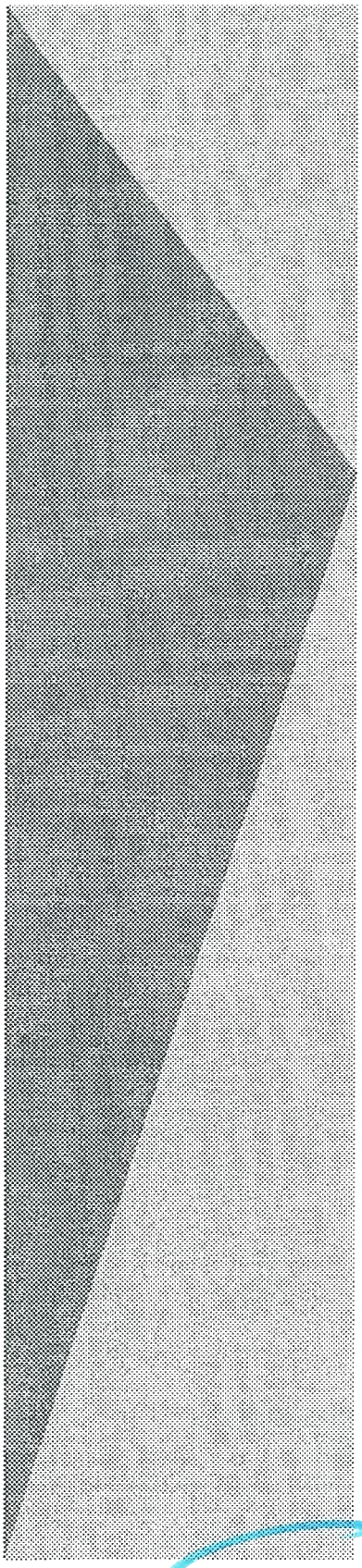
SCK•CEN
STUDIECENTRUM VOOR KERNENERGIE
CENTRE D'ÉTUDE DE L'ÉNERGIE NUCLÉAIRE

FLINS

Volume 2



Intelligent Technologies for Man-Machine Interaction at the OECD Halden Reactor Project

Special Presentations of FLINS'94

Edited by Da Ruan

SCK•CEN BLG-665

FLINS, an acronym for Fuzzy Logic and Intelligent Technologies in Nuclear Science, is the name of a new international research forum aiming to advance the theory and applications of fuzzy logic and novel intelligent technologies in the domain of nuclear science and engineering.

D. Ruan
FLINS chairman, SCK•CEN
Nuclear Research Centre
Boeretang 200, B-2400 Mol
Phone: + 32 14 33 22 01
Fax: + 32 14 32 15 29
e-mail: flins@bmlsck11.bitnet

FLINS'94, the first international workshop in this framework, was organized by the Belgian Nuclear Research Centre SCK•CEN and successfully held in the Sun Parks Hotel in Mol, Belgium, September 14-16, 1994. The workshop was co-sponsored by Belgoprocess, ECN-Petten, FBFC International, OMRON Electronics Europe BV, NIRAS/ONDRAF, Belgonucléaire, and the Belgian National Science Foundation.

Of more than 70 papers submitted from 13 countries, 56 were accepted for the FLINS'94 proceedings and published by the World Scientific Publishing Co. in Singapore, in August 1994. The workshop was attended by about 80 people from Austria, Belgium, China, Czech, France, Germany, Korea, the Netherlands, Norway, Russia, the United Kingdom, and the United States of America.

The FLINS'94 workshop was very successful in launching the new activities between scientists working in nuclear science and engineering, and the fuzzy research world. A total of 37 speakers lectured on mathematical tools, engineering, nuclear science, and the Halden reactor project in Norway. In particular, they covered the domains of radiation protection, safety assessment, human reliability, safeguards, nuclear reactor control, production processes in the fuel cycle, dismantling, and waste and disposal, with a clear link to theory and applications, robotics, man-machine interface, and decision-support techniques.

This second FLINS volume is dedicated to the special session on the Halden reactor project presentations during the FLINS'94 workshop. It provides elements of intelligent technologies for man-machine interaction at the OECD Halden reactor project. The volume starts with a brief introduction about the Halden reactor project by Marc Vankeerberghen and Frans Moons (co-researchers and coordinators of the Halden reactor project at SCK•CEN). Then follow the four full papers abstracted in the FLINS'94 proceedings: "Man-machine systems research at the OECD Halden reactor project" by F. Øwre, T. J. Bjørlo, and K. Haugset, "Computer-based operator support systems" by Ø. Berg, T. J. Bjørlo, and F. Øwre, "Halden Project activities on software dependability" by G. Dahll and T. Sivertsen, and "Retrofitting of NPP computer systems" by G. Pettersen.

