the plant information system. In this sense the paper deals with early disturbance and failure diagnosis and outlines developments and applications in German nuclear power plants, with emphasis on work performed at GRS and IST. Beginning with principles of an overall information concept, the methodologies and systems are treated in two main chapters: System/process diagnosis comprising system status surveillance and integrated disturbance analysis, considering also recent progress in developing a real-time on-line expert system, and early diagnosis of component failures or malfunctions comprising vibration diagnostics (passive systems and rotating machinery) and loose parts monitoring. In the appendix basic viewpoints on on-line real-time expert systems are given.

1. INTRODUCTION

By the progress in information technologies and computer systems today, now tools and methods are made available, which can be used for further improvement of reactor safety. One of the important fields under extensive discussion is the enhancement of the man-machine interface, which not only means considering human factors engineered control rooms, but also advanced technical features to ensure adequate information about the status of the plant. Amongst those new features early disturbance and failure diagnosis plays an increasingly important role. This is because knowing about plant deficiencies in status nascent provides the maximum time for adequate countermeasures. Consequently diagnosis has two main goals:

- to inform the plant staff about arising abnormal deviations of processes (and systems),
- to inform the plant staff about the onset of mechanical deficiencies.

The paper deals with developments of the Institute for Safety Technology GmbH (IST), especially with the results of tests of diagnosis systems in an industrial environment and in practical applications. The basic idea is the on-line analysis of selected signal patterns with the aim of assessing the trend of dynamic process behavior or the trend of observed mechanical deficiencies.

2. INFORMATION CONCEPT

In practice diagnosis systems have been introduced step by step in the plants. They have been used complimentary to the traditional informations available in the control room. Envisaging an
advanced control room adequate integration of the diagnosis provided is essential. This is achieved by a comprehensive information concept.

The basic information concept as shown in Fig. 1 is built up hierarchically and can be represented as a pyramid. The top level provides information on the momentary plant status, and the balance between nuclear power generation (core), the heat transfer (primary system) and the heat removal (secondary system). Parameters such as generator power, thermal reactor power, neutron flux, primary pressure, primary temperature, primary steam flow, steam generator water level are logically connected and displayed in pictorial form.

The second level consists of the necessary information about system states. This applies to systems, a disturbed state of which can influence nuclear power production, power transportation or power removal. The cause of the disturbance may be within the special system itself or induced by other (sub)systems. In the demonstration example (see Section 3.2) the information dealt with concerns especially the feedwater system, steam generation and transportation system, the turbine, the condensate system, the main coolant pumps and the pressurizer. Additional parameters reflect the status of important instruments and relevant flows, water levels, pressure and temperatures. The information allows the operator to follow the effects of a disturbance or of (automatically) initiated actions.

The third information level deals with single messages and combines important alarms about reaching of limits and announcement of dangerous situations. This information is to focus the attention of the operator on any disturbed part of the plant even when his interest is in the analysis of a special disturbance path. Besides announcements of dangerous situations especially messages which inform about an approach to a limit or which initiate automatic actions are of importance.

The bottom level of the hierarchical information structure is formed by the detailed disturbance analysis down to the component level. Here preanalysed disturbance sequences are stored within the computer in reference models, if a disturbance occurs the operator can immediately get information about causes and consequences according to the detailed modelling.

While choosing disturbances for analysis to provide examples, we preferred those which need relatively many system parts so as to provide a broad analysis spectrum (tank and balance supervision,
trend detection, supervision of characteristic curves and gradients). On the basis of evaluation of operational experience, first coarse system analysis as well as the possibilities for operator interactions, the following (sub)systems were taken into account: residual heat removal system, pressurizer (coolant pressure control), containment isolation, condenser, main and auxiliary condensation system and feedwater system.

Figure 2 shows all the functions of the IST concept of early disturbance and failure diagnosis. The functions which are highlighted by background shadowing will be described in this paper.

3. SYSTEM / PROCESS DIAGNOSIS

System/Process Diagnosis needs powerful computerized operator support systems. Experience shows that such support systems will be accepted by operators only if they are continuously applicable and not only during certain safety relevant occurrences. This is especially true for early disturbance and failure detection, where those systems must also be helpful for "normal" operation. We therefore have to bear in mind power operation (including load follow operation) as well as startup/shutdown operation.

---

**System / Process Information Concept**
- GENERIS program package
- Integrated Disturbance Analysis
- Symptom Oriented Display of Disturbed Plant Situation
- Status Surveillance of Components and Plant Systems
- Alarm Reduction
- Post Trip Analysis

**Component / Partial Process Surveillance Concept**
- COMOS, MEDEA, ROMADIS, RAMSES
- Vibration Monitoring of Passive Primary Components
- Acoustic Monitoring of Loose Parts, Leaks
- Anomaly Detection of Thermohydraulics
- Rotating Machinery Monitoring of MCP, Shaft, Vibration
- Sensor Surveillance of Malfunction, Time Response
- Active Safety System Monitoring

---

MCP: main coolant pump

Fig. 2: IST concept of early disturbance and failure diagnosis in NPPs
A major prerequisite for information conditioning and condensation with regard to early failure and disturbance detection is the provision of possibilities for complicated signal processing. This is made possible by modern computers and color graphic screens. The whole range is available starting from simple logical signal combinations up to on-line numerical models of complicated control algorithms.

The GENERIS (generic information system) program package [1] was established by GRS. Based on this, five different applications were realized in co-operation with a plant manufacturer (Siemens/KWU) and utilities (NPPs Biblis B and Philippsburg II):

- symptom oriented display of disturbed plant situations
- status surveillance of components and plant systems
- alarm reduction
- post-trip analysis
- integrated disturbance analysis.

Original software development costs for each of these functions would be in the order of US $2 million. Using the GENERIS software package the development costs can be reduced to about 20% of this figure. All applications have been realized in such a way that they can be extended on the basis of additional system analysis.

The presentation of the task oriented condensed information is given by corresponding color graphic pictures (on raster displays). Two of the functions realized are of major importance for early detection of failures and disturbances and will be described subsequently. Recently GENERIS has been used as a basis for the development of an expert system working on-line and in real-time. A general description of expert system paradigms & technology is given in the Appendix.

### 3.1. System status surveillance

A major technical process such as nuclear power plant operation nowadays comprises about 10000 - 15000 binary and 1000 - 2000 analogue values to be measured for surveillance, monitoring and disturbance detection. To enable the presentation of a complete overview of the plant status on a color graphic screen and to keep and update a high degree of information, condensation before presentation is necessary. To achieve this goal all signals which describe the status of a component are logically combined in a "status vector". Each of these status vectors may be combined with its technologically corresponding partners to form a new status vector which then describes a higher level system.

In an application for the nuclear power plant Philippsburg a total of about 600 of those status vectors has been defined by the plant vendor (Siemens/KWU). All of these vectors are combined into a corresponding status signal for each functional unit. As the vector is represented in a "status word" (16 bit), the display system can easily utilize the information provided on components and functional units to determine colors and other status information in plant schematic diagrams. For example, information on the status of a pump (on/off), external/internal fault, power operation/startup/shutdown and also on whether a signal is plausible or not is given by the status vector.

Status monitoring is particularly useful for the evaluation of the type and severity of a malfunction, for assessment of the affected or still available functions and for identification of the most effective means of intervention (success paths). The status vector approach represents the new destination oriented philosophy (with the human operator in mind) as opposed to the traditional origin oriented philosophy which displayed whatever was considered relevant at the design stage [2].
3.2. Integrated disturbance analysis

For this application, disturbances, i.e. any kind of deviation from the desired operational status of the plant or of its components, are registered. Considering the history of signal values, especially the gradients of analogue values, it is possible to detect such disturbances from the very start. Using preanalysed models for disturbance sequences, operator support is provided for diagnosis as well as prognosis. Normally only those sequences are modelled which provide enough time for the operator to initiate actions to rectify the disturbance or at least mitigate the effects.

In order to achieve these goals it has been necessary to build up a function oriented information structure and a hierarchical presentation scheme which has been realized with color graphic overview pictures and trend curves. They have been oriented to the information concept described in chapter 2. The realization of the integrated disturbance analysis is furthermore based on a pilot project (Grafenrheinfeld NPP) which was carried out some years ago [3]. The information goals remain unaltered (namely detection of primary causes and prediction/estimation of possible consequences) except that now emphasis has been shifted to early disturbance detection. This was possible because, in the application at the Biblis B plant, we had direct access to analogue process variables which - as opposed to the Grafenrheinfeld application - permits analysis before some fixed limits are violated.

Of these applications "integrated disturbance analysis" was chosen for this paper in order to illustrate the type of pictures presented to the operator [4]. Figure 3 gives an example of how the time behavior of measured analogue variables can be presented. The left part of the picture displays a set of variable names from which the operator (or the system itself) can choose a subset of four variables for presentation. For the selected subset the course of the last 30 minutes is shown as well as a prediction for the next 15 minutes. If the actual value has reached a given distance from a limit the actual absolute distance in digital format is inserted in the picture as well as the calculated time until

![Fig. 3: Picture of transients (integrated disturbance analysis).](image-url)
the limit will be reached with regard to the current gradient. Additionally, text may be highlighted in information windows. Figure 4 gives a pictorial overview of the status of the systems of the secondary side: steam generation, l-vat, and coolant transportation of a PWR. The measured values of the main variables are shown (e.g., as bar graphs or as digital values) as well as information on subsystems status and as to whether the necessary signal correlation still persists. The severity of a disturbance is indicated by a colour coding according to three classes. Further on specific symbols are used to indicate the degree of deviation from normal and the positive or negative trend (gradient) of the parameter presented.

The application was tested with actual process data of an NPP during a disturbance (loss of main heat sink). The main result was that valuable additional information can be given to the operator. The next steps of development will be the implementation of a picture hierarchy and an explanation module to give the operator the opportunity to go into detailed subsystem information presentation in case of subsystem faults.

3.3. Real-time on-line expert system

Research work carried out at GRS [5] has resulted in a prototypical expert system integrating the features that are discussed in the Appendix. Fig. 5 shows the outline of the expert system which operates in an on-line environment, i.e. it gets most of its data from a technical process (the nuclear power plant). As the results must be available in due time it is also required to operate in the real-time domain.

![Fig. 4: Overview picture (integrated disturbance analysis).](image-url)
The system itself is event-based and generic in the sense that it can be configured to fulfill a variety of different informatical goals. Some are listed below according to increasing complexity:

- Alarm Reduction
- Post Trip Analysis
- Dynamic Operating Manual
- System Fault Identification and Analysis
- Success Path Monitoring
- Living PSA
- Qualitative Simulation and State Prediction

The system can be used interactively or non-interactively as the function requires. Interaction means the user is supposed to supply (user-)events to the system whereas in the non-interactive case events are received only by the process or the system internally. Such a generic expert system basically consists of three main event sources:

- process events
- user events
- internal events.

All these events are based on associated objects. Process events report about changes in the process. User events initiate some actions or queries in the expert system. Internal events are the result of stimuli either from the user or the process that had to be postponed (e.g. a pump takes 15 secs. to build-up full pressure and so an alarm should only be given if this state is not achieved after that time). A model to represent this could look like in Fig. 6. Internal events are stored in the so-called internal event queue which is embedded at the interface between the models and the reception of process and/or user events respectively.

---

**Fig. 5: Outline of the structure of a dynamical expert system**
In the example given in Fig. 6 an event E1 is generated at time t. This event is listed in the internal event stream for showing up at time t+15 [secs]. Of course, chances are, the conjunction C1 may not hold any more as the pump might have been closed down again. In such cases the element E1 is simply removed from the internal event stream. It should also be noted that these streams applied to our models or rather objects, possibly produce another event stream which can in turn be applied to other objects and so on. Thus the models not only serve to monitor basic events but may be regarded as a filter that conveys only important events to a higher level. This property makes the concept especially adaptable to hierarchical approaches in either the temporal, topological or functional domains.

In conclusion, building an expert system for application to large technical processes requires software paradigms far beyond "rules". Limitation from the "rule"-paradigm cannot be accepted. The dynamical requirements in on-line and real-time applications need to be satisfied by an integrated and homogeneous concept. This is not only necessary to cut down software development costs but even more so because of licensing and verification problems [6]. However, the power of today's hardware and the great progress in interoperability yields good prospects for the future. A full-fledged system based on the prototype mentioned above is being developed by IST.

4. EARLY DIAGNOSIS OF COMPONENT FAILURES OR MALFUNCTIONS

Similar to the systems discussed before, which provide better information about the overall status of the plant by means of process parameter trends and system disturbance analysis, major progress has been achieved also as regards surveillance and early failure detection at the component
and equipment level, by applying modern signal analysis methods and advanced computer technologies. Methods demanding high data compression and high storage capabilities can be applied today economically.

Single or small faults in components may exist and remain undetected or may be non-relevant during normal power operation, especially in a fault-tolerant system such as a nuclear power plant. However, either potential subsequent failures or demands, in abnormal environmental or process conditions (during an accident) can develop into a more severe situation. An early warning of such defects or malfunctions can reduce this risk; the countermeasures can be performed without time problems and stress. It is essential for a realistic safety philosophy concept to concentrate efforts in developing surveillance and diagnostic systems for components and equipment, since with modern computer technology, the necessary prerequisite is there allowing powerful and nevertheless economical solutions.

Concerning the mechanical state of the plant, in the past there was little or no direct information to the operator; he rather had to draw his conclusions from the process behavior supplemented just by a few sensors indicating the status of active components. In the seventies research work sponsored by the German Federal Ministries BMFT (research and technology) and BMU (environment and reactor safety) has been performed by GRS and the industry with the aim of developing methods and systems for on-line assessment and diagnosis of mechanical structures in the primary system. In particular, emphasis was placed upon the early detection of mechanical deficiencies of reactor internal and primary circuit components. Indirect measuring methods based on acoustic, vibration and process signal noise analysis have been developed successfully.

Loose parts monitoring systems are available in all German nuclear power plants, vibration monitoring in all PWRs. Safety standards require these systems and repetitive analyses. The importance of early failure detection (EFD) methods has to be seen in the light of the non-accessibility of most components during operation and of the radiation exposure of the inspection and repair personnel during shutdown of the plant. Hints from on-line measurements localizing mechanical deficiencies as precisely as possible are of utmost importance for providing spare parts in time and for preparing the repair strategies. Safety and availability can be increased considerably when EFD systems are applied correctly, i.e. when careful and detailed signal analysis is performed. For a long time GRS has concentrated its efforts in this area, in order to enhance the precision and reliability of signal interpretation with respect to potential mechanical faults. Current activities are directed towards

- gathering operation experiences from different plants in suitable data banks,
- building up a detailed knowledge base for interpretation of signal patterns and feature trends and
- enhancing effectiveness by applying more automated and "intelligent" systems on site.

In Fig. 2 the different methods of the IST component surveillance concept are summarized on the right hand side. Typical for all methods is the use of stochastic primary information; as a consequence much more effort has to be placed on signal analysis and interpretation as compared to "normal" reactor instrumentation. Depending on the problem, analysis methods either in time or frequency domain are applied. Very often essential information is taken from the interrelations between different channels (correlation analysis, burst pattern analysis), a typical property of multisensory systems which generally are coming into use in machinery and process diagnostics.

The overview in Fig. 2 shows the different noise diagnostic methods which have been or are being developed at GRS/IST for early failure detection of components or in partial processes. Amongst them there are methods such as sensor surveillance (signal validation), leakage detection, anomaly detection in processes, active safety system monitoring. In the sequel vibration and loose parts monitoring will be discussed, since these methods are already used extensively in practice. Their benefit has been demonstrated impressively by successful diagnoses and, just recently, considerable improvements achieved regarding the man-machine interface.
4.1. Vibration and loose parts monitoring

The sensor and instrumentation concept of vibration monitoring systems (SÜS) and loose parts monitoring systems (KÜS) has been published several times [7-12]. The instrumentation and signal conditioning of the SÜS are genuine multisensory systems, in the standard version consisting of a combination of 20 vibration sensors (four absolute displacement gauges at the reactor vessel, 16 relative displacement gauges at the loops), eight ex-core neutron detectors (noise) and three dynamic pressure gauges in the reactor coolant. Extensive work performed during preoperational tests and at-power measurements with correlation and long-term investigations in several plants as well as theoretical 3-loop and 4-loop model investigations have led to a broad and detailed knowledge base: The vibrational behaviour is represented now by means of fully interpreted power density spectra with the mechanical vibration of components allotted to the measured peak frequencies. Acceptable or non-acceptable (failure-caused) trends and margins of peaks and coherences have been determined or estimated.

Meanwhile a number of successful diagnoses led to a high acceptance of the SÜS analyses by the utilities and the supervising authorities. Examples of such diagnoses [8] are the predictions of failed hold-down springs at the flange of the reactor vessel and of loosened screws at the secondary core support (flow baffle). Both failure warnings could be given months before the next refuelling so that the repair could be well prepared. Other examples are described in [11] presented at the SMORN V conference: Relaxations of the hold-down spring forces, for instance, could be detected and predicted in two plants.