This FLINS volume will be of interest to researchers working in the domains of both nuclear science and intelligent technologies. Moreover, it will stimulate the FLINS activities in today's world. I would like to thank T. J. Bjørlo for his permission, on behalf of the OECD Halden reactor project, to issue this FLINS volume; all the above-mentioned contributors for their kind cooperation and extended papers; and P. D'hondt, P. Govaerts, and E. Kerre for their encouragements and advice regarding the FLINS activities.

Contents

The Halden Project is an internationally funded and staffed nuclear research and development organization with its headquarters in Halden, Norway. It is operated under the auspices of the OECD and is sponsored through an agreement between the participating organizations. These represent a complete cross section of the nuclear industry, including national research organizations, reactor and fuel vendors, utility companies, and licensing or regulatory authorities.

The Halden Reactor Project

M. Vankeerberghen,
F. Moons

The following countries, through their representatives, participate in the joint programme of the Halden Reactor Project:

- Belgium: Nuclear Research Centre (SCK•CEN);
- Czech Republic: Nuclear Research Institute (NRI);
- Denmark: Risø National Laboratory;
- Finland: Ministry of Trade and Industry;
- France: Electricité de France (EdF);
- Germany: Gesellschaft für Reaktorsicherheit (GRS);
- Italy: Ente per le Nuove Tecnologie, l'Energia e l'Ambiente (ENEA);
- Japan: Japan Atomic Energy Research Institute (JAERI);
- the Netherlands: NV Tot Keuring van Elektrotechnische Materialen (KEMA);
- Norway: Institutt for Energiteknikk (IFE);
- Spain: Centro de Investigaciones Energéticas, Medioambientales y Tecnológicas (CIEMAT);
- Sweden: Nuclear Power Inspectorate (SKI);
- Switzerland: Federal Nuclear Safety Inspectorate (HSK);
- United Kingdom: Nuclear Electric plc;
- United States of America: Nuclear Regulatory Commission (NRC).

These countries determine the joint programme's direction, through two Programme Group and Board of Management meetings per year, and have at their disposal the research results of the Halden Reactor Project. They can also actively take part in the research activities by seconding staff to Halden or performing related research at their respective sites. Besides the joint research programme, bilateral research contracts are possible, too.

The strength of the Halden Project is largely built on the characteristics of the Halden Boiling-Water Reactor. This reactor has a great operational flexibility and its spacious and accessible core enables extensive in-core instrumentation. This feature has made the Halden reactor one of the most versatile test reactors in the world. The research programmes of the Halden Project address the development of man-machine systems and the performance of nuclear fuel and materials.

Man-machine systems

Man-machine systems are of particular interest to FLINS (Fuzzy Logic and Intelligent Technologies in Nuclear Science). They emphasize human factors analysis and computer-based control and monitoring of the operational aspects of plants, such as nuclear power plants.

The research and development efforts focus on
- software reliability in a safety-critical environment;
- human factors that affect the interaction between man and computer;
- surveillance and control systems for advanced control rooms;
- tools for the efficient creation and integration of user interfaces in process control;
- computerized operator support.

Topics of specific research include
- formal software development using algebraic specification;
- safety assessment methodologies for proprietary software;
- evaluation of expert systems for diagnosis of reactor malfunctions;
- development and evaluation of an integrated surveillance and control system;
- early fault detection and computerized alarm handling systems;
- computerized procedure system;
- computerized accident management support;
- user interface management system;
- core surveillance system.

Fuel and materials

The reliability of fuel and core material still is the prime motivation for the activities at the Halden Project. Potential performance-limiting parameters are studied in steady and transient operation.

The research and development efforts focus on
- extended burnup performance of nuclear fuel;
- nuclear materials testing;
- rig instrumentation;
- experimental-data management.

Topics of specific research include
- fuel conductivity degradation;
- gap conductance in fuel rods;
- fuel-rod stored heat;
- fission-gas release;
- development of fuel-rod instrumentation;
- cladding creep, corrosion, and stress corrosion;
- in-reactor component ageing;
- water chemistry effects.