The loose parts monitoring systems (KÜS) are multisensory systems consisting of a set of accelerometer gauges distributed between the reactor pressure vessel (six sensors) and the steam generators (at least two sensors at each generator). The system monitors for metallic impacts within the pressure retaining boundary using the audible frequency range. Delay times of bursts in different channels and the shapes of these bursts are used for loose parts location and energy/mass estimation by the analysing specialist. For that purpose the burst patterns of actual impacts are displayed with a high resolution, for related signals in parallel. The patterns have to be assessed and interpreted using the theory of stress wave generation (Hertz theory) and pulse propagation in solid structures and by means of experimental results of reference impact tests with known impact energies and impact locations. A number of events and successful diagnoses performed in the last 15 years have led to a broad acceptance of this diagnostic technique [12].

4.2. Recent developments regarding the man-machine interface of noise diagnostic systems

In recent years GRS/IST has collected an enormous number of noise signatures of plants with different size and power, of normal and abnormal process conditions, of operationally influenced or failure-caused deviations, of KÜS burst patterns, of feature trends etc. For SÜS and KÜS, data banks have been established at GRS/IST enabling a fast access to reference signatures for comparison purposes. This continuously growing knowledge base can be used to consult the utilities or authorities and to assist them in signature interpretation as well as in current research activities directed to the development of automated knowledge based diagnosis systems.

The following questions have been investigated in order to improve early failure detection based on noise diagnostics:

- How to ensure fast access to the GRS/IST signature data banks in order to assist the on-site personnel in interpretation?
- How to transfer the centralized know-how to the plants and to install more intelligent systems on the site?
- How to automate the monitoring and signature storage procedures?
- What are the needs for signature and feature presentation and which communication capabilities are needed for the man-machine dialogue?
4.2.1. Vibration and noise diagnostics

Considerable progress has been made; especially the man-computer interface has been improved. For vibration and noise signals, GRS/IST is able now to provide three methods of assistance in data analysis:

- For older plants without advanced systems the signals are synchronously recorded in pulse code modulation (PCM) technique on magnetic tapes and analysed at the IST Analysis Centre (this has been a standard procedure for several years). Using the code package IRAX all auto and cross-correlations of up to 32 channels are calculated with just one short computer run. The results are stored on a matrix tape and can be displayed on a CRT. The dialogue capabilities have been improved considerably. All desired functions, coded in different colours, can be superimposed by the analyst on a colour graphic screen and interpreted with respect to deviations from stored reference functions. The functions needed for the documentation are plotted.

- Between the GKN-1 plant and the IST Analysis Centre a test and demonstration system for remotely controlled fast data transmission has been established using the public telephone network. Whenever anomalies are detected on the site or when interesting operational conditions occur, data transfer for up to 8 channels with 9600 baud can be started. The interpretation using the IST signature data bank can be done immediately in the laboratory [13].

The third possibility is a very successful, mostly applied development of GRS/IST, the condition monitoring system COMOS (see. Fig. 7 and [9]) which means an "intelligent" system with monitoring, storage and diagnosis capabilities on the site and only transfer of reduced data to the IST Analysis Centre (using tape cassettes, telefax, etc.). Statistical quantities (discriminants) are used for feature monitoring and following trends within allowed bands of deviations. These properties seem to be important especially for fast escalating failures (e.g. shaft ruptures in main coolant pumps), but also the on-line monitoring of all the normal SÜS signals can be performed automatically in a second mode (with a lower calculation rate). COMOS systems are already operating in seven PWRs (GKN-1, GKN-2, KKG, KKI-2, Biblis A, Biblis B, KKP-2), a further system is in use in the BWR KKI-1 monitoring the vibrational behaviour of the steam turbine.

4.2.2. The Condition Monitoring System COMOS

As a first step in developing COMOS, a detailed investigation of discriminants was performed. Twenty-seven discriminants were tested to see whether they could be used effectively for comparison of actual and reference features in the vibration spectra. By applying artificial and real noise signals, deviations in frequency, amplitude and peak width were investigated with respect to reliable monitoring properties.

The hardware of COMOS consists of commercially available equipment. The heart of the system is a modern 32 bit computer in conjunction with a two channel frequency analyser. Up to 32 signals can be monitored automatically. In the spectra of each signal up to ten frequency bands with adjustable bandwidths (features) can be determined. Margins are set individually around learned reference states. The trends of the different features (coded by different colours) are displayed graphically below the spectra. Daily and monthly trend curves can be shown as well as single spectra, quadruple spectra or waterfall representation of spectra history, etc. (menu driven functions).

Two monitoring modes were implemented: in mode 1 signals with possibly fast escalating features are monitored (e.g. main coolant pump vibrations, 16 calculations per day for 16 signals), in mode 2 the other SÜS signals (one calculation per week for 32 signals). The presentation of the results to the operator is in highly concentrated form, taking into account human mental capacity for optical correlations (Fig. 8):
2-channel frequency analyser
32-channel multiplexer
isolation amplifiers
multi colour plotter
colour video monitor
keyboard
printer
streamer tape
hard disc
32-bit computer

Fig. 7: The IST Condition Monitoring System

Fig. 8: Standard display of COMOS (coloured screen)
- the actual spectra of four related signals (i.e. belonging to the same component) are displayed on the screen simultaneously, each together with its reference band (in dark colours) as determined during the learning phase;

- related features in the four spectra (e.g. belonging to the same vibration mode) have the same colours, allowing a fast check, to see if the amplitude has changed (electrical distortion or real phenomenon);

- trend curves of all discriminants calculated from each feature in corresponding colours below the spectra as daily trends, markers for plus and minus thresholds, date and clock for exact time correlation of events.

These are the standard displays automatically switched from one group to the next. Once a day all spectra and trends are plotted on one document (status plot).

By use of a new information correlation (linkage) matrix, rules for vibrational relations in various signals and frequency bands can be programmed to realize diagnose properties. Step by step the comprehensive and still growing knowledge base can be implemented in on-line monitoring, so that in a not too far future a diagnosis system in the sense of an expert system for vibration and anomaly monitoring will be available.

4.2.3. Loose parts diagnostics

For the analysis of KÜS signals the computer based MEDEA system (Fig. 9) is used in the IST Analysis Centre. It consists mainly of a 16 channel transient recorder, a 32 bit UNIX workstation with CRT and mass memories [12]. Burst pattern data are transferred by FM magnetic tapes, streamer tapes and floppies to IST. In addition if needed modems and telephone lines can be used.

![Diagram of the IST system MEDEA](image)

Fig. 9: The IST system MEDEA
The burst patterns are classified with respect to different features and stored in the data bank, by application of the digital RAMSES system. RAMSES consists of four transient recorder storage modules, controller, modem and graphic display and is based on an automatic computer communication to the MEDEA analysis system. Since the system can be set up on request in a temporary way at the plant, the analog techniques, used in older German plants, can be supplemented in an effective manner. RAMSES contains software packages for remote controlled settings of the transient storage modules via the telephone line, for storage of the data to the onsite computer after event detection and for data transfer of qualified signal patterns to the IST Analysis Centre.

For that purpose the patterns at first are displayed on a colour screen, allowing the specialists to identify and determine the features. By use of the cursor the values are fed into the computer, which provides the necessary information for diagnosis. Software packages for location and mass estimation are available. Figure 10 shows the result of an impact location in a steam generator using vessel development and hyperbolic graphs.

5 CONCLUSIONS

By applying modern computer systems, methods for early detection of disturbance and failures have been developed:

- at the system and process level,
- at the component and partial process level.

Emphasis has been placed on high information compression and good ergonomical visualization of diagnostic results. Various systems developed by GRS/IST together with utilities and industry have been presented, which have been tested successfully on the site and are now already

Fig. 10: Impact location with MEDEA
applied in German nuclear power plants. Extensions are possible with respect to monitoring of other systems, processes and components and with respect to further transfer of more "intelligence" to the on-site systems, i.e. continuous supplementing of the knowledge bases and implementing of further feature linkage rules. IST is working on these objectives.

The provision of expert knowledge and automated failure identification capabilities will make available powerful diagnosis systems which can assist the operator at an early stage, when disturbances or faults are arising in the plant. The systems described form an important basis for reliable operation. This contributes to the performance and safety of nuclear power plants.

REFERENCES


About ten years have gone by in which artificial intelligence became a serious candidate eligible for industrial applications. This is due to the fact that first of all computers have become fast enough to process high-level programs and also because goals have been clarified and semantics have been shaped so that problems could be described and solutions derived and implemented.

The classical expert systems (i.e. the rule-based ones) have shown their applicability to many domains, but at the same time exhibited their limitations with regard to their expressive power. Many paradigms popped up to satisfy particular requirements. Integration efforts were strong, yet, the universal expert system has not been discovered (will it ever be?).

To make things even worse, because hardware permits, on-line and real-time applications would enter the stage of possible realization, were it not for lack of methodology to keep up with the dynamical behavior and consistency maintenance in the time domain. In the sequel it is attempted to clarify some of the basic aspects and to show possible solutions to the problems of real-time process monitoring, diagnosis and prediction.

Most of the proposals originate from research work in the field of reactor safety in Germany. Even though the plant or process usually is a nuclear power plant of the 1200 MWe PWR or BWR type, the results can be applied to any continuous (non-batch) process.

One of the major components of the approach outlined in the sequel is the process model as one would say in the simulation field. In the expert system domain one rather talks of knowledge-bases and inferences. In the following chapters the equivalence of these concepts is outlined and the necessity of integrating them.

1. PROCESS MODELLING

Building models or knowledge-bases is necessary to gather knowledge about the components of a process and their interaction. Therefore, the knowledge can be classified into structural and functional knowledge, respectively.

The process must satisfy some goal to be considered as meaningful. A nuclear power plant must produce power at an acceptable level of safety.

A complex process or plant can only be realized by decomposing it into smaller sub-processes that interact with each other. Fig. 1 gives the generic decomposition of a nuclear power plant. The achievements of the main goals is assumed to be composed of the achievement of subgoals. Apart from the fact that this allows for redundancy it also accounts for the provision of contingencies, i.e. goals can be reached in several ways. The plant must be started-up, operated, and shut-down, i.e. it operates in different plant modes.

A model that represents the behavior or the structure of the process can give the operator more transparency of what is going on, what is going wrong, what may be going wrong, and what can be done to rectify something that is going wrong.

2. MENTAL MODEL VERSUS KNOWLEDGE MODEL

When operating the plant, the responsible personnel is informed via symbols derived from process instrumentation. From their education and training the operators have developed a so-called mental model, i.e. a good idea of what, given one state of the plant, it should be in next. The
subsequent state can be verified by comparing the changes in the instrument readings with the expectation (prediction) from the operator's model. Although operator error and human factors exist this has shown to be a very reliable configuration. However, it can be improved using knowledge models.

Instrument readings tend to be rather limited: lights of different colors, gauges etc. in the old times, CRTs with textual as well as graphical information nowadays. All only work because a distinct mental model of the operator exists. The operator can only associate in his mind, he cannot see the results of his derivations. Chances are, his performance is improved not in the least from a reliability point of view, if some way can be found to replicate and visualize his own inference. Here, knowledge models can be very helpful.

3. WHAT IS A KNOWLEDGE MODEL?

First of all we must ask, how a process can be described according to specific aspects. Fig. 2 shows known process description paradigms and attempts to relate them.

We start out at the process of which an image or model is constructed. We have basically two categories: structural and functional. The structural models replicate the system topology and allow to answer questions like "where is a specific component", "what are its attributes", when was the last check-up", "how can maintenance or repair be organized". The integrated plant management system (IBFS) [1] is an example which uses such a model (Fig. 3)

The characteristics of such models are they are dynamical in the sense that they provide slots into which information can be entered or changed. The main initiator of such changes is the personnel and as such the frequency in depth* of such changes must naturally be rather low. However, due to the fact that many people may access such a system in parallel, the mutual exclusion problem must be observed and the frequency in breadth may be quite high. (Frequency in depth vs. frequency in breadth refers to the chronological changes in one objects as opposed to the relatively simultaneous changes in many objects.) So, this situation very much resembles a data-base application. Nevertheless there are significant differences to pure data-base applications: the degree of implications between objects, e.g. one item may not be updated unless some prerequisites have been satisfied, or, the updates of the items must be performed in a chronological order. As we can already see, the degree of object orientation is significant. We will come back later to this subject.
Fig. 2: Process description paradigms

Location: Plant  
Workshop  
Inventory

Events:
- Pump has damage and needs to be exchanged
- Issue order and check prerequisites
- Authorize execution of task
- Remove pump
- Move X1 to workshop
- Move X1 to inventory
- Move X2 to Workshop
- Move X2 to plant
- LAB10(X2) moved in place
- Install LAB10(X2)
- Test equipment
- Report completion of task
- Plant subsystem can be restarted

LAB10(X1)  
LAB10(X2)  
LAB10(X1)  
LAB10(X2)  
LAB10(X1)

Fig. 3: Events recorded in an Integrated Plant Management System (Example)

The example in Fig. 3 deals with a problem of a damaged pump in the feedwater circuit of a PWR. We assume that there were means to identify the situation. As a consequence this pump must be replaced in due time to avoid unnecessary plant outage. Because there are three redundant pumps of this kind in the PWR, two of which need to be operational, a plant shutdown is not required for the time being.

The pump is identified by X1 to avoid confusion with the pump with which it should be replaced, i.e. X2. The pumps are all listed in a database with specific attributes, especially their location. The problem then is to devise a plan for replacement, observe constraints and monitor the carrying-out of the plan. This plan essentially consists of a succession of events, necessarily chronologically ordered. At every point in time, the responsible management is informed about the state of the task executing and about the whereabouts of the respective pumps. The pumps are listed as records in the database. These records change attribute (location of X1 changes from plant to workshop to inventory, whereas X2 goes the other way round). However, it would not be possible to replace pump X1 by X2 unless X1 was removed prior to the task of installing X2.
Even though, the concept used here is already very powerful it has its shortcomings as it does not integrate the items (database records, objects) and events in the plan, and because it does not take events from the process directly into account (for instance, something may happen that is prohibitive to the continuation of the plan). Moreover, the IBFS is realized on the basis of a commercial database system which also includes limitations from its implementation.

4. FUNCTIONAL MODELS

A process or a component thereof is something that "works" in a specific way. We can see this either by the result it produces (like machines that move, or some product that is being brought to existence) or we have to measure parameters that are otherwise invisible, to make them perceptible to the human senses. The main sense utilized is vision. We can see current and voltage on meters and gauges, as well as pressure, levels etc. The interactions or relations of these parameters tell us whether the process works, i.e. performs its intended function. We can describe these relations either because we used them to design the process or we have, after the construction of the process, found certain characteristics in the relations of these parameters.

There is no unique way of description of the behavior. The description is governed by several parameters the most important of which is purpose, i.e. we must know what we would like the description to use for. Another one is degree of required precision.

A classical term for the description of the process behavior is simulation or, more precisely, simulation model. Simulation models can be represented in several ways. Two of the most important are mathematical or physical.

4.1. Mathematical Representation

A mathematical representation of a simulation model abstracts the process with regard to the key parameters. The interactions of the key parameters can be described by equations. There are two main characteristics of a process that are also reflected in their (mathematical) representations; statical and dynamical. A statical system can be expressed in terms of algebraic equations. Dynamical systems are determined not only by the present state, but also by their history. They are mathematically described by differential equations.

Mathematical descriptions of the process behavior have one significant advantage: They can be evaluated either symbolically or numerically. No matter which way is used, a computer can perform this task, fast and precisely. If one succeeds in solving the questions symbolically, things are fine. However, very few systems are so linear to yield to this approach. If we solve the equations numerically we have to find a compromise. The discretion process imposes precision constraints as well as reliability limits on the prediction. The important fact, however, is that a transformation from infinitely many states (phases) to a finite number takes place.

This is what we all reach for, as the human can only deal with a limited i.e. finite number of steps, states, items etc. Nevertheless, the number of states may still be enormous and therefore further attempts exist to reduce this number by grouping into taxonomies. We can either reduce the grid frequency at the expense of decreasing precision or we can try to apply specific criteria to "filter" the state sets. One such filtering method is known a qualitative simulation [2].

4.2 Qualitative Representation

The semantics to these criteria are that when some function is monotonically increasing or decreasing, we have, more or less, a constant derivative which, in turn, such is the underlying assumption, means that there is certainly a change going on in the process. But, by and large, this
change is not all that interesting. However, the beginning or end of such a monotonic phase is considered important. These points are called landmarks. For example: A pump is turned on and as it transports liquid the level in a container, as a result, is rising. The vicinity to rule-based expert systems at least as far as the result is concerned, is quite obvious. Rules like

IF pump is turned on THEN level is rising

can be found in many example applications. There is an additional advantage though, since the derivation process of these rules follows some kind of formalization [3] and is bit purely heuristic as is the direct construction of the rules.

On the other hand, one cannot fail to see the degree of imprecision induced by such an approach. At a basic level these relations may be quite helpful. One cannot guarantee though, that the combinations automatically also yield correct results. The qualitative simulation approach also shows that rule-based systems must necessarily be very imprecise unless their premises and inferences are of rigorous boolean nature and applied to a process of this kind (e.g. an interlock system). This approach, as well as sign algebra [3] etc, may yet be used for coarse derivations of important categories.

In the defence-in-depth concept with respect to nuclear accidents one can imagine situations where details do not matter so much any more rather than global categories into which current situation can be classified. Here, this approach may be quite helpful.

4.3. Physical Representation

Just for the sake of completeness physical representation of a simulation model is mentioned. This has been done via analog computers and is not so widely used any more. Even if physical models are patched, they are rarely performed physically. Rather, they are transformed in a digital scheme and then evaluated numerically. So, we again end in a mathematical representation.

5. REQUIREMENTS

What then are the requirements we must subject an expert system to that is supposed to yield information or even knowledge about a technical process?

First of all it must be event oriented. This is due to the fact that the system must react to events (i.e. changes in process states) from the process. Another event source is the user of the expert system (usually the operator). Both these sources very heavily depend on one key parameter: time.

Events are tied to time points (or more precisely, time stamps). This, as a consequence, has the advantage that they can be ordered chronologically. If we have several streams of events (chronologically ordered sets of events) we can merge these into one, again chronologically ordered, stream. This does naturally yield a mechanism for synchronization of different event sources. This is very important as there are at least two event sources that need to be synchronized: the process and the user of the expert system.

The inferential state of knowledge-base can change without user intervention on account of events from the process. Moreover, the state of the knowledge-base can change without any intervention from outside (i.e. neither from process nor user). This is due to the fact that dynamical systems are capable of storage (or memory). In practice, this implies that an event from the process need have impact on the output only after a specific time delay. Therefore, the paradigms for representing the knowledge in the knowledge-base are required to include semantics of this kind.
Something that would be very helpful: A paradigm that allows for the description of topological, temporal, mathematical and qualitative knowledge alike.

6. THE EQUIVALENCE OF "EVENT" AND "MESSAGE PASSING"

In the sequel it will be shown how the software paradigm of object orientation has dynamical knowledge-base and inference capabilities.

An object is a collection of items (variables, structures, etc.) and procedures. The procedure can be invoked by passing a message to the object (if there is more than one procedure the message must be qualified by the respective procedure it is to invoke). Procedures can again pass messages to other objects and so on. Although, in a normal software environment, it may not be very desirable to create loops in this way, it is crucial in expert-system applications to technical processes. This is due to the fact that the processes usually consist of many control loops that must also be reflected in the knowledge-model. However, passing a message from one object to another, conceptually takes no time. In control loops though, feedback does take (conceptually and practically) time, however small. This means the messages must be kept somewhere for later use.

We can define objects that represent a basic mathematical function like AND or ADD (mapping into the boolean or real domain). The object has as many receptors as there are parameters to the equivalent mathematical function and produces an event or message if the previous value of the function changes on account of the change of at least one parameter. Unlike the classical object orientation all objects have a state that depends on time, i.e. each object has a time-stamp on it.

Viewing every part in an equation as a (functional) object, we can build an object tree of this equation. The functional decomposition of the equation yields a predecessor-successor relation on the objects. This implies that especially for very complex mathematical functions (as are found in simulation models) only the path that accounts for the changes need to be traversed by passing the respective messages. Thus, a significant gain in performance can be achieved.

As process events are tied to process variables, i.e. those physical entities that permit the visualization of the process, it is straightforward to define these as objects with the value of the physical variable at time \( t \). Whenever a change occurs, the object is passed a new message with the new value and new time-stamps. If the object has successors tied to it, the value is passed on, until no more changes occur.

6.1. Objects and Database Items

As objects have attributes, they are eligible for treatment as database items. However, unlike database records, where only two main operations exist (add, delete) because changes in records are rather rare (e.g. a customer record in the customer database changes when there is a change of address). Moreover, the change history is usually taken care of in the computer environment (e.g. backup strategies on the files). As opposed to this, objects can be used to dynamically (but virtually) form database records. These virtual records serve all query requirements including those like "How often has the customer’s address changed", a query that affords to dig into the object’s change history. Because a conceptual paradigm to treat such situations exist in object orientation, a natural embedding of such queries can easily be achieved.

6.2. Relation of Change History to Process Event Streams

Process event streams are essentially a set of chronologically ordered change records, i.e. each change in a process variable creates such a change record and so does each change initiated by the user of an expert system. Thus, from such an event stream, given an initial configuration, all changes
can be reproduced. Moreover, viewing each event as an incarnation of a specific object, queries can very easily be extended to the time domain. Also, all queries referring to time relations can be modelled like "what happened in the last hour" translates into "return all objects with NOW - 3600 [sec] < time-stamp > NOW.

NOW is a very special concept, as it refers to the present that is not a fixed point in time. Rather, NOW "moves with Time" and therefore, a query like the one above does not stop returning objects as long as something is happening or until it has been cancelled (on account of a user event, for instance).

REFERENCES


CORE MONITORING SYSTEM FOR VVER-440 NUCLEAR POWER PLANTS
F. ADORJÁN, L. BÜRGER, I. LUX, M. MAKAI
J. VALKÓ, J. VÉGH
KFKI Atomic Energy Research Institute, Budapest, Hungary
I. HAMVAS, Z. KÁLYA
Paks Nuclear Power Plant Company, Paks, Hungary

Abstract

The core monitoring system VERONA, developed for the Hungarian VVER-440 Nuclear Power Plant is presented. After a short overview of the instrumentation available for monitoring purposes, the hardware and software configuration of the original and of the upgraded VERONA versions are described. It is shown that the services offered by the system satisfy an extremely broad range of the possible operational needs. It is concluded that the present version, the VERONA-u represents the state-of-the-art reachable in conjunction with the VVER-440 nuclear power plants.

1. INTRODUCTION

For the safe and efficient operation of a nuclear power plant capable and reliable core monitoring is essential. For this reason extensive research and development has long been initiated in the KFKI Atomic Energy Research Institute, Budapest and the results of this program are the successive generations of the VERONA core monitoring system.

Replacing conventional methods of core monitoring by the VERONA system is a reliable way to improve safety and economics of power production by VVER 440 nuclear power plants. In order to facilitate the operator's comprehension of the actual core status colour display monitors are applied for data presentation in the unit control room. All the necessary information is at the operator’s disposal in any particular operational condition, without an excess amount of superfluous data. All the four operational units of the Paks NPP are equipped with the VERONA core monitoring system. The system is operational since 1985 at Units 1 and 2 and since 1986 and 1987 at Units 3 and 4, respectively. The upgraded version VERONA-u system is running parallel to the original one at Unit 1 and will be fully operational in 1993. Detailed information on the VERONA systems is available in References 1 through 7.

2. INSTRUMENTATION AND PRIMARY PROCESSING

The core instrumentation is based primarily on in-core self-powered neutron detectors and assembly outlet thermocouples. The Rhodium self-powered neutron detectors (SPNDs) are arranged in strings, each string consists of seven SPNDs and one cable for detector cable-current compensation. The SPND strings are located at the central tubes of the fuel assemblies, there are altogether 252 detectors in the core (in 36 different fuel assemblies at 7 elevations).

The temperature of the coolant at the assembly outlet is measured by 210 thermocouples (TCs). The TCs are connected to 12 temperature compensation boxes which form the cold junctions of the TCs. The temperature of the compensation boxes is measured by resistance thermometers and the cold junction compensation is automatically performed by the software.

In addition to in-core measurements, core performance monitoring is relying on a number of other measured values such as ex-core neutron detectors, boron concentration, temperatures, pressures,
flows in the cooling loops, etc. The actual status of the reactor system is further characterized by a number of digital data corresponding to the condition of valves, pumps, control rods, etc.

In the original system the measurements were collected by the intelligent HINDUKUS data acquisition system consisting of analog multiplexers and A/D converters. A complete set of measured data is forwarded by the HINDUKUS system to the VERONA system in digital form in every 16 seconds.

In the upgraded version of the core monitoring system the HINDUKUS system is replaced by a distributed data collection and primary signal processing system, called PDA. The PDA consists of five measurement cabinets, each containing a number of standard VME modules for primary data acquisition, and a 20 MHz, 32 bit Motorola processor with 4 MByte RAM and 1 MByte EPROM for primary data processing and forwarding to the VERONA system. The important measurements are introduced into two PDA cabinets thus minimizing the loss of information in case of a hardware component failure.

The upgraded system scans cca. 700 analog and 360 discrete signals with a processing cycle tuneable depending on the actual VERONA computer. The typical cycle time for a MicroVAX 3100 computer ranges from 2 to 4 sec.

3. THE HOST COMPUTER CONFIGURATION

The first generations of the VERONA core monitoring system run on a TPA-11/440 megamini computer with 3 Mbyte operating memory, with two 80 MByte discs, magnetic tapes and two colour display monitors. A CAMAC interface system and 16 channel synchronous multiplexer serve the connection of the host computer with the data concentrator and operator interaction devices.

In the upgraded version two MicroVAX 3100 computers (with 28 MByte RAM, 1.2 GByte SCSI disc and 1.2 GByte streamer tape each) running under VMS operating system form the hosts of the VERONA system. One of the host is the 'active' system, the other, running parallel to the first one serves as a hot standby. Both computers have active links with the PDA's through a doubled Ethernet network. Four DEC station 320sx PCs, with 4,6 MByte RAM and 20" 8 colour-layer SVGA monitor each, serve for displaying purposes and also for the operator interface.

4. THE VERONA SOFTWARE SYSTEM

The VERONA software system consists of a number of real-time tasks and service (utility) programs. The highly modular program system has been particularly tailored for VVER-440 type reactors. The measured information is preprocessed by performing primary validity checking, lienarization, scaling and filtering.

The ultimate goal of the processing of the measured information is the reconstruction of the three-dimensional power distribution in the core and the determination of the heat generation in each fuel assembly. There are several parameters which are subject to limitations depending on the actual operational status of the reactor (characterized e.g. by the number of operating main cooling pumps or the total reactor power). The variation of the limits due to such changes are automatically taken into account by the software. For example, the maximum assembly power, as well as the maximum assembly wise power peaking factors are subject to operational limitations. These maximum values may occur in non-measured assemblies, therefore it is essential to give reliable estimates for every fuel assembly. In the VERONA system the estimation is based on the 210 assembly outlet temperature and 252 SPND measurements as well as on theoretical information elicited form the reactor calculational model.
The 3D power distribution, assembly wise coolant heat-up, power and burn up distributions and many other distributions are presented in the form of colour coded, as well as of numerical valued core-maps, printed reports and event logs. The system collects and stores on magnetic tape all the necessary information required for subsequent re-evaluation of the core states at any time.

In the upgraded version VERONA-u the database handling has been shifted to a new, object oriented base. The main idea behind the VERONA VOX Database approach is that modification of existing element or introduction of new elements should influence the existing codes as little as possible. Besides, the possibility of defining new abstract objects via arbitrary set operations makes the use of the database extremely flexible.

The quality of the man-machine interface (MMI) is a key issue in the acceptance of an operator support system. When designing the upgraded VERONA system considerable effort has been invested into the selection of MMI tools as well as into the determination of the screens and figures presented to the operators. When establishing a user friendly and easy-to-use MMI, the application of the X Window system was evident. The DEC station PCs are used as X-terminals, the host computers perform the necessary operations and the standard X client-server model is implemented.

5. VERONA SERVICES

The main services of the system can be summarized as follows:

- displaying the assembly wise power distribution at ten elevations of the core
- displaying the assembly wise coolant heat-up distribution
- displaying a number of other important assembly wise distributions and quantities (such as burn-up, limit violations, invalid measurements, distributions scaled with respect to safety limits, etc.)
- presenting the Safety Parameter Display screen
- displaying the axial power distribution in selected assemblies
- presenting detailed data on selected assemblies
- scanning, sorting and presenting event lists
- selecting, preparing, listing and printing various logs
- preparing high resolution colour, or grey-scale hard copies
- preparing long-term data and event archives
- displaying on-line and archive trend curves of any variable in the system
- displaying detailed information on every attribute of any object in the system
- supplying detailed help on the system usage
- interactive play-back facility for analysing archived events
- opening DEC term terminal sessions
- flexible and exhaustive database handling and displaying system running parallel to the on-line processing
- versatile archives managing and sorting facility

6. SUMMARY

On-line core monitoring is a standard practice at all four units of the Hungarian Nuclear Power Plant, Paks for almost a decade. During that time both the operators and the constructors of the VERONA system have gained a great deal of experience of its application. Based on this experience on one hand and on the contemporary hardware and software tools on the other hand a great step has been made to match the international state-of-the art level by the development and installation of the upgraded version VERONA-u. The importance of the VERONA system in the reliable and safe
operation of the plant is generally acknowledged by its users, and we have every reason to believe that
the upgraded version - the capacity and services of which make it unique among the VVER core
monitoring systems - will again become an indispensable tool of the reactor operators in Hungary.

7. REFERENCES

[1] ADORJÁN, F., et al.: Experiences with the VERONA core monitoring system recently
installed at Paks NPP, KFKI-1985-96 Report, Central Research Institute for Physics, Budapest,
1985.

Research Institute for Physics, Budapest, 1986.


Mtng. on Reactor Physics and Shielding, Chicago, USA, 1984.


[6] VÉGH, J. et al.: Upgrading of the VERONA Core Monitoring System at Unit 2 of the
Tokyo, Japan, 18-22 May, 1992.

COMPUTER-BASED OPERATOR DECISION AIDS

Y. SHINOHARA
Systems Safety Department,
Nuclear Power Engineering Corporation,
Toranomon, Minato-ku, Tokyo, Japan

Abstract

This report describes briefly recent trends in the development of computerized operator decision aids, taking Japanese efforts as examples. The major functions developed in the five year project of COSS (Computerized Operator Support System) included standby system management, disturbance analysis and post trip operational guidance functions, which utilize extensively computer-driven CRT displays. Some of the technological achievements of this project are being applied to commercial nuclear power plants under construction. More sophisticated technologies have been developed in the eight year project of MMS-NPP (advanced Man-Machine Systems for Nuclear Power Plants) using artificial intelligence techniques. These included the development of knowledge-based management, operation method decision support and intelligent man-machine interface systems.

1. INTRODUCTION

The research and development activities in Japan to utilize the efficient and flexible information processing capability of digital computers for nuclear reactor operation began in the early sixties using research reactors and an experimental power reactor. Then routine utilization of on-line process computers in commercial nuclear power plants was commenced at the beginning of the seventies for collecting plant data, monitoring process variables and evaluating plant performances.

More systematic effort to improve the man-machine interface systems for safer and more efficient operation of nuclear power plants by application of on-line computers was made in the Improvement and Standardization Program which was initiated in 1975 with the support of Japanese government and jointly implemented by utility companies and LWR manufacturers with the aim to enhance the reliability of reactor components and thereby to improve the availability of nuclear power plants.

This effort was further intensified after the TMI accident in the five year project to develop a nuclear power plant operation management aid system (NUPOMAS) carried out from 1980 to 1984 with the support of the government. This project consisted of the development programs of automated surveillance systems and instruction systems. The latter included the development program of computerized operator support systems (COSS) to provide operators with relevant information on the operational status of the plant by intensive use of digital computers together with computer-driven CRT display units.

Following the NUPOMAS project, a new government-supported eight-year project for the development of advanced man-machine systems for nuclear power plants (MMS-NPP) was started in 1984 with the aim to improve further the technology of computerized operator decision aids by applying rapidly developing artificial intelligence techniques such as knowledge-based system techniques. The development of such advanced systems requires more extensive use of advanced hardware as well as software technologies of modern computers.

The historical trend [1] in Japan of the development of operator decision aids and other related technologies is schematically shown in Fig. 1.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Stage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Main Theme in C &amp; I</td>
<td>Introduction of Technology</td>
<td>Enhancement of Reliability</td>
<td>Improvement in Monitoring</td>
<td>Enhancement of Ope. &amp; Mainte. Support Function</td>
<td></td>
</tr>
<tr>
<td>Control Room Panel (CRP) Development</td>
<td>Conventional CRP (Domesticated/Improved)</td>
<td>New CRP</td>
<td>Advanced CRP (under development)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration of Information</td>
<td>Use of Color CRT</td>
<td>Advanced Cabling Techniques</td>
<td>Optical Data Transmission</td>
<td>Optical Data Transmission Network</td>
<td></td>
</tr>
<tr>
<td>Plant Automation</td>
<td>High Reliable Digital Control System</td>
<td>Digital Control of Main Operating Function</td>
<td>Integrated Digital Control Network</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supporting System</td>
<td>Normal Operation Guidance</td>
<td>COSS*</td>
<td>MIS-NPP**</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*COSS: Computerized Operator Support System
*MIS-NPP: Advanced Man-Machine System for Nuclear Power Plant

Fig. 1 Development of operator decision aid systems and related technologies.
2. DEVELOPMENT OF COMPUTERIZED OPERATOR SUPPORT SYSTEMS (COSS)[2-6]

2.1. Objective

The objective of the COSS program was to develop the technology of computerized operator
decision aids for BWRs and PWRs

(1) to aid operators in recognizing the situation quickly and easily and taking proper actions in
case of anomaly under various operational conditions, and

(2) to reduce operator's workload during various operational states of plant and thereby to prevent
erroneous judgment and operation.