SCK•CEN and the Halden Project

SCK•CEN represents private and public Belgian organizations to the Halden Reactor Project. Currently, it acts in its own name and on behalf of AIB Vinçotte Nucléaire, Belgonucléaire, and Tractebel.

The nature of the exchange between SCK•CEN and Halden is both technical and managerial. On the technical level, the cooperation concerns instrumentation, data acquisition, development of models, BR2 refurbishment, and neutronic calculations. Managementwise, discussions focus on topics of common interest as training, use of reactor facilities, marketing, and programmes for nuclear fuels and materials. The cooperation between SCK•CEN and Halden is particularly relevant because of the complementary nature of SCK•CEN's BR2 reactor—the Belgian Reactor 2, a materials testing reactor—and Halden's BWR (Boiling-Water Reactor).

In the framework of FLINS, the cooperation between SCK•CEN and the Halden Reactor Project must be seen in the broader light of artificial intelligence. The control rooms of the future will make increasing use of computers for alarm handling, procedures, surveillance, fault diagnosis, etc. Halden's approach is presently orientated towards the use of knowledge-based systems to assist the operator. They develop tools to support this approach and perform verification and validation studies on the used software. SCK•CEN has introduced the fuzzy logic approach in some of its research activities (see *Basic Concepts in Nuclear Research. Core Activities at the Belgian Nuclear Research Centre.* Edited by Da Ruan, SCK•CEN FLINS vol. 1, BLG-653, 1994).

Halden contributions to FLINS'94

The present BLG report of SCK•CEN presents the four contributions of the Halden Reactor Project to the first international FLINS workshop on Fuzzy Logic and Intelligent Technologies in Nuclear Science organized by SCK•CEN. The first of these Halden-FLINS papers gives an overview of the activities in the area of man-machine systems research at the OECD Halden Reactor Project. The second paper touches on the specific topic of computer-based operator support systems. The third paper analyses the issues involved in developing reliable software. The last paper shows the possibilities of introducing some of those ideas when retrofitting nuclear power plant computer systems.

MAN-MACHINE SYSTEMS RESEARCH AT THE OECD HALDEN REACTOR PROJECT

F. Øwre, T. J. Bjørlo, K. Haugset
OECD Halden Reactor Project
Halden, Norway
Phone: +47 69-183100
Fax: +47 69-187109

ABSTRACT

The OECD Halden Reactor Project is a joint undertaking of national organisations in 15 countries sponsoring a jointly financed research programme under the auspices of the OECD - Nuclear Energy Agency. One main research area is man-machine systems addressing the operator tasks in the control room environment. The overall objective of these efforts is to provide a basis for improving today's control rooms through introduction of computer-based solutions for effective and safe execution of surveillance and control functions in normal as well as off-normal plant situations. The programme comprises four main activities: 1) verification and validation of safety critical software systems, 2) man-machine interaction research emphasising improvements in man-machine interfaces on the basis of human factors studies, 3) computerised operator support systems assisting the operator in fault detection/diagnosis and planning of control actions, and 4) control room development providing a basis for retrofitting of existing control rooms and for the design of advanced concepts.

1. Development trends and research needs in I & C and control room technology for NPPs

The fields of Instrumentation & Control (I & C) as well as general information technology have developed rapidly over the last decade. Currently new I & C systems are largely based on digital solutions replacing the old analogue equipment. In the area of computer technology there have been dramatic improvements in costperformance for both hardware and software.

Within non-nuclear industry this new I & C technology has been taken widely into use, and fully digitally based I & C systems and control room solutions are commonplace. So far this new technology has only to a limited extent been taken into use in operating nuclear power plants. The nuclear industry is, however, recognising the need for upgrading the instrumentation and control systems in existing nuclear power plants. Many operating NPPs have I & C systems of yesterday's technology. The components of these systems are becoming obsolete, and the support from the I & C industry for these old systems deteriorates leading to escalating maintenance and operation costs for the NPPs utilising these old systems. Upgrading and backfitting of existing control rooms are thus high priority issues within the nuclear industry, and backfitting programmes, introducing computer-based solutions for surveillance and control as well as for improving man-

machine interfaces, are taking place at many NPPs. The EPRI initiated "Integrated Instrumentation and Control Upgrade Plan " within the US nuclear industry is a prime example of such upgrading efforts, (1).