For this purpose, prototype systems for BWRs and PWRs were developed and tested for
verification and validation using the man-machine interface systems connected to the corresponding
real-time plant dynamics simulators.

2.2. Major Functions

Various functional systems for operator decision aid were developed in the COSS program.
The major functions of the COSS are shown in Fig.2 in relation to the operator's role and plant
behavior. The major functional systems of the COSS will be described briefly taking the case of
BWRs as an example.

2.2.1 Standby-System Management

The objective of the standby-system management system is to monitor the standby status of
the engineered safety features during normal operation in order to assure their proper function at the
onset of emergency situations. If any failures are found in the engineered safety features, the system
provides operators with appropriate guides for corrective actions such as surveillance, repair and plant
shutdown according to the technical specifications. As a part of its functions the system provides the
surveillance test guide and stores the test results for evaluation of the functionability of the engineered
safety features.

The engineered safety features covered by this system include the emergency core cooling
system, emergency power supply, auto-depressurization system and reactor core isolation cooling
system.

The main functions of the standby-system management system are:

(1) standby status monitoring including the responses to operator's inquiry,

(2) repair management of the engineered safety features such as the repair time limit
management and the admission of repairs upon inquiries from operators,

(3) surveillance test management including the surveillance schedule and the guidance of
test procedures.

2.2.2. Disturbance analysis

The plant subsystems covered by the disturbance analysis system (DAS) are selected mainly
from the view point of the subsystem's contribution to plant unavailability.
### Operator's Role

<table>
<thead>
<tr>
<th>Operator's Role</th>
<th>Plant Setup</th>
<th>Accident &amp; It's Mitigation</th>
<th>Securement of Plant Safety Function</th>
<th>Accident Convergence</th>
</tr>
</thead>
</table>

### Plant Behavior

- Normal Ope. Condition
- Plant Set-up
- Equip. Failure
- Accidental Condition
- Scram Activation
- Emergency Shutdown
- Safety Systems Activation
- Secure Core Cooling Ability
- PCV Integrity

**Fig. 2** Major functions of the COSS in relation to the operator's role and plant behavior.
According to the evaluation of operating experiences of BWRS, the following subsystems were selected for the development of DAS:

- main steam system,
- reactor coolant system including the recirculation flow control system,
- feedwater system including the reactor water level control system,
- condensate water system,
- circulation water system,
- turbine system including the turbine pressure control system,
- generator system.

The DAS is divided into two parts. One is the on-line part which consists of four main modules: i.e. the plant data acquisition module, the disturbance detection module, the disturbance analysis module, the man-machine interface and the data-base supporting these functions. The other is the offline part which consists of the data-base editing module. The on-line part coupled with the plant interface functions in real-time.

The input signals from the plant are sampled periodically by the plant data acquisition module. The disturbance detection module checks periodically whether or not the limits predetermined for each signal have been violated, and identifies the off-normal variables. The off-normal variables are registered into the plant status table and the disturbance detection module activates the disturbance analysis module. Using the plant status table, the disturbance module determines the prime cause of the disturbance, recognizes current plant status and evaluates further possible propagations. As the result of the disturbance analysis, message identifiers and display control flags are registered into the message control tables.

In the man-machine interface, the relevant information is selected from the message file according to the message control table and is displayed to the plant operators on color CRTs.

2.2.3. Post-trip operational guidance

The objective of the post-trip operational guidance is to support plant operators in performing diagnosis and corrective action after plant trip. Since the disturbance analysis technique is generally suitable for small perturbations in plant behavior, large transients after plant trip seem appropriate to be treated by a separate methodology. The functions of the post-trip operational guidance system are to monitor the performance of the engineered safety features, to identify the plant status and to provide guides of appropriate corrective actions for plant operators to achieve safe plant shutdown.

The guidance system consists of two parts. One is the monitoring and diagnosis system for the performance of the engineered safety features and the status of the plant. This system is further divided into three subsystems:

(1) protection system monitoring and diagnosis,
(2) engineered safety features monitoring and diagnosis,
(3) plant status monitoring and diagnosis.
The other is the operational guidance system which is grouped into two classes, the one treating the reactor pressure vessel and the other treating the primary containment vessel.

The reactor pressure vessel guidance system aims to provide plant operators with necessary information regarding the appropriate actions and their timings. This information is derived by applying the rules stored in the guidance system to the plant status obtained by the monitoring and diagnosis system.

The primary containment vessel guidance system also aims to provide plant operators with necessary information regarding the protection of the primary containment vessel, which is an important barrier for external radiation release during abnormal plant situations.

The functions of this guidance system are to monitor the primary containment vessel status using the process variables, to obtain the information on the functionability of various means and to decide the priority of various means taking account of the demand from the reactor pressure vessel guidance. The information processing scheme of this guide is the same as that of the reactor pressure vessel guidance system.

3. MMS-NPP PROJECT [7-11]

The MMS-NPP project, started in 1984 and still at R&D stage, is essentially the continuation of the above mentioned COSS program for further development of the operator support system technology by introduction of more sophisticated techniques such as knowledge-based system technique to expand its application area, as shown schematically in Fig.3. The goals of the MMS-NPP project are:

(1) Support of flexible planning of operation during plant startup, shutdown and load following.

(2) Support of efficient and reliable management for plant operation and maintenance.

(3) Support of detection of anomalies in the plant, identification of the plant status and provision of appropriate operational countermeasures.

(4) Realization of user-friendly and intelligent man-machine interface matching with the operator's cognitive process.

The main role of the MMS-NPP is to support operators' decision making under various operational situations of a plant. Since the operators control the plant by using their knowledge of detailed functions of the plant as well as the expertise obtained from their operational experiences, such knowledge is to be installed into the knowledge base of the MMS-NPP and is used for inference in executing operator decision support functions. The functional scheme of the MMS-NPP is shown in Fig.4.

3.1. Knowledge-Base Management System

The knowledge-base management system supports engineers in building efficiently a large knowledge-base used in the MMS-NPP. The knowledge inputting support function is used to obtain the heuristics from experts of plant operation and maintenance work and the so-called deep knowledge existing in plant system design documents and drawings. The knowledge-base verification function maintains the integrity of the knowledge-base by examining for completeness and consistency of the knowledge. The knowledge edition function transforms the verified knowledge into an on-line knowledge-base so as to maintain high speed processing performance, which is required for on-line
inference. The framework of the knowledge-base management system has been established and the key techniques for building the knowledge-base of MMS-NPP have been identified.

MMS-NPP: Advanced Man-Machine System for Nuclear Power Plant

COSS: Computerized Operator Support System
SVC: Supervisory Control System

Fig. 3 Operator decision aid systems.

Fig. 4 Functional scheme of the MMS-NPP.
3.2. Operation Method Decision Support System

The operation method decision system comprehends plant conditions, decides operating methods and procedures and then generates operator guidance information. The system supports normal plant operation, anomaly and accident management and maintenance work planning by using simulators when the estimation or prediction of plant state is needed.

3.2.1. Normal Operation Support Function

The normal operation support function includes the supports for the operation planning such as the reactor re-startup planning during unplanned shutdown and the supervisory control during startup, shutdown and load following operations based on the predetermined operation planning. These operation planning and supervisory control activities require quick search and evaluation of the plant status and operational constraints which require processing of a large amount of operational data within a short period of time.

The normal operation support function also includes the support for inspection and management of a large number of components including the standby components of safety systems which must be ready at any time to respond to the startup demand and therefore must be monitored and dynamically tested at appropriate intervals for their proper functioning.

3.2.2. Anomaly and Accident Management Support System

The anomaly and accident management support function provides detection and diagnosis of plant anomalies and offers relevant operational guides for corrective actions by using the knowledge of the plant structure, plant functions, plant operation expertise and so on along with the results of plant state change predictions. In order to cope with the events beyond the scenarios of anomalies and accidents, the knowledge-base in this support function must provide knowledge representations of the plant functions compatible with the operators' mental model of the plant so that cooperation between the operators and the computer system may be made smoothly.

3.2.3. Maintenance Work Planning Support Function

The maintenance work support function provides the maintenance workers with the guides for maintenance procedures and an optimal schedule for the maintenance tasks, including isolation of the problematic components based on the judgment of the interferences among tasks and between tasks and of the plant operation that are inferred by this function.

3.3. Intelligent Man-Machine Interface

Design of the man-machine interface or operator interface is very important in the development of the operator decision aids as a whole because operators can utilize the support functions only through it. The operator support functions may not be utilized properly unless the man-machine interface system is well designed from the human factor view point. The intelligent man-machine interface is designed

1. to accept the operator's requests and to evaluate the operator's focus of attention and the plant status leading to appropriate information to display, and

2. to provide the information in easily understandable form by applying multi-media communication,

by using a voice recognition system, CRT units with touch-screens and so on. It includes dialogue management, information edition and presentation functions.
The dialogue management function consists of voice recognition, required input processing and query understanding sub-functions. The voice recognition sub-functions accepts the operator's voice commands instead of multi-step manual inputs and interprets the sentence structure, context and meaning of discourse to understand the operator's interest. The required input processing sub-function accepts the input requirement through push-buttons and touch-sensitive screens. The query understanding sub-function performs the control of smooth dialogue between the man-machine interface and the operators.

The information edition function decides the information to be presented in accordance with the plant state and the operator's request history.

The information presentation function provides appropriate information to the operators in an easily understandable manner using oral and visual presentation.

4. NEW OPERATOR INTERFACE SYSTEM

The technologies developed in the above mentioned development projects are to be introduced gradually into the advanced light water nuclear power plants. They are implemented after careful verification and validation tests performed using plant dynamics simulators with participation of the veteran operators from utility companies. The design of the operator interface system in the control room of the next generation nuclear power plants has been changed to a large extent from the conventional ones by introduction of these new technologies.

As an example, Fig. 5 shows key features of the operator interface system in the control room of the Advanced BWR [12] to be put into operation in Japan in the latter half of the nineties.

Fig. 5 Operator interface system of ABWR.
4.1. Operator Interface System and Function

The operator interface system consists of a main control console for the primary operator control and monitoring functions and an integrated wide display panel to presents an overview of the plant status.

4.1.1. Main Control Console

The main control console, from which the total plant is controlled for all phases of operation, includes touch-screen CRTs, flat display devices and a limited number of switches as the primary operator interface devices.

The primary means for operator monitoring and control is provided by the seven color-graphic CRTs mounted on the main control console. The CRT displays are driven by the redundant plant process computer system. There are many types of formats which can be displayed on the CRTs. These include summary plant status displays, trend plots, system status formats, alarm summaries and operating procedure guidance functions. Although each CRT is assigned a default display for a given operating condition, the operators have the flexibility to select any display on each of the seven touch-screen CRTs. This multi-redundant display capability ensures continued normal plant operation in the event of a failure of one or more of the CRTs.

The system status displays provide information on individual plant systems. The touch-screens on the CRTs provide direct control for nonsafety-related systems at the system component level.

The alarm summary displays support the operator’s decision-making process. The presentation of alarms employs optimization techniques designed to suppress nuisance alarms which require no specific operator action such as the audible alarms associated with the reactor protection system during the period of a reactor scram.

The main control console also provides flat displays for extended monitoring and control capability. These touch-control flat displays are driven by microprocessor-based controllers which are completely independent of the plant process computer system. This diversity of displays and controls in the console design enables continued plant operation even in the unlikely event of a total loss of the redundant process computer system. The flat display devices are used to support both safety and nonsafety system monitoring and control functions.

In addition to the touch-screen CRTs and flat display devices, the main control console is equipped with dedicated hard switches located on the horizontal desk surfaces of the console. These dedicated switches give faster access and feedback to the operator than the software-driven, touch-screen controls on the CRTs and flat displays.

4.1.2. Wide display panel

The wide display panel, located directly behind the main control console, provides summary information on plant status, critical parameters and key alarms to the operators, supervisors and other technical support personnel in the main control room. It includes a fixed mimic display, a variable display, top-level plant alarms and touch-control flat displays. Spatially-dedicated alarm windows for critical plant-level alarms are also provided on the wide display panel. At the base of the wide display panel there are multiple touch-controlled flat display devices for individual system surveillance, monitoring and control. The purpose of the wide display is to provide information on overall plant status during all phases of plant operation.

The fixed mimic display, arranged on two adjacent upright panels at the center and right-hand sections of the wide display panel, is driven by microprocessor-based controllers which are independent of the plant process computer system. Information on this panel includes critical plant
parameters provided by safety-related systems. Specific information displayed on this panel includes the status of the core cooling system, reactor pressure vessel and core parameters, containment and radiation parameters, and the status of safety-related equipment. The information displayed completely satisfies the requirement for post-accident monitoring without the need for any other display equipment.

The basic purpose of the variable display, located on the left upright panel of the wide display panel, is to provide information on important plant process parameters which supplements the overview information on the fixed mimic display. The variable display is driven by the plant process computer system. Therefore, any display format available on the main control console CRTs can also be displayed on the large variable display. Examples of the full color graphic displays that can be shown on the variable display are the various safety parameter display formats which would be selected under plant emergency conditions. The information presented on the large variable display can be changed depending on the plant operating condition and the needs of the operators.

The touch-controlled flat displays provide the capability for surveillance of systems and equipment during normal plant operation. In addition, these devices can be used for monitoring and control of plant system during maintenance and refueling outages and also during periods when a portion of main control console may be taken out of service for maintenance. These flat displays are driven by microprocessor-based controllers which are separate from the plant process computer system.

With the new operator interface system together with the computerized operator support system and the enhanced plant automation capabilities, the role of the operators will primarily be the monitoring of the status of individual systems and the overall plant and the progress of automation sequences rather than the traditional role of monitoring and controlling individual system equipment.

4.2. System Configuration

The basic configuration of the operator interface system is shown in Fig.6. Multiple levels of redundancy are incorporated into the system for high availability and to ensure that component failures or system disturbances will not adversely impact plant operation.

The touch-screen CRTs on the main control console are driven by the redundant process computer system. Communication between the process computer and the plant system controllers is primarily provided by the plant-wide networks for data acquisition and control using fiber-optic multiplexing system. Separate networks are provided for safety-related and non-safety-related plant systems. Communications with the process computer are provided exclusively via the non-safety-related portions of the multiplexing system.

The non-safety-related, flat displays on the right-side of the main control console are driven by dedicated controllers which are independent from the process computer. System-level control switches on the main control console are connected directly to the system controllers without interfacing with the plant process computer system.

The safety-related operator interface devices on the left-side of the main control console communicates directly with the divisional controllers of the plant protection systems. Four separate divisions of safety logic and control, including four separate, redundant multiplexing networks, are provided for absolute assurance of plant safety.

The variable display is driven by the plant process computer system while the fixed mimic display, top-level alarms and flat display devices on the wide display panel are all driven by dedicated controllers which are independent of the plant process computer system, thereby providing additional redundancy and diversity in the main control room displays and controls.
5. CONCLUDING REMARKS

The surprisingly rapid progress of the computer and the related technologies has made it possible to develop sophisticated technology of operator support system for safer operation of complex nuclear power plants. The activities of developing the COSS and the subsequent MMS-NPP are good examples.

However, the introduction of new and sophisticated technologies into nuclear power plant operation generally takes a long time before their practical application because it requires careful verification and validation as well as the considerations of not only technical and economic factors but also human and organizational factors such as the shift of the role of operators in the increasingly automated plants.

ACKNOWLEDGEMENT

The author wishes to express his sincere gratitude to Dr. K. Monta of Toshiba Corporation, Drs. T. Kiguchi of Hitachi Ltd. and Dr. Y. Fujita of Mitsubishi Atomic Power Industries, Inc. for providing reference materials.

REFERENCES


COMPUTER-BASED SUPPORT FOR OPERATION,
MAINTENANCE AND MANAGEMENT

A. ANDERSSON
Swedish State Power Board
Ringhals Nuclear Power Station,
Väröbacka, Sweden

Abstract

Computer-Based support for operation, maintenance and management at a nuclear power plant, will in
this report be exemplified by describing the routines at Ringhals Nuclear Power Plant. Ringhals Nuclear Power
Plant on the Swedish west coat, is the largest power station in the country. One of the two government-owned
nuclear power plants in Sweden. The plant, with it’s tree PWR and one BWR unit, produces approximately 25
billion kWh a year, which is 16% of the total electricity production in Sweden.

1. RINGHALS INFORMATION SYSTEM (RIS)

RIS is the administrative computer- based information system developed by Ringhals Nuclear
Power Plant as a support system for operation, maintenance and management of a nuclear power
station.

RIS gives support for almost every function at a nuclear power plant. The system is run on
a main-frame computer (UNISYS 2200/423). RIS includes all applications on the main-frame
computer. RIS is the general and basic support for everyone.

RIS is a terminal oriented information system. The first functions have been in practical use
at Ringhals since 1982. The system has during the years become a more and more complete computer
support.

The 1200 employees at Ringhals continuously use the system from 800 terminals at plant.

1.1. User functions

The main menu showing all subsystem assists those new to RIS. When you have entered
(logged in) to RIS you may freely (if you are authorized) move around and directly get information
from all administrative routines.

RIS is designed for those not expert at typing. It includes an intelligent use of function keys.

RIS replaces most paper forms. Directly on the terminal you enter your budget, order or
request of spare parts, request of external order, report a fault, create a work order, request access
authority for contractors and visitors.

By RIS also most printed lists and reports are replaced Information and reports can be
searched and created directly online at your terminal. Most terminals and PC:s have local printers.

1.2. Construction principles

RIS is based on one common database. The different sub-systems are logically linked together
by e.g. component designations, project numbers, order numbers etc.

RIS has a standardized user-interface. All subsystems are build up by using a few standard
screen-layouts, which are efficient for entering and updating basic data and for searching and
presenting information respectively. The user-demands for new application will always be formed to
fit into the standard.
Each type of screen (user function) is created by predefined database structures and programs. A few different solutions can be chosen depending on the volume and frequency of updating and on the data volumes.

Most reports and information can be obtained directly online. Optimized search files are normally used for presentation. The files are separated from the database for the basic data. Standard modules are used to update the search files online or in batch daily or weekly depending on the demands. In this way the presentation module can be used in the same way for all information, independent of if the basic data is handled in RIS or in a subsystem.

Presentation of information in RIS is structured in two ways:

- according to the demands of the basic function
- as prepared and aggregated information according to business demands and according to the need at different levels within the organization (for low-, mid- and top management).

A common report routine is used for RIS. All reports can be started by using one online function. You specify selection conditions, layout, sort order, printer etc. The last example of each report is stored in the database as documentation. You may e.g. select a subsystem and by paging get actual examples of all existing reports.

The construction principles make RIS a system designed for handling large data volumes with high performance. Standardized screens, programs and database structures in separated modules make fast and simple developing and maintaining RIS applications.

1.3. Function areas

The RIS program is divided into six main information areas: Maintenance, Materials Administration, Finance, Personnel Administration, Executive Information and Specific Nuclear Power Systems. Each area will briefly be described further on in the report.

To make information more easy to use, the general presentation of information from the different functional computers are also included in RIS.

2. COMPUTER BASED ADMINISTRATIVE SUPPORT AT RINGHALS

2.1. Technical base

A general communication network (Ethernet, TCP/IP) is gradually build up at Ringhals. It replace an old star type network. The new net is the base for the actual information structure.

All computers, e.g. process computers, local servers and the administrative mainframe computer are connected to the net. By connecting a PC or a UNIX workstation everyone should be able to reach all relevant functions and data.

2.2. System structure

The computer based administrative support at Ringhals is build up at three levels, the main-frame with Ringhals Informations System, functional computers and local/personal computing.

Ringhals Informations System (RIS)

RIS is the main-frame computer support at Ringhals.
Functional computers

The main-frame based support is complemented by local computers for specific functions, e.g. process computer, company accounting, salary routines, access control, dosimeter control and evaluation, valve testing etc..

Most of these computers are logically connected to the main-frame applications. Input data for various applications are created and maintained in RIS. Data for presentation is periodically transferred to RIS.

Normally a limited number of end-users work directly with the systems. General search and presentation of information is done within RIS.

Local/personal computing

Each group or office have their terminals (PC) connected to a local PC-server. The servers are mostly used for local computing at office and personal level based on standard PC products as word processing, graphic presentation, spread sheets and project planning.
Information searched and presented in RIS can be transferred as input to the different PC products. Data transfer from RIS to PC can be controlled by applications or spontaneously.

End-user interface

To make the administrative support more user-friendly, all applications on the different computers are (or will be) run under the WINDOWS user interface.

That means e.g. that an end-user can simultaneously run RIS (the main-frame applications) and different local applications in different windows on his terminal. He can use standard WINDOWS functions as cut and paste.

3. MAINTENANCE

3.1 Summary

The RIS maintenance system includes production systems, outage and operation planning support, engineering project planning and property maintenance routines. The component data base forms the foundation of the maintenance system. This contains information for all power station components (pumps, monitors, ventilation fans, instrumentation, etc.). The component number is the key to the information. Other maintenance information is tied to the component data base. Online the following information is obtainable via function keys:

- Technical documentation (drawings, instructions and handbooks) and administrative documentation (maintenance instructions and reports).
- Work orders (work-in-progress and reported faults).
- History (previous controls, observations and faults of respective component).
- Preventive maintenance and outage program (contains collected experience regarding the needs of each component, and current official standards to be met).

Work orders and permits (to carry out work) are created for the annual outage with the help of the preventive maintenance data and the engineering project data. All work is scheduled automatically using the outage plan. Requisites for outage in the form of work orders, permits, shut-downs and schedules are printed out.

3.2. Outage planning

We get the real benefits of the different basic data bases when we make use of the integration between the systems. One example is the handling of outages.

During autumn and winter the operation, maintenance and engineering departments prepare their subsystems for the next outage.

The operation department creates and checks their shutdown areas (isolations, padlocks). The shutdown areas define how to stop different functional areas for maintenance. In RIS is registered which activities have to be carried out to stop respectively take in operation a shut down area. For each area a list of components which can be maintained during a stop is entered.
For each unit there are several hundreds of prepared shutdown areas comprising smaller or bigger areas. The system gives the operators a proposal, which shutdown areas are appropriate to use based on the actual workload. Maximised maintenance work should be done with minimized administration and work for the isolations.

The maintenance departments adjust the outage program within the system for preventive maintenance (PM). Adjustments are based on experience from last outage, information from other plants and demands from the authorities.

Planning and modification of workorders and the PM-program can be entered efficiently. You request a selected and sorted list of the wanted activities. By using function keys you get the fields you want to update presented as columns in the list. Then you may do paging and updating of one page (15 activities) at the same time.

The engineering department creates together with operation and maintenance the program for modifications during next outage. Construction is made for decided projects. All work supported by the systems for projects and technical documents. The installation activities relate to the work order routines.

3.3. Outage work

A month before the outage all workorders will be created from the PM-program and from the project system for installation activities.

Based on the workload for the outage the system makes a proposal, which shutdown areas are appropriate to use. The operation department schedules the chosen shutdown areas according to the main time schedule for the outage. RIS connects the around 2500 outage workorders to the selected shutdown areas. The workorders are marked with time for earliest start and latest finished.
The planning of workorders is controlled by help of GANT schemes per maintenance group or supervisor. Maintenance complements with detailed planning of the workorders. This will be an iteration process. If the resource demand is too high for some jobs, the schedule for the affected areas has to be adjusted. RIS makes the replanning, adjusts the workorders.

When planning has been finished, information is created for the work permits (the permits from the operation to carry out a workorder) and radiation permits. The system prints out forms for workorder, work permits, radiation permits and detailed instructions (including tags) for the shutdown areas (isolation work).

The work permit system makes it possible for operation department to supervise the outage. They can e.g. list jobs online (on the screen) which are current, not started or delayed for chosen maintenance group, foreman, functional system or shutdown area.

For added activities and after a change of the main outage schedule each maintenance group will automatically get a printout of the workorders, which after the change are planned to be done outside the new time limits.

3.4. Routines during operation

Planning and decision for maintenance during operation is done at the daily morning meeting at each unit. Meetings with representatives from operation, maintenance, chemistry and radiation departments.

Entered and remaining workorders are controlled in RIS. You may online get workorders listed on the screen in an arbitrary way. You yourself choose the selection, sorting and presented fields in the list. You can e.g. check the reported workorders for your unit during the last 24 hours.

Preparation of and data entry for workorders can be done directly by changing the actual data in the listings. This as an efficient way of minimizing the data entry work.

4. MATERIALS ADMINISTRATION

4.1. Summary

We hire a large number of contractors (up to 1000/unit during an outage). The store is mostly a security store. The material administration routines have been constructed according to these assumptions.

Data bases to this system are store articles, orders, invoices and financial transactions. The store data base contains articles in store, order points and history. The order data base collects all orders for further processing. Article, order and verification numbers are the keys to the information.

One main objective of the subsystem is to make it possible for the purchase department to concentrate on agreements and large orders.

- For store parts the system makes order proposals per supplier according to reservations, estimated consumption and order points. An increasingly large proportion of order volume can be rationalized due to order proposals realized within RIS.

- The purchase function is partly distributed. Specific users can be authorized to create orders based on the order requests entered in RIS. The authorization is given individually with a limited maximum order amount.
The system writes out all order letters. Delivery followup, delivery reporting, invoicing and outpayments are dealt with using previously obtained information.

![Diagram of RIS - Material administration]

**FIG. 3.**

### 4.2. Logical provision flow

The user initiates a purchase order by enter in RIS a request for a new order. To minimize data entry work, you may copy parts of former orders.

Request for parts from store are done within RIS. The store system includes search functions to find spare parts in an easy way. Your searching can be based on your own withdrawals during the last years or on spare part information.

For consumption parts the system creates order proposals based on order requests And order points in the store. The proposals are based on information from former suppliers, orders, agreements and calculated consumption prognosis.

For spare parts the persons in charge at maintenance and quality control departments get an online list of the parts they have to handle. Total information for rebuying is stored in RIS. They complement and adjust the information from last repurchase and approve the rebuying by entering their signature. The approval could be for an individual repurchase or for a specific time period. When both maintenance and quality control department have entered their approval, RIS generates an order-proposal.

The purchaser checks and approves the proposals. The order letters for approved orders will be printed out.

After the orders have been sent to the suppliers they will be supervised with help of the delivery follow-up module. The purchaser enters all notes as information for the users (customers).

The store staff checks the deliveries towards the order information and makes the data entry. RIS prints adhesive labels with information and address for distribution to customers or for storage purposes.
The data entry work is minimized. For delivery reporting the system presents not delivered quantities from that order. The store staff confirms or adjusts the divergences.

4.3. Invoice routines

Entered order and delivery information is the base for the invoice module.

RIS handles automatically invoices to small orders. The system controls the invoices and creates payment and accounting transactions based on order information. Significant discrepancies between deliveries and done payments will be listed monthly.

The invoice controllers take care of invoices to large orders. They specify order number and the time interval the invoice refers to. RIS summarizes the deliveries and creates a checked outline for the invoice. From a correct outline, information for payment and accounting is created. Otherwise the controller has all information within the system for further control.

5. FINANCE

5.1. Summary

All financial information and control at Ringhals is done directly by using a RIS-terminal. All forms and reports on paper have been abolished.

RIS automatically creates transactions for economic activities such as time reports for contractors and employees, deliveries, store movements and invoices. RIS transfers to and gets appropriate information from the Swedish State Power Board central accounting system.

The economic control within Ringhals is result oriented. Each group has to sell their activities to other departments. The prizing shall be based on each groups internal costs. An internal invoicing system creates automatically the economic transactions based on agreements between 'sellers' and 'buyers'.

Each group at lowest level enter their budget and internal agreements.

RIS gives you online functions for budget-, cost- and result follow-up, balance sheets and detailed cost analyses at all levels.

5.2. Budget

At Ringhals we have one official budget based on production cost and sale of electrical energy. This budget is complemented by internal budgets. The base for internal invoicing. Each group budget their buying and selling of services and their internal costs. The budget for internal costs gives the pricing (price/hour) for the group. Key values are price/hour and percentage sold hours.

Each group enters their budget in RIS. The system gives summing up and presentations at all levels.

5.3. Agreements

Agreements between departments at Ringhals are used as a specification for an internal invoicing function. Agreements for all projects are entered in RIS. For approved agreements (signed in RIS by buyer and seller) RIS creates monthly transactions for invoicing and payments.
For fixed agreements transactions will be created according to a decided payment plan. For running agreements RIS creates transactions based on the turnout.

5.4. Accounting

In order to be able to correlate the turnout to budget the accounting in Ringhals is based on booking of used resources.

Costs for contractors and materials are booked to order price when we use the resources (data entry of timereports and deliveries). Eventual differences are booked at payment of the invoices.

Accounting for The Swedish State Power Board (Vattenfall) is done with a central accounting system (EPOK), which is run on a computer at the head office in Stockholm. All transactions for the accounting are generated from RIS. Transactions from time reports for employees and contractors, delivery and withdrawal of material and invoices.

5.5. Economic analysis

At the end of each economic period (around the 20th of each month) information for economic analysis is updated in RIS. Transactions are generated from budget and agreements (internal invoicing). The turnout (costs) is fetched from the central accounting. The transactions are complemented with information from the basic subsystems in RIS.

The economic analysis is supported by functions at three different levels:

- The general view will be given by a set of result reports. The reports can be presented at all levels of the organization. The economy department designs the reports by using a report generator.
- All totals in the reports can be specified by using the economic analysis module.
- The detailed follow-up module gives information for groups and projects down to individual orders, material requests and time reports for employees and contractors.
All information and reports will be created and presented directly (online) with good response times.

6. PERSONNEL ADMINISTRATION

6.1. Summary

We need a safe method of handling and controlling our own staff, visitors and the around thousand contractors at site during the outage period. The base of this system is RIS.

RIS includes, except the normal personal information, functions for access supervision, radiation protection, administration of training and health care.

All personnel, contractor or visitor information is looked after by RIS. For each person you can e.g. get the following information:

<table>
<thead>
<tr>
<th>Personal data</th>
<th>Dosimeter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salary information</td>
<td>Radiation doses</td>
</tr>
<tr>
<td>Basic education</td>
<td>(totally) and per task</td>
</tr>
<tr>
<td>Training (history and planned)</td>
<td>Car pass</td>
</tr>
<tr>
<td>Access card</td>
<td>Clothes locker</td>
</tr>
<tr>
<td>Keys</td>
<td>Loan of material</td>
</tr>
</tbody>
</table>

![FIG. 5.](image)

6.2. Personnel information

The personnel routines are divided between RIS and routines at head office.

The salary systems are run on the central computer. The information is transferred monthly to RIS.

At each RIS-terminal the employee can see his personal and detailed salary information and each manager is authorized to see the aggregated information for his department or group.
6.3. Access routines

The access control system is used to administrate access permits and documents for all personnel (employees, contractors and visitors) who has access to the Ringhals plant.

Contractors and visitors should be announced by using the request of access module in RIS. For announced persons actual radiation information, date for latest radiation training course and medical examination are fetched from the national radiation file. The information is stored in RIS. The access department will have complete information to be able to prepare the access in advance.

Within the system are handled access cards, car access cards, dosimeters, keys for offices and clothes lockers.

Access information is automatically transferred to the PC-net, which controls the gates. If the person gets a dosimeter, information is also transferred to the specific computer for the dosimeter readers.

RIS stops the use of access cards and dosimeters when the permitted time has expired.

6.4. Radiation system

Through the radiation system in RIS we store and supervise individual and collective doses at Ringhals. Within the system is administrated the official radiation doses and the doses for individual jobs (work doses).

The official dosimeters (type TLD) are evaluated each month. The evaluation is done by local computers (PC:s). RIS stores the doses and transfers the information to the national radiation file.

The 'work dosimeters' (type ALNOR) uses special readers for in- and out-passing to controlled areas. The readers are connected to RIS through a minicomputer. At outpassing the
received doses is calculated and presented. The information is continuously transferred to RIS. When a person gets too high dose, RIS gives alarm and stops automatically the access card.

RIS creates statistic information based on the radiation permits.

7. EXECUTIVE INFORMATION SYSTEM

7.1. Summary

RIS executive information system is an easy-to-use presentation function for high quality graphs.

The function is automatically included in RIS when you have one of the personal computers which we use as terminals for the RIS-system.

The system includes management information at Ringhals and department level. At Ringhals level, information is included for control of production, economy, environment, security and personal. The graphs are updated automatically or manually. Manually when the information has to be controlled and commented upon.

8. NUCLEAR POWER SPECIFICS AND OTHER SYSTEMS

8.1. Summary

Several systems have been collected in this section of RIS. Some of the most important are handling of waste, fuel administration and different kinds of documentation.

8.2. Waste

Data base for all waste produced at Ringhals. Nuclide content and radiation calculated for each dispatch. Functions for specification of transport to the national sealed waste store outside Forsmark.

8.3. Fuel administration

The fuel administration system consists of two main functions:
- Fuel usage and movement accounts (according to IAEA standards),
- Generation and check of operation orders for the annual refuelling. The fuel is moved from the reactor to a fuel basin. Part of the fuel is replaced, after which it is moved back to the reactor according to a redesigned pattern.

8.4. Documentation

In RIS all official documentation is included. RIS has routines for:
- Technical documentation (drawings, handbooks ...)
- Administrative documents (reports, internal and external letters)
- Library functions for books and journals (circulation and subscription)
- Nuclear regulations and standards.
- Documentation and administration of the communication net for computers and tele.
- Documentation of RIS routines and programs.

The documentation routines are combined with text search functions.
COMPUTER EMPLOYMENT IN PROTECTIVE ACTION CONTROL SYSTEMS FOR VPBER-600 NUCLEAR POWER PLANT

A.B. POBEDONOSTSEV
Experimental Machine Buildings,
Design Bureau,
Nizhny Novgorod, Russian Federation

Abstract

This paper deals with prerequisites for the technological and economic justification of the use of computers in protective action control systems (PACS). The main approaches to the use of computers in PACS are described as an example of system design a VPBER-600 nuclear power plant. The purpose of PACS in the general structure of reactor plant PCS, is described. The PACS structural diagram is given. The functions performed by each PACS module are described in detail.