At the same time designs for tomorrow's power reactors are developed, characterised by almost fully digital instrumentation and control systems, and advanced, computer-based control rooms. These designs take advantage of the developments which have taken place within I & C and information technology. Generally, the trend in these new designs are towards a higher automation degree, changing the operator's role towards supervision, error detection, problem solving and planning rather than routine plant control functions. The N4 series of PWRs under construction in France (two first units under construction at Chooz) (2) and the Advanced Boiling Water Reactors (ABWR) under construction in Japan (3) are examples of highly automated plants, with advanced, computer-based control room solutions.

The introduction of digital I & C systems and computer-based control room solutions in NPPs, both through backfitting existing plants, as well as through construction of new plants with modern I & C and control room design, requires research and development efforts to ensure that the new technology provides the expected improvements in operational safety and efficiency. There is a need for establishing standards and guidelines for safety-related and safety critical software, especially licensing issues in connection with such software. Further, design guidelines are needed for improved man-machine interfaces, utilising the potentials of the new technologies. There is also a need for establishing a validation methodology for the new man-machine systems, especially with respect to the human factors issues. The changing role of the operators due to the higher degree of automation requires development of systems supporting the new operator role, assisting him/her in error detection, problem solving and planning.

2. Man-machine systems research at the Halden Project

The research programme at the Halden Project addresses the research needs of the nuclear industry in connection with introduction of digital I & C systems in NPPs. The programme provides information supporting design and licensing of upgraded, computer-based control room systems, and demonstrates the benefits of such systems through validation experiments in Halden's experimental research facility, HAMMLAB and pilot installations in NPPs.

The programme includes four main areas: 1) verification and validation, 2) man-machine interaction research, 3) computerised operator support systems, and 4) control room development. Fig 1 illustrates how these areas are interconnected and also shows the type of deliverables from the different areas.

The activity on *verification and validation* addresses software safety and reliability aspects. The work comprises investigations of methods and tools which can be used to improve the reliability and verify the safe use of computerised control and supervision systems for nuclear power plants. The results provide a basis for establishing guidelines for design and licensing of safety related software.

The work in the *man-machine interaction* area aims at enhancing safe and efficient operation of nuclear power plants through improving the man-machine interfaces of the control room systems based on human factors considerations. To this end experimental evaluation of the systems is performed in HAMMLAB using operators from the Halden Reactor as test subjects. In addition to improving the man-machine interface of the specific operator support systems being developed at Halden, the analyses of these validation experiments provide a more general understanding of factors influencing operator behaviour. This knowledge is utilised to establish technical bases for guidelines for design and evaluation of man-machine interfaces.

The work on *computerised operator support systems* addresses development of systems assisting the operator in functions like fault detection, diagnosis and prognosis, and advisory systems aiding him in action planning and implementation. The work in this area is primarily aimed at developing systems for backfitting in current control rooms, but the resulting systems are also applicable as modules within more integrated surveillance and control systems in advanced control rooms.

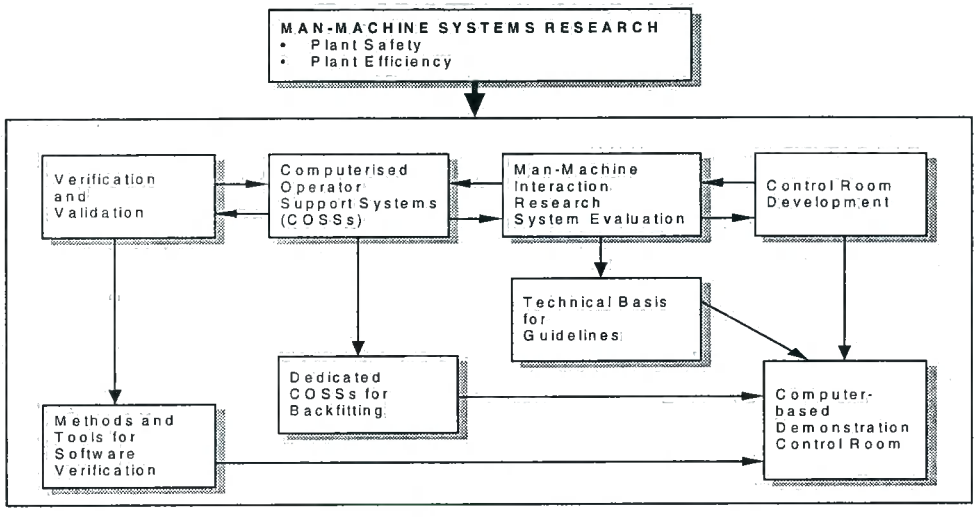


Fig.1 Man-Machine Systems Research Programme

Upper four boxes show the four main programme items, lower four shows the main products from the research programme at Halden.