Modern digital technique extends considerably monitoring and control functions that creates the prerequisites for wide employment of computers in nuclear power plant (NPP) systems.

Now, the employment of computers in protective action control systems (PACS) is limited in Russia. Mainly, it is due to deficient reliability of general industrial computer hardware.

At the same time, because of development of advanced nuclear plants for NPPs with enhanced reliability and safety, some new prerequisites for computer employments in PACS has appeared, able to justify their technological and economic expedience[1]. Such prerequisites are:

- inherent safety of reactor plants that is the ability to self-regulation and self-limitation of reactor power in terms of natural feedbacks over the whole range of reactor parameter changes;

- the equipment of new reactor plants with built-in self-actuated passive devices, able to provide irreversible actuation of safety systems by the elementary algorithms immediately from regime parameters omitting control channels with electronic components.

But the built-in self-actuated passive devices do not show the adaptability and accuracy, the electric controlling systems can provide.

Therefore the self-actuated devices are employed when the controlling systems with electronic components fail to operate.

Besides the PACS should be feasible to control safety system mechanisms not only at accident but also during nominal operation especially when preparing to NPP commissioning.

From the other hand there is national standard requirement for automatic controlling and diagnosing of PACS hardware and software serviceability [2,3].

These prerequisites may be realized through extended precision, algorithm variety and higher intelligence of PACS.

It is suggested to consider the main approaches to the employment of computers in PACSs by way of example of such system design for VPBER-600 nuclear power unit with inherent safely and passive self-actuated devices.
The possibility of computer employment in PACSs is caused both by reactor inherent safety, passive self-actuated devices and by PACS reliability realized using electronic components. The latter is reached due to usage of highly reliable special computers and structural hardware decisions.

Power unit process control system is a decentralized system consisting of several computer complexes, each being able to realize independently the problems of controlling the corresponding part of power generation process cycle.

The central computer complex of power unit is intended to coordinate the functioning of compute complexes in different operating regimes. Information computer system (ICS) connects operator workstations in control rooms and PCS controlling computer complexes.

ICS is a dual local network with connected workstations and peripherals. PCS structural diagram is given in Fig. 1.

PACS is a constituent part of PCS firmware complex.

PACS is intended to operate safety system actuating mechanisms when accidents occur and to control their operation. PACS actuates system mechanisms providing reactor emergency shut-down, emergency heat removal, radioactive media confining in the design boundaries, controls system equipment ensuring safely system functioning. It provides also monitoring and control of above mentioned mechanisms, when preparing the technological systems to operation (filling with working medium, etc.) before reactor start-up.

PACS is made by hardware as two independent sets, each capable to provide all safety functions required. Structural diagram of one PACS set is given in Fig. 2.
Set hardware and cable communications over the plant site are arranged so that internal or external event (fire, air crash, etc.) can not fail simultaneously more than one PACS set.

Each set consists of controlling computer complex, primary information conversion and command issue equipments associated with this complex, emergency control panels in main and stand-by control rooms and cable system.

In each set the controlling computer complex is four-channel and the other hardware is three-channel. Each channel hardware is made as individual devices having separate secondary power sources.

Cable communications between the devices are separated into channel paths. Different PACS sets are diverse. The diversity is attained due to:

- different controlling computer complexes sets' development by different designers;
- different read-only-memory use;
- fabrication by different vendors;
- Primary information conversion equipment (PICE) implements;
- analogous and discrete transducers inquiry;
- information conversion into digital code;
- inner diagnostics and self-checking;
- information transfer to the controlling computer complex;
- information transfer path diagnostics.

The PICE is made as three-channel one. The channels function independently. When one channel fails PICE operation is not disturbed as a whole. The PICE is connected with controlling
computer complex by controllers. When transferring the information the conductive decoupling is provided. Every PICE channel transfers the information to every controlling computer complex channel.

The command issue equipment is intended to transfer commands from controlling computer complex and remote control commands issued by an operator (omitting the controlling computer complex) to safety system actuating elements (SSAE), such as valves, pumps, etc. The command issue equipment (CIE) is made as a three-channel one.

The CIE ensures:
- reception of automated and functional-group control commands from controlling computer complex and remote control commands from operator panel;
- command conversions into positional code;
- power gain
- control command issue to actuating elements (majoritation of CIE channel outputs is provided in cable network),
- command passing validity check
- hardware and communication link diagnostics. The CIE consists by hardware of one-channel conventional structural unit sets.

Command issue for reactor trip is realized otherwise.

To control the reactor during normal and emergency regimes the PCS is provided for reactor control and protection system (CPS). To realize reactor emergency protection function according to neutron-physic parameters the system is made as a two-set one with thrice-repeated inner redundancy of each set.

To execute the reactor emergency protection function it is necessary to de-energize CPS drive motors. Thereby the compensating members drop under gravity and shut down the reactor. To implement emergency protection function there is an emergency protection unit (EPU) in each CPS set.

Neutron-physics and heat-engineering parameter signals (from the controlling computer complex of associated PACS set) and operator commands from main control room and stand-by control room enter the EPU through three channels.

The entering of any command through not less than two channels causes CPS drive power circuits break in two points and realizes emergency protection function. EPUs are made with logics realized by hardware. To ensure two break points in one circuit diverse breakers are used (see Fig.2).

PACS controlling computer complex where logic processing of information is implemented is the main part of the system. The controlling computer complex is fourfold redundant, where each channel is a specialized controlling computer.

The controlling computer complex provides:
- obtained information processing by program methods to determine its validity;
- logic information processing to reveal the emergency;
- command set forming according to protection algorithm required in specific emergency;
realization of prohibitions, priorities, change of setpoints according to controlled object state and operation mode;

- inner self-diagnostics of hardware and software;

- reconfiguration of the system and change of output signal processing logic (two of four) when faults occur;

- required information transfer to other PCS subsystems and to the displays of emergency panels of main control and stand-by control rooms.

The controlling computer complex ensures the possibility of functional test checks.

The programs of protective action realization (algorithms) are invariable what is achieved by firmware methods and are stored in non-volatile memory in ROM of controlling computer complex.

The controlling computer complex is diagnosed mainly by software, possible faults at diagnosing are not influencing the capability of controlling computer complex to execute the required functions for safety system actuation.

PACS controlling computer complex is connected to other PCS subsystems through fiber-optics communication lines.

Emergency control panels with control members and information displaying means are provided in main control and stand-by control rooms to display safety information and to control remotely safety system mechanisms.

Both in main control and stand-by control rooms it is possible to control and to obtain information from both PACS sets.

At emergency control panel there are safety display, central signalling system, individual digital indicators, function keyboard and individual remote control key for especially important safety system mechanisms.

Besides, safety information can be represented on normal operation displays, because all required information on safety systems is transferred from PACS controlling computer complexes to PCS through power unit controlling computer complex.

The adopted decisions for PACS construction, in addition to natural reactor characteristics (power self-limitation) and self-actuated devices should provide the efficient and safe operation

CONCLUSIONS

1. Computer applications in inherent safety reactor plant PACS is considered to be expedient and justified.

2. The use of computers for diagnostic and auxiliary functions, for organization of information representation control is justified, because it facilitates operation, reduces the probability of personnel errors, and improves system operation reliability as a whole.

3. Protective action invariable algorithms with firmware employment and independence of safety functions from possible failures, when diagnosing system firmware, improve PACS operation reliability.
1. INTRODUCTION

The latest Advanced Gas Reactors (AGR) have been constructed at Heysham II in the Northwest of England and at Torness in the Southeast part of Scotland. The overall design is very similar to the successful Hinkley and Hunterston AGR stations, with one exception being the control and instrumentation system and its associated cabling. This change reflected the impact of computer and micro-processor technology on plant protection, control and operator displays.

For the South of Scotland Electricity Board (SSEB), now Scottish Nuclear, a major change in philosophy was the use of direct digital control for the complex task of total plant control. NNC Limited, who were the main nuclear island design and construction agency, had experience with the application of DDC on power stations. However, the detailed design proposals were more ambitious at that time than on any power station or plant process in the world. This approach had, therefore, some risks for Scottish Nuclear due to its limited experience of computer control at that time.

Torness NPS is a twin unit AGR station. Each reactor is rated at 660 MWe. Unit 1 has been supplying electricity to the national grid since Max 1988 and Unit 2 since February 1989.

This paper discusses the successful Torness computer system, with particular emphasis on the Direct Digital Control (DDC) which was successfully applied. The contents is derived directly from References 1, 2, and 3.

2. HARDWARE AND SOFTWARE SYSTEM SUPPLY

The supply of the Torness Control and Data Acquisition Systems was open to competitive tendering and this resulted in Ferranti Plc being awarded the contract for the supply of the complete unit control system, data acquisition and operating system software but excluding any applications software.

NNC Limited were awarded the contract to write the applications software based on their expertise in writing the applications software for the Hartlepool and Heysham 1 AGR computer systems for display and direct digital control.

The Ferranti Argus hardware system had previously been used on nuclear plant and the processor arrangement offered a number of upgrade options which could be taken up if the initial estimates of processor loading proved to be incorrect.

CORAL was chosen as the computer language because it is block structured, with a long history of successful use for high integrity application in the UK. The Ferranti ARGUS range of computers also has well proven CORAL development extensions to the standard operations system.
In nuclear power station construction, the supply of equipment, the installation and the supporting documentation must follow very rigorous and well defined Quality Assurance (QA) path. The SSEB had identified the dangers of incorrect interpretation by programmers of the real requirements, the difficulties of testing large software systems and the difficulties of monitoring the progress of software production.

The SSEB’s strategy therefore consisted of:

1. Close control of the system design and software development with minimal disturbance to contractors.
2. Close control QA arrangements.
3. The intention to use the simulator for independent monitoring of software production.
4. Fast resolution of important problems and issues.

The software provided by NNC included that for alarm processing, logs and records, operator interface support, standard and special calculations, and reactor management. All plant signals to be processed were identified and scheduled by NNC. The NNC strategy for testing relied on a progressive buildup test coverage, using a joint commissioning team on site led by NNC. Testing included:

a) Comprehensive off-line tests by the contractors.

b) Signal input injection and output monitoring on each target configuration.

c) Staged commissioning tests which integrated the plant with the computer systems.

The difficulties in achieving software production targets were identified early in the project and a number of packages were subcontracted by NNC to Digital Applications International Ltd. (DAI Ltd.). The form of the detailed design and test documents produced by NNC made it relatively straightforward to split the software production and tests between DAI and NNC.

DAI were also engaged to assist NNC in the software systems building and testing. Although the control system is distributed, communication can only occur if all the software in each node is correctly linked together in a Super system build. With no software changes allowed on site, a complete build was required for each software change identified by the site team. Executed manually, this build process was error prone and could take a number of weeks. Total automation of the offline test and build processes enabled modified software to undergo a precise repeat of its original test and build route, with a guaranteed delivery date of the verified software to the site team: A rebuild turnaround of less than one week was achieved using the off-line service systems. With over 20 rebuilds necessary before "raise power," these techniques were of crucial importance both in time scale and QA terms.

3. INSTRUMENTATION AND CONTROL SYSTEM OVERVIEW

At Torness Power Station, the amount of normal instrumentation within the Central Control Room (CCR) is limited to that which is necessary to allow continuous operation at steady load for a short period in the event of a catastrophic failure of the Data Processor (DP). The operator interface must therefore be comprehensive, accurate and flexible. This is achieved by a custom designed set of VDU formats complemented by a small number of operator configurable formats.
The Torness on-line computer system provides the primary method of instrumentation presentation and data processing for the operators and provides full DDC of all control functions needed for operation at powers between 30% and 105% of full design output.

The computer system consists of a network of computer nodes, based on the Ferranti Argus 700 range of computers, assigned to each reactor unit, except where common station facilities are required. For each reactor unit, the computer system provides both data processing and automatic control functions. For essential data capture, control and display to the CCR operators, the processor hardware is duplicated. These are termed Level 1 systems and are shown in Figures 1 and 2. Single processor systems which collect data not considered essential for continued unit operation are termed Level 2 systems. Figure 3 illustrates the Level 2 computer system for both units.

Torness NPS probably has the most complex computer configuration of any operating nuclear power station. The auto control "supersystem" consists of, per reactor, ten input multiplexing computers ("muxes"), eleven control computers (CCO1, CCO2 to CCI1) and a dual online/standby supervisory computer ("CS"). Each of these computers is a node in the hierarchical control supersystem shown schematically in Figure 2.

---

![Diagram of Level 1 Data Systems](image)

Figure 1. Level 1 Data Systems
4. OPERATOR INTERFACE DESCRIPTION

The MNI (Man-Machine Interface) in the CCR at Torness consists of an extensive set of VDUs for format displays, joysticks, keyboards and a graphics printer. The distributed database contains approximately 40,000 data points and is maintained throughout the network by autonomous transcription via proprietary communications software.

In the event of total failure of System DBT, connection of CCR display controllers directly to Systems A, D, CS allows plant monitoring to continue. A simplified subset of formats is used for this purpose.
Figure 3. Level 2 Data Collection Systems
4.1 VDU Formats

Approximately 320 complex VDU formats are grouped functionally as follows:

- **Plant mimic formats** grouped into 26 plant systems. Access to, between and within each plant system is predefined and implemented by "soft keys" on each format.

- **Engineering formats** again grouped into plant systems. These simple tabular formats were automatically generated off line from the current database and were used extensively during the early stages of plant commissioning.

- **Help formats** to assist the operator in using the operator interface. Maximum use of references to operation and maintenance manuals is made.

- **Operator variable formats.** Three types are available: a range of trend formats where the operator can enter up to 7 database parameters per trend; a range of tabular displays where the operator can similarly select database entries and the current values only are displayed; operator variable logs where the operator can specify content, duration and sample frequency for up to 8 logs with 32 parameters per log.

- **Alarm support formats.** Two types of alarm formats inform the operator of the plant condition: All alarm lists and plant system alarm lists where the operator processes alarms; Unit and plant system alarm mimics where quantitative information is presented, but alarm processing is not permitted.

- **Logging and recording support formats.** These formats are used to gain access to logging activity information, freeze trends for subsequent analysis, recall historical data for on-line display, and send results to the graphics printer for subsequent analysis.

4.2. Hardware Interface

The operator communicates with the computer system via System DBT using joysticks and custom designed keyboards. Function keys are allocated to specific activities, e.g. "accept alarms," and are complemented by the standard "QWERTY" key pad layout.

In addition, the operator is also able to insert trims into control loops using a combination of the Computer Input Panel (CIP), and a predefined set of VDU formats. The software supporting the CIP ensures that the appropriate format is on display before a new trim is inserted into the control algorithm.

5. THE AUTO CONTROL SUPERSYSTEM

The muxes and CCs do not have any disc storage capacity - all software and operational data is held in volatile random access memory (RAM). The mux and CC software is therefore downloaded from CS (via a CC in the case of a mux). There is battery backup on the muxes and CCs in the event of a power failure.

CCO2 to CC11 and CS are multiprocessor machines, containing more than one processor. Several programs run concurrently by time slicing on one processor. Programs can also run on separate processors in parallel.
There are analog and digital inputs to the control supersystem but all outputs are digital, or driven for a precise time by the control software. Most control room pushbuttons and thumbwheels are connected to the muxes, but a few are connected directly to CS for the amendment of control trims in the CCS.

The muxes and CCO1, which do not have a mux, together have approximately 1600 analog inputs and 1100 digital inputs. The CCs together have approximately 640 digital outputs. There are no terminal or printer operator interfaces to a mux or CC, which are simply connected directly to a higher machine in the hierarchy via a serial communications link (HDLC). CS has hard copy consoles, alphanumeric VDUs, color graphics VDUs and a thumbwheel input panel to allow auto control trims to be adjusted in the CCs, the values being transmitted to the CCs along the serial links. In addition to the inputs panel, system software enables operators to inspect variables or modify control constants in the CCs from CS. CS is also used to process and report alarms and event messages generated throughout the control supersystem.

The auto control applications software is divided into several programs, each using separately coded and tested standard modules and libraries.

6. MODULATING CONTROL SYSTEM

The overall automatic control combines operation of control systems for five distinct plant areas:

1. The regulation of the reactor heat rate using uniformly distributed regulating rods.
2. The regulation of the mass flow rate of the coolant gas.
3. The regulation of total feedwater flow.
4. The regulation of feedwater flow to individual boiler (or half units) to correct asymmetric temperature profiles created by onload refuelling.
5. The regulation of the setpoint of the turbine speed governor.

The reactor heat rate (Item 1 above) is a separate, clearly defined system: the reactor is divided into zones, the reactivity of each zone being regulated by a single control rod. The measured variable for the control of a zone is derived from the coolant gas temperatures at the outlets of the fuel channels.