The activity on *control room development* addresses the potentials and possible problems of completely computer-based control rooms including several operator support systems. The work comprises integration of these systems focusing on co-ordination and prioritisation of information, man-machine interfaces and underlying hardware/software structures. A demonstration version of a fully digital control room is established in HAMMLAB. This demonstration control room is utilised to gather information of relevance for the introduction of digital control room solutions in nuclear power plants.

3. Verification and Validation of Software Reliability

Currently, there is a lack of well-established criteria for development and validation of safety critical software within the nuclear industry. This has caused some serious problems in the introduction of such systems in NPPs, e.g., the delay in the start-up of the Darlington plant in Canada due to licensing issues concerning the computer-based protection system, (4) and the abandoning of the P20 CONTROBLOC control system for the N4 plants in France due to too complicated software structures and uncertainty about 1E qualification of the system, (5).

The Halden Project has for a number of years been working in the field of software verification and validation. The overall goal of these efforts is to investigate and assess methods and tools which can be used to improve the reliability of computer-based systems and to verify their safety when used in the control and supervision of nuclear plants. Methods and tools which can assist in the licensing process of software in safety critical computer systems are particularly addressed, including guidelines used by the producers of software as well as by licensing authorities for the certification of safety related software, (6).

The research programme is focused on the following topics:

- *Formal Methods in Software Development*

The use of formal methods in software development is based on applying mathematical techniques to describe the properties of the desired system. A formal method provides a mathematically based framework within which specification, development and verification of software systems can be done in a systematic and precise way.

In a joint project between the Safety and Reliability Directorate (SRD) in UK and the Halden Project, assessments of different formal methods with respect to their applicability in development of safety-related software for NPPs are being performed.

The Halden Project is also developing a method and associated tools for formal software development based on the use of algebraic specifications. The practical applicability of formal methods in software development will be investigated in a realistic case example for a safety function of a NPPs as part of the on-going research programme at the Halden Project.

- *SOftware SAfety Tools (SOSAT) Project*

The SOSAT project is a co-operative effort between the Halden Project and German member organisations. The objective of the SOSAT project is to improve practical analysis and assessment of safety related software through developing tools which can assist in the program analysis by automising parts of the necessary manual routine work. A set of tools has been developed which can analyse programs implemented on a variety of microprocessors, (7). The approach is based on "reversed engineering" starting from a hexadecimal memory dump of the implemented program in the processor. A disassembler extracts the program from this core dump and translates it into a common

assembly language CAL. The CAL code forms the basis for the further program analysis. Various types of analysis can be performed using the SOSAT tools set such as basic program measurements and checks, and static and dynamic program analyses to verify that the program as implemented in the processor is in agreement with the program specification.

- *Safety Assessment of Proprietary Software*

A research programme has recently been started aimed at establishing an assessment framework for proprietary software. The "proven design" principle is often used by producers to state the quality of their software systems. An investigation of what kind of information the producers should provide to get their software accepted as proven design will be made, and a proposal for accepted "proven design" material should be included in the assessment framework.

4. Man-Machine Interaction Research

The process used for man-machine interaction research at Halden is shown in Fig. 2 which identifies the five major elements of this process: problem identification, development of computerised operator support systems (COSSs) and man-machine interfaces (MMIs), experimental evaluation, human performance analysis, and technical bases for guidelines.

The experimental evaluation of systems in HAMMLAB is the basis for the research programme. As shown in Fig. 2 the results from the analyses of the experiments provide direct design feedback to the specific systems being evaluated as well as general knowledge on man-machine interaction which can be used for development of generic guidelines for design and evaluation of computerised operator support systems (COSSs) and man-machine interfaces (MMIs).

- *Problem Identification*

The goal of the problem identification activity is to identify the real and most urgent problems in today's control rooms in order to have a basis for suggesting and realising solutions to these problems. The activity thus provides important input to the development of COSSs and MMIs at the Halden Project.