The effects of the control systems are highly interactive because all affect the transfer of heat from coolant gas to water/steam in the boilers. Because of this interaction, there are two options for regulating the transfer of heat from the fuel to the water/steam. Either,

(a) the gas mass flow is "forced" and the feedwater flow is under closed loop control to maintain the desired boiler heat transfer, or
(b) the feedwater flow is "forced" and the gas mass flow is under closed loop control.

Because of the once-through boilers, the pressure of the steam leaving the boilers is very sensitive both to the response of the turbine speed governor to frequency fluctuations and to changes in feed pressure. It is necessary, therefore, to maintain the steam pressure within close limits. Again, two options for automatic control:
(i) The steam pressure can be controlled by regulating the setpoint of the speed governor. A consequence of adopting this option is that load variations initiated by the speed governor are removed by the steam pressure control action. With this configuration, the load generated is regulated by "forcing" the heat rate of the steam supply, employing option (a) or option (b) above.

(ii) The steam pressure can be controlled by regulating the feedwater pressure. Unit load is then regulated via the setpoint of the speed governor.

The sensitivity of the steam pressure to speed governor action imposes a stringent response requirement on its automatic control and loss of automatic control, leaving a unit vulnerable to a trip. Thus, AGRs which have electronic turbine speed governors reduce the control gain of the governor when operating at normal power.

Both options (i) and (ii) have been employed on the various AGRS. From a station operation viewpoint (i) is more attractive because it has the capability of "shielding" the plant from external disturbances.

At Torness the control structure makes the reactor take the lead for any load manoeuvre (option (i) above). Reactivity control via individual control of each of the 44 regulating control rods gives improved automatic control of axial temperature and power profiles across the reactor. A computer system also allows the project risks to be minimized since changes can be implemented quickly with minimum impact on the station commissioning program.

SSEB's policy of minimizing site changes meant that all control constants, gains and controller settings had to be calculated in detail and issued formally before being used at the site. This exercise made use of the extensive reactor and plant modeling facilities which had been developed to substantiate the original system design.

7. OPERATING EXPERIENCE

7.1 DDC Systems

The design effort of identifying in full all control constant values was well rewarded during the raise power phase when only some ten items out of a possible 1000 control variables had to be changed and no delay to the startup program was incurred by unsatisfactory control performance. The first attempts at raising power to 30%, 60% and 100% were on full automatic control. The initial power raise to 100% at Torness was the first power raise of a UK nuclear station under full automatic control. Other "firsts" included successfully controlling the plant following the loss of two out of the total of eight boilers from full load, successfully controlling a major loss-of-feed transient and successfully controlling a rod drop fault. These are major transients which generally cause loss of generation on AGRS.

7.2 Display Formats

Since format design proceeded in parallel with plant and cabling design, commissioning and setting to work, operational usage of some formats was delayed. Consequently, several adjustments to the design became necessary, causing difficulties with initial operator acceptance. However, the majority of recommended changes to the design of selected formats were of a minor nature. The recommendations arose from both operational experience and station commissioning tests.

VDU formats were delivered to the station in batches to meet plant commissioning requirements. During the early commissioning period, the engineering formats were mainly used and required very little training. The engineering formats are now used as "bench marks" to compare doubtful signals on the mimic formats.
Although CCR Operators were not initially given formal training in the use of the computer system facilities, several "ad-hoc" teach-in sessions, both on the unit desk and on the simulator training facility, proved effective. A User Guide for each format at the unit desk ensures continued awareness of the initial functional objectives and correct usage. Formal training is now the responsibility of the station training department.

Several formats now support "Identified Operator Instructions" required for safety and data calculated by the reactor management applications software is displayed as RMS trip/alarm monitoring information.

As a result of the large number of formats and the duplication of signal displays, each operator and shift uses a variety of formats for the same plant monitoring requirement. With the exception of fault investigation, only a small proportion of formats, approximately 30% of the total available formats, were used. The widest spread of format usage occurs during unit startup. The most popular formats are in the control system family, indicating the importance of the control system to most station operations from the control room.

A formal fault-reporting scheme is in operation, involving the station, HQ and original software suppliers. Computerized registries of fault reports are maintained. The figures show that the number of "genuine" faults (160) is small in comparison to the total number of formats (234) combined with the total number of signals displayed (24714), indicating a measure of success for the QA in general and the test methods in particular. The most common type of format fault reported is incorrect plant status representation, e.g. a valve displayed open when in fact it was dosed. This type of fault is difficult to detect prior to plant availability and operation.

7.3. Computer System Performance

The system performance is gauged by observing the following properties:

- Time taken to update a display (2 secs from DBT database)
- Time taken to process alarms
- Time taken to print a log
- Time taken to can a format to the screen

Interest in system performance by the UK licensing authority (NII) led to a series of investigations and upgrades. Prior to initial power raise to 23% (th) on Rl, the processor configuration of a "GZ" (4 MIPS) and 2 GLs (1 MIPS each) was increased by an additional GL processor, giving an achieved 10% increase in overall processor power. During the initial R1 power raise, the availability of the data processor part of the system was 99%, and the auto control part (excluding CCO8, which had a persistent fault now cured) was 99.8%.

8. CONCLUSIONS

The computer system in general and the display system in particular have proven to be essential items in the construction, commissioning and operational phases of Torness Power Station. The facilities to meet major station milestones were available. Commissioning facilities, e.g. operator variable logs and trends, removed the need for extensive use of chart recorders in the Control Room.

Although the display system was selected to reduce the amount of information shown to the operator in a "nondestructive" manner, relatively little use has been made of the zoom, pan and declutter facilities.
With the exception of fault investigation, only a relatively small proportion of the VDU formats are used. Furthermore, a steady-state plant monitoring, which is the normal operating mode, an even smaller proportion, approximately 3% of the total is required.

In future applications, the CCR operator interface requirements should be established as early as possible to allow the computer system design to be frozen early.

The contractors (Ferranti, NNC, Digital Applications International Ltd.) and the SSEB collaborated throughout the contracts and station construction period to produce a highly successful and reliable hardware and software system on which the total station operation depends.

Once commissioned, the Torness auto control system has exceeded all expectations since, historically, automatic control has been commissioned in a piecemeal fashion and has required much modification, refinement and optimization. The Torness computer system has performed well since its initial use and is a credit to all contractors associated with it.

REFERENCES


ENHANCED FUNCTIONS OF PROCESS COMPUTER SYSTEMS FOR NUCLEAR POWER PLANTS

B. SINGER
Science Applications International Corporation,
Marietta, Georgia, United States of America

S. BHATT, B. K.-H. SUN
Nuclear Power Division,
Electric Power Research Institute,
Palo Alto, California, United States of America

Abstract

The plant process computer system is a system of computer hardware and software that is integrated to acquire large amounts of plant data on a real-time basis. The purpose is to perform calculations which will provide plant operators with critical operating parameters in normal and emergency situations. There have been numerous efforts in nuclear power plants around the world to upgrade or replace plant process computers with enhanced functions. This paper describes the system operation and performance of process computers, their functionalities and communications, and their enhanced functions in software and hardware. A prudent approach to upgrade process computers with enhanced functions can help utilities address obsolescence problems, support improved fuel design, reduce operation and maintenance cost, and increase plant and people productivity. In addition, it provides a framework for plant-wide monitoring to support future instrumentation and control upgrades.

1. INTRODUCTION

The plant process computer system (PPCS) provides the plant operators with critical operating parameters in normal and emergency situations. This is a system of computer hardware and software that are integrated together to acquire large amounts of plant data on a real time basis for the purpose of performing calculations and other functions like scan, log, and alarm, data archival and retrieval on a Central Processing Unit (CPU), and displaying data processing results through the system’s Man Machine Interface (MMI). The real time data is gathered from field sensors located throughout the plant. Figure 1 depicts an overview of the PPCS basic functions and Figure 2 shows a typical configuration of a PPCS.

Figure 1. Plant process computer system functional overview.
Figure 2. A plant process computer system configuration.
In recent years, there have been efforts in nuclear power plants around the world to upgrade or replace plant process computers. The replacement or upgrade of the PPCS is a complex procurement activity for the utility which involves several functional groups within the utility (e.g., Purchasing, Engineering, Operations, Training, Computer Maintenance, Instrumentation & Control, etc.), and several suppliers to the utility (e.g., computer hardware, applications software, and engineering support services, etc.).

Because the PPCS is a significant element in the nuclear plant's technology, its upgrade is justified through its contribution to the plant's overall performance and operational point of view. Consideration of performance issues focuses upon the reduction in the number and length of unscheduled outages, and the increase in time between outages due to the acquisition of better and more reliable data about the plant's operations. Modern PPCS has the capacity to integrate the information processed by various existing plant computer systems. The following are needs which motivate utilities worldwide to upgrade or replace their old PPCS:

- Aging of computer system with resulting increases in maintenance costs
- Limitations for utilizing current software or adding new software applications
- New data sensors added to the plant that cannot be monitored by the existing PPCS
- Access to actual plant data necessary to analyze unusual events and trips such that plant engineers can determine, timely, the effects of these events.
- Plant data archival and retrieval to support performance analysis (i.e., fuel performance with actual plant operation data), and trouble shooting during plant startup.
- Data acquisition, storage and trending functionality to benefit the efforts of maintenance, performance, and technical support engineering groups.
- Real time plant data for emergency exercises
- A system that enhances operator actions and responses to upsets when working under Emergency Operating Procedures (EOP).

2. SYSTEM OPERATION AND PERFORMANCE

System operation and performance requirements for PPCS should be specified functionally in terms of reliability and response times.

Reliability is expressed as the minimum acceptable percentage of time that the system is operational, and typically ranges from 99.0 to 99.9 percent. The ability of the system to meet this requirement will be primarily constrained by the mean time between failure of and mean time to repair the system hardware configuration. The required level of availability will dictate the hardware configuration in terms of whether a single highly reliable system or two less reliable redundant systems are required; and will have a major impact upon system cost. At the current state-of-the-art, a redundant configuration is required for availability at or above 99.8 percent.

Response times are expressed in terms of the system's ability to sample the plant instrumentation and generate displays on the graphic terminals. Typical sample requirements for field inputs are once per one millisecond for sequence of events field inputs and once per 10 milliseconds for analog and contact field inputs. Response times for displays can be specified in terms of the amount of time it takes from when the operator requests a display until the time that the display
begins, or until all information is displayed, or both. The utility must also decide if this minimum
time is to be location-dependent, for example, displays requested from terminals located in the control
room versus the emergency operating facility. The utility must also decide if, in addition to this
requirement, a minimum time should be specified between updating the data on the graphic display
terminals. Values for bringing up displays range from 0.5 to 5.0 seconds, depending on the location
and type of display; for example, historical and current value displays. Values for updating rates vary
from one to five seconds. Some additional response time requirements worth considering are
specifying the time between request and output of spooled files to the printer devices, and the time
required to bring the computer system back on line due to non-hardware failures.

Seismic and environmental operational requirements also need to be considered. The portion
of the computer system to be located in the control room, e.g., display terminals and printer devices,
must be designed to withstand the vertical and horizontal forces at the design basis safe shutdown
earthquake. In addition, the range of expected temperature and humidity conditions over which the
computer system is required to operate uninterruptedly needs to be specified.

3. SOFTWARE FUNCTIONALITY

The functionality of the software is specified at both the operating system level and
applications level. The operating system software requirements define the environment necessary to
support the applications software and handle the peripheral hardware devices. The applications
software functionality defines how data from the plant instrumentation is collected, processed and
displayed to the user.

The system software is usually the latest version of the operating system provided with the
central processing unit(s) as obtained from the hardware vendor. It has operating and diagnostic
capabilities that support a multi-user, multi-tasking environment and communication, with input and
output devices such as disk drives, tape drives, and printers, as well as other plant computer systems.

The applications software can be categorized broadly into the scan, log, and alarm, plant
monitoring and performance, and man-machine interface (MMI) functions. The scan, log and alarm
function serves to sample the plant instrumentation inputs and log each current value into the
database. This process includes converting the incoming signal to an appropriate engineering unit
and then checking this value against various alarm limits to determine if the signal is valid and if it
warrants further attention. In addition, data is selectively archived for subsequent retrieval to support
engineering analysis of historical events. The plant monitoring and performance functions then
process the database information to support operational monitoring and performance requirements.
The MMI provides the interface to the system for controlling these functions as well as to access
information from them. The relationship of these functions is illustrated in Figure 3.

Some base-line scan, log, alarm and MMI functions are common to both boiling water reactor
(BWR) and pressurized water reactor (PWR) computer systems. The requirements for the plant
monitoring and performance functions, however, differ considerably between BWRs and PWRs due
to the different way in which power is controlled. Power changes in a PWR are typically performed
in a core-wide manner by moving groups of control rods, whereas power changes in a BWR are
performed more locally within the core by moving individual control rods. This requires that the
BWR process computer system contain nodal reactor core fuel monitoring functions and the ability
to collect local core data to support off-line detailed calculations. Consequently, PWR process
computer systems generally include more functions to support overall system monitoring and
performance calculations and BWR process computer systems generally include more functions to
support reactor core monitoring.

The general software functions for BWR and PWR applications are listed in Table 1.
Flows → Pressures → Levels → Temperatures → Component Status → SCAN

Database Log → Human Machine Interface

Data Archive

ALARM DISPLAY

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>VALUE</th>
<th>UNITS</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>RCS TEMP</td>
<td>XXX</td>
<td>DEGF</td>
<td>GOOD</td>
</tr>
<tr>
<td>RCS PRESS</td>
<td>YYYY</td>
<td>PSIA</td>
<td>HIGH</td>
</tr>
<tr>
<td>PZR LEVEL</td>
<td>ZZZ</td>
<td>INCH</td>
<td>LOW</td>
</tr>
</tbody>
</table>

Plant Monitoring & Performance

React Power Level

Time

Figure 3. Plant Process Computer System Software Functional Relationship.
<table>
<thead>
<tr>
<th>SOFTWARE FUNCTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General to BWRs and PWRs</strong></td>
</tr>
<tr>
<td>Point Processing</td>
</tr>
<tr>
<td>Database Management Alarm Monitoring</td>
</tr>
<tr>
<td>Logs and Reports</td>
</tr>
<tr>
<td>Sequence-of-Events Monitoring</td>
</tr>
<tr>
<td>Pre-Trip and Post-Trip Review</td>
</tr>
<tr>
<td>Data Archival and Retrieval</td>
</tr>
<tr>
<td>Man-Machine Interface (MMI)</td>
</tr>
<tr>
<td><strong>BWR Specific</strong></td>
</tr>
<tr>
<td>Periodic Core Evaluation</td>
</tr>
<tr>
<td>Periodic Core Performance Summary</td>
</tr>
<tr>
<td>Periodic Core Energy Increment</td>
</tr>
<tr>
<td>Drifting Local Power Range Monitor (LPRM) Diagnostics</td>
</tr>
<tr>
<td><strong>BWR Specific</strong></td>
</tr>
<tr>
<td>LPRM Calibration and Base Distributions</td>
</tr>
<tr>
<td>Core Thermal Power and Average Power Range Monitor (APRM)</td>
</tr>
<tr>
<td>Thermal Data for Specified Fuel Bundle</td>
</tr>
<tr>
<td>Present Control Rod Positions</td>
</tr>
<tr>
<td>Present LPRM Readings</td>
</tr>
<tr>
<td>Axial Interpolation Data</td>
</tr>
<tr>
<td>Preconditioning Interim Operating Management Recommendations</td>
</tr>
<tr>
<td>Isotopic Composition of In-Core Fuel</td>
</tr>
<tr>
<td>LPRM Sensitivity</td>
</tr>
<tr>
<td>Substitute and Unknown Control Rod Positions</td>
</tr>
<tr>
<td>Computer Outage Recovery Monitor</td>
</tr>
<tr>
<td>Target Exposure and Power Data</td>
</tr>
<tr>
<td>Reprint Periodic Core Performance Logs</td>
</tr>
<tr>
<td>LPRM Alarm Trip Recalculation</td>
</tr>
<tr>
<td>Refueling Update Monitor</td>
</tr>
<tr>
<td>Balance of Plant Performance Monitoring</td>
</tr>
<tr>
<td>Rod Position Indication System</td>
</tr>
<tr>
<td>Rod Worth Minimizer</td>
</tr>
<tr>
<td>Traversing Incore Probe</td>
</tr>
<tr>
<td><strong>PWR Specific</strong></td>
</tr>
<tr>
<td>Axial Flux Difference</td>
</tr>
<tr>
<td>Control Rod Monitor</td>
</tr>
<tr>
<td>Flux Mapping</td>
</tr>
<tr>
<td>Reactor Coolant System Heatup and Cooldown Monitor</td>
</tr>
<tr>
<td>Incore Thermocouple Monitor</td>
</tr>
<tr>
<td>Setpoint Supervision</td>
</tr>
<tr>
<td>Primary Plant Performance Monitor</td>
</tr>
<tr>
<td>Balance of Plant Performance Monitor</td>
</tr>
</tbody>
</table>
4. HARDWARE FUNCTIONALITY

The hardware functionality describes the minimum hardware requirements necessary to support the applications software and system performance requirements. The basic system is typically comprised of the following general hardware and configured as illustrated in Figure 4:

- Data Acquisition Unit(s)
- Central Processing Unit(s)

![Diagram of General Plant Process Computer System Hardware Functionality](image-url)

Figure 4. General plant process computer system hardware functionality
Unless a specific hardware solution and/or configuration is desired, the hardware functional requirements should be general to allow the system integrator the freedom to select a configuration utilizing a standard design that meets the system operation and performance requirements. For example, the system availability requirements could be met with a single highly reliable hardware configuration which can typically satisfy a 99.0 to 99.5% availability requirement by having a large mean time between failures. Alternatively, the availability requirements can also be met with a redundant hardware configuration which can typically satisfy up to 99.9% availability requirement. It is important to weigh the cost and benefit of each solution when the final configuration is selected. For example, while a single hardware system costs less, it is subject to single failures that could render it unavailable to the plant. On the other hand, a redundant hardware system, where one portion is in standby and ready to take over should the other portion fail to meet present operating and performance criteria, provides a system with a higher overall availability as well as a secondary system for developing and, to some extent, testing of new or modified applications software.

An example redundant configuration for the general system hardware is illustrated in Figure 5. This particular configuration employs redundant data acquisition units which feed two redundant central processor units (CPUs). Each CPU has its own system disk and tape drive unit for

![Redundant Data Acquisition Unit](image)

**Figure 5. Redundant hardware functionality.**
off-loading data, but shares redundant data disks. The CPUs also serve a common set of graphic display terminals.

5. COMMUNICATION LINKS

The minimum number and type of communication ports to support the peripherals and other computer systems are specified in terms of interface type and baud rate. Typical baud rates for peripheral communication range from 300 to 38,400. Many standard interfaces are available such as RS-232. If communication with off-site devices is required, such as those located at the corporate office, then the need for modems should be addressed.

Networking both within the PPCS framework and between the PPCS and other plant computer systems can be accomplished using Local Area Network (LAN) technology. A LAN offers high-speed communications channels for connecting information and processing equipment. It is ideal for connecting together equipment located remotely from the computer room; for example, Data Acquisition, Control Room, Technical Support Center, and Emergency Operating Facility.

It is also well suited for networking with other plant computer systems such as those listed in the following:

- Safety Parameter Display System
- Plant Simulator
- Meteorological Information Data Acquisition System
- Personal Radiation Information System Monitoring (PRISM)
- Effluent Monitoring System
- Equipment Tag Out System
- Personnel badging INformation Data EXchange (INDEX)

The LAN is typically composed of coaxial, fiber optic and twisted pair cables due to their varying cost and capability. Fiber optic cable is the most expensive but offers the broadest bandwidth, that is, it can transmit the most data at the highest speed. Fiber optic cable is, therefore, typically used to connect the data acquisition hardware to the host CPU due to the large amount of data collected and the high collection frequency. Coaxial cable costs less than fiber optic cable and has lower, but still substantial bandwidth. Coaxial cable, therefore, is typically used to connect nodes (equipment in same location) to the network due to their typically being located a long distance from the computer room. Coaxial cable is also normally used to network the PPCS to other plant systems. Where a significant distance exists between the computer room and other equipment areas, a LAN bridge is placed in line with the coaxial cable to boost the signals. Twisted-pair cable is significantly less expensive than coaxial cable but it has a very limited bandwidth. It is, therefore, more suitable for connecting peripherals with a single location. A single twisted cable is limited to about eight peripherals. An example of using these communication links is illustrated in Figure 6.

6. FUTURE FUNCTIONALITY ENHANCEMENT

Computer technology has been advancing rapidly. There are areas where hardware and software technology improvements are considered beneficial to the nuclear industry. The following are activities underway within the industry to produce these improvements to the plant process computer system.
6.1 Software

Future software will likely contain the following attributes:

- Data structures will become more object oriented.
- Information to the control room will become more hierarchical in nature with minimal raw process data immediately presented.
- The concept of sampling in classes (10 msec, 100 msec, 1 sec, etc.) will disappear as data acquisition capabilities exceed the rate of the field inputs.
- Modeling of data objects will allow design changes to be observed and documented as they occur.
- Computer Aided Software Engineering (CASE) tools will become prevalent with easy validation of robust software protocol.

Future monitoring and diagnostic capabilities can be extended to create PPCS applications to support normal and abnormal plant operating conditions and include the following:
6.1.1 Emergency Operating Procedures Tracking

This system is designed to support the operators’ decision-making process by continuously monitoring and comparing the current plant state against the symptoms in the EOP’s and providing the recommended operator actions. This type of application could be very useful for operator training of EOP’s as well as serve those individuals responsible for emergency management.

6.1.2 Accident Sequence Prediction

This would be an expert system that would use current plant conditions during an abnormal event to determine where the plant is headed and provide guidance so that the event does not lead to an accident condition. This system would be useful to both the plant operators as well as to those individuals in the Technical Support Center (TSC) and the Emergency Operating Facility (EOF) responsible for emergency management.

6.1.3 Safety System Status

This application gives the status of critical safety systems to aid the operators in responding to an abnormal event. This system would also be useful to those individuals in the TSC and EOF responsible for accident management. Some versions of this program exist; however, the numerous field inputs required to support these applications do not always exist and so the status of these components must be fixed. This limitation in field instrumentation could limit the program’s usefulness during a dynamic plant event.

6.1.4 Off-Site Dose Prediction

Personal computer and mainframe-based applications exist to predict the dose to the public from radiation released to the environment. This type of application could be integrated with the PPCS to form a cadre of codes to serve those individuals responsible for radiation protection.

6.1.5 Voice Recognition

Voice recognition applications would enhance the man-machine interface for requesting and receiving PPCS information. Data could be requested by object (e.g., reactor coolant system loop temperatures), opposed to database attributes (e.g., temperature analog input point and received in verbal, graphical, or tabular format. This response could be made conditional on verbal limits, e.g., temperature verbally announced periodically or if it rises above certain threshold.

6.1.6 Plant Performance Monitoring

A long-term data archival/retrieval and analysis application would provide longterm monitoring of component efficiency to identify maintenance problems that are slow to develop.

6.1.7 Calibration Reduction

Application of signal validation techniques for performing calibration reduction would be useful to monitor sensor outputs for single degradation by comparing actual readings against expected values.

6.1.8 Alarm Filtering

An alarm filtering application would reduce nuisance alarms and provide alarm prioritization. This application could also aid in the identification of database alarm limits that are improperly set.
6.2 Hardware

Future hardware will likely contain the following attributes:

- Computer-based intelligence will be further distributed and specialized.
- Data acquisition hardware will allow local analysis and present an object-oriented current value of database.
- Data presentation hardware will allow natural graphical modeling with less distinctions between interfaces of man and machine.
- Multi-tasking of applications and display will improve display hardware utilization.

Several hardware enhancements to the PPCS identified for future consideration are:

6.2.1 Optical Disk

This application of optical disk storage would enhance data storage and archival purposes. Use of Write Once Read Many (WORM) technology could improve the speed and ease of current magnetic tape backup storage of parameters tracked over long time periods, and be applied to tracking software Configuration Management and database changes.

6.2.2 Large Monitors

The application of large monitors (above 25" diagonal width) would improve viewing from afar as well as supporting multiple display (e.g., tiles or windowing).

7. CONCLUSION

Original plant process computers at nuclear power plants are becoming obsolete, resulting in increased difficulties in their effectiveness in supporting plant operation and maintenance. Plant process computer replacement and upgrade involves significant cost to the utilities. A prudent approach to upgrade with enhanced functions can not only solve the plant process computer obsolescence problem, but can also help utilities reduce the operation and maintenance cost, can support improved fuel designs, and increase plant and people productivity. The plant process computer upgrade can also provide a key note for the utility-wide and plant-wide monitoring, as well as diagnostic network, to support future plant instrumentation and control upgrades.

REFERENCES


<table>
<thead>
<tr>
<th>ABBREVIATIONS</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGR</td>
<td>advanced gas cooled reactor</td>
</tr>
<tr>
<td>BWR</td>
<td>boiling water reactor</td>
</tr>
<tr>
<td>CAD</td>
<td>computer aided design</td>
</tr>
<tr>
<td>CANDU</td>
<td>Canadian heavy-water reactor</td>
</tr>
<tr>
<td>CRT</td>
<td>cathode ray display</td>
</tr>
<tr>
<td>DDC</td>
<td>distributed digital control</td>
</tr>
<tr>
<td>EOP</td>
<td>emergency operating procedures</td>
</tr>
<tr>
<td>EQ</td>
<td>equipment qualification</td>
</tr>
<tr>
<td>ESF</td>
<td>engineered safety features</td>
</tr>
<tr>
<td>I&amp;C</td>
<td>instrumentation and control</td>
</tr>
<tr>
<td>IWG NPPCI</td>
<td>international working group on nuclear power plant control</td>
</tr>
<tr>
<td>LAN</td>
<td>local area network</td>
</tr>
<tr>
<td>NPP</td>
<td>nuclear power plant</td>
</tr>
<tr>
<td>O&amp;M</td>
<td>operation and maintenance</td>
</tr>
<tr>
<td>PLC</td>
<td>programmable logic controller</td>
</tr>
<tr>
<td>PWR</td>
<td>pressurized water reactor</td>
</tr>
<tr>
<td>QA</td>
<td>quality assurance</td>
</tr>
<tr>
<td>ROM</td>
<td>read-only memory</td>
</tr>
<tr>
<td>SPDS</td>
<td>safety parameter display system</td>
</tr>
<tr>
<td>SPIN</td>
<td>a French design of integrated digital protection system</td>
</tr>
<tr>
<td>TMI</td>
<td>Three Mile Island</td>
</tr>
<tr>
<td>UATP</td>
<td>protection acquisition and processing unit</td>
</tr>
<tr>
<td>ULS</td>
<td>safeguard logic unit</td>
</tr>
<tr>
<td>VDU</td>
<td>video display unit</td>
</tr>
<tr>
<td>V&amp;V</td>
<td>verification and validation</td>
</tr>
</tbody>
</table>
CONTRIBUTORS TO DRAFTING AND REVIEW

Aleite, W.  
Siemens AG, KWU Group  
P.O. Box 3220  
D-91050 Erlangen, Germany

(1)

Andersson, A.  
Swedish State Power Board  
Ringhals Nuclear Power Station  
S-430 22 Väröbacka, Sweden

1)

Andersson, O.  
Swedish State Power Board  
Forsmark Power Station  
S-742 03 Osthhammar, Sweden

(1,4)

Barache, J.M.  
Chef du Départament Information  
Electricité de France  
6 Rue Ampere  
93208 Saint-Denis, France

(2,3)

Bastl, W.  
Gesellschaft für Reaktorsicherheit mbH  
Forschungsgelaende  
D-85748 Garching, Germany

(1,2,3,4)

Boothroyd, A.D.  
International Atomic Energy Agency  
Division of Nuclear Power  
Wagramestrasse 5, P.O.Box 100  
A-1400 Vienna, Austria

(1,4)

Cook, A.B.  
Canatom Inc.  
184 Front Street East, 5th Floor,  
Toronto, Ontario M5A 4N3, Canada

(1,2,3,4)

Dusic, M.  
International Atomic Energy Agency  
Division of Nuclear Safety  
Wagramestrasse 5, P.O.Box 100  
A-1400 Vienna, Austria

(1)

Elshin, A.V.  
Science and Research Institute of Technology  
188 537 Sosnovy Bor  
Leningrad Region, Russian Federation

(4)

Ets, A.  
Smartware Associates, Inc.  
4805 Davron Street, Laurel  
Maryland 20707-3105, United States of America

(4)

Farað, P.  
PAKS Nuclear Power Plant  
H-7031 Paks, P.O. Box 71, Hungary

(1)

Faya, A.  
Atomic Energy Board  
Ottawa K1P 5S9, Canada

(4)

Hamar, K.  
Nuclear Safety Inspectorate  
P.F. 676, Budapest 14, H-1539, Hungary

(4)

Kossilov, A.  
International Atomic Energy Agency  
Division of Nuclear Power  
Wagramestrasse 5, P.O.Box 100  
A-1400 Vienna, Austria

(1,2,3,4)

Leret, E.  
EDF-DFR  
6, Quai Watier  
F-78400 Chatou, France

(4)

Lux, I.  
Central Research Institute for Physics  
Institute for Atomic Energy Research  
H-1525 Budapest 114, P.O. Box 49, Hungary

(1)
McPhedran, M.T. Ontario Hydro
Control Computers Section, Darlington Engineering Dept.
700 University Ave. H16 A14
Toronto, Ontario M5G 1X6, Canada

Nozdrin, G.N. Institute "Atomenergoproekt"
7 Bakuninskaya str.
Moscow 107815, Russian Federation

Pobedonostsev, A.B. Design Bureau, Burnakovsky proezd, 15
Experimental Machine Buildings
603603 Nizhny Novgorod - 74, Russian Federation

Shinohara, Y. Nuclear Power Engineering Corporation
Systems Safety Department
Fujita Kanko Toranomon Bldg., 5F
3-17-1, Toranomon, Minato-ku, Tokyo 105, Japan

Spohn, D. Electricité de France
Service de la Production Thermique
B.P. 26, 13-27 Espl. Charles de Gaulle
F-92060 Paris la Défense Cedex 57, France

Sun, B. Electric Power Research Institute
Nuclear Power Division
3412 Hillview Avenue
Palo Alto, CA 94303, United States of America

Wall, N. Atomic Energy Agency
Building B41/309, Winfrith, Dorchester
Dorset DT2 8DH, United Kingdom

Welbourne, D. NNC Ltd
Booths Hall, Chelford Road
Knutsford, Cheshire WA16 8QZ
Risley, Warrington WA3 6BZ, United Kingdom

Advisory Group Meetings

Consultants Meetings
Vienna, 2-6 December 1991 (2), Vienna 5-9 October 1992 (3)
1984 Nuclear Power Plant Instrumentation and Control. A Guidebook
   (Technical Reports Series No. 259)

   Guide (Safety Series, 50-SG-D8)

1985 Diagnosis of and Response to Abnormal Occurrences at Nuclear Power Plants
   (IAEA-TECDOC-334)

1987 Improving Nuclear Power Plant Safety Through Operator Aids
   (IAEA-TECDOC-444)

1988 Man-Machine Interface in the Nuclear Industry (Proceedings of International
   Conference, Tokyo, 15-19 February, 1988 (STI/PUB/781)

1988 Manual on Quality Assurance for Computer Software Related to the Safety of Nuclear
   Power Plants (Technical Reports Series No. 282)

1989 Manual on Quality Assurance for Installation and Commissioning of Instrumentation,
   Control and Electrical Equipment in Nuclear Power Plants
   (Technical Reports Series No. 301)

1990 Control Rooms and Man-Machine Interface in Nuclear Power Plants
   (IAEA-TECDOC-565)

1990 Reviewing Computer Capabilities in Nuclear Power Plants (IAEA-TECDOC-561)

1991 Safety Implications of Computerized Process Control in Nuclear Power Plants
   (IAEA-TECDOC-581)

1992 Balancing Automation and Human Actions in Nuclear Power Plants (Proceedings of
   International Symposium, Munich, 9-13 July, 1990 (STI/PUB/843)


1992 The Role of Automation and Human in Nuclear Power Plants (IAEA-TECDOC-668)

1992 Safety Analysis of Nuclear Power Plant Automation and Robotics (IAEA-TECDOC-
   672)

1994 Software Important to Safetry in Nuclear Power Plants
   (Technical Report Series No. 367)

1994 Operator Support Systems in Nuclear Power Plants (IAEA-TECDOC-762)
QUESTIONNAIRE ON IAEA-TECDOCs

It would greatly assist the International Atomic Energy Agency in its analysis of the effectiveness of its Technical Document programme if you could kindly answer the following questions and return the form to the address shown below. Your co-operation is greatly appreciated.

Title: Computerization of operation and maintenance for nuclear power plants
Number: IAEA-TECDOC-808

1. How did you obtain this TECDOC?

[ ] From the IAEA:
   [ ] At own request
   [ ] Without request
   [ ] As participant at an IAEA meeting
[ ] From a professional colleague
[ ] From library

2. How do you rate the content of the TECDOC?

[ ] Useful, includes information not found elsewhere
[ ] Useful as a survey of the subject area
[ ] Useful for reference
[ ] Useful because of its international character
[ ] Useful for training or study purposes
[ ] Not very useful. If not, why not?

3. How do you become aware of the TECDOCs available from the IAEA?

[ ] From references in:
   [ ] IAEA publications
   [ ] Other publications
[ ] From IAEA meetings
[ ] From IAEA newsletters
[ ] By other means (please specify)
[ ] If you find it difficult to obtain information on TECDOCs please tick this box

4. Do you make use of IAEA-TECDOCs?

[ ] Frequently
[ ] Occasionally
[ ] Rarely

5. Please state the institute (or country) in which you are working:

Please return to: R.F. Kelleher
Head, Publishing Section
International Atomic Energy Agency
P.O. Box 100
Wagramerstrasse 5
A-1400 Vienna, Austria