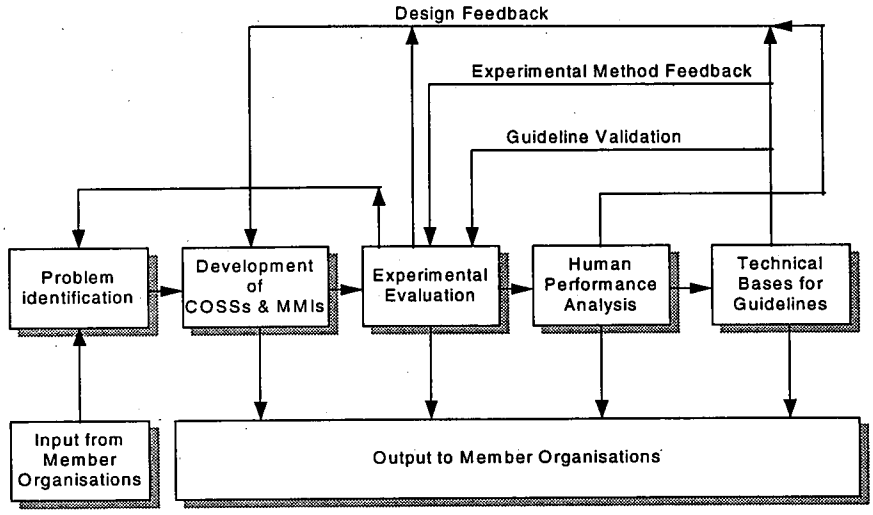


Fig. 2 Man-Machine Interaction Research Process

- *Experimental Evaluation*

The experimental evaluation of the COSSs and MMIs developed at the Project forms the basis for the human factors work at Halden. The setting for this experimentation is the NORS simulator situated in HAMMLAB. NORS is a full-scale simulator of a PWR plant and while not being an exact replica of any one nuclear power plant, is, nevertheless, representative of a typical PWR.

Over the years a well-established infra-structure and methodology for performing evaluation experiments of new operator aids and man-machine interfaces has been developed. Operators from the Halden Reactor take part as test subjects in these experiments. A variety of data can be collected during the experimental sessions: video and audio recordings of the activities in the control room, logs of all interactions between the operators and the simulator (displays used, control actions performed, etc.) as well as logs of critical process parameters of relevance for judging the performance of the operating crew during a particular transient. In addition, operator interviews, questionnaires, debriefing sessions, verbal protocols, etc. are utilised to extract additional information for the later analysis of the experiments.

The experiments performed in HAMMLAB are of different types. Some studies focus on providing direct design feedback to a specific system, while other experiments aim at providing more general knowledge for use in defining technical bases for system design and evaluation.

In addition to evaluating the final systems, there is also need for evaluations at different stages of system development to provide early feedback on the quality of certain system features. The process illustrated in Fig. 2 is therefore often iterative, running through a series of experiments on a particular system, each contributing to a better design and an improved final system.

Over the years a number of COSSs have been evaluated in HAMMLAB, (8, 9, 10).

Currently, the work is focused on human error in cognitively demanding tasks, like diagnosis, planning and accident management.

- *Development of Technical Bases for Guideline Formulation*

While guidelines for design and evaluation of control rooms using conventional man-machine interfaces are in general available today, the basic knowledge required for design and evaluation of computer-based control rooms needs to be further developed. Existing guidelines for computer-based systems mainly address the questions of *how* to present information (symbols, colours, font size, etc.), while little guidance is given on *which* information is important, and how process control should be executed in an efficient manner. Thus, existing guidelines for evaluation of computer-driven man-machine interfaces and digital based control rooms are incomplete. System and control room developers as well as organisations evaluating and licensing man-machine interfaces are therefore in need for guidelines in this field.

A major objective of the human factors research at the Halden Project is to provide experimental data which can contribute to formulation of guidelines for design and evaluation of computer-driven man-machine interfaces. A considerable part of the experiments in HAMMLAB are thus focusing on generic issues in connection with operator performance in an advanced control room environment. A key issue in this work is to find a suitable format for describing the generic results such that they easily can be applied by member organisations in formulation of their guidelines. Presently, the Project is preparing "lessons learned" reports from the evaluation experiments performed at Halden where emphasis is placed on making the information relevant for guideline formulation available in a structured and easily accessible way.

5. Computerised Operator Support Systems (COSSs)

A common goal for both the human factors work and the systems work at the Project is to generate and test reliable and effective human-computer interfaces which can ensure operator awareness of plant situations and operating states. The work on surveillance and support systems addresses questions related to human-machine interaction in operator tasks such as fault detection, diagnosis, prognosis and procedure implementation. One emphasis is the development and tests of actual surveillance systems, another is developing man-machine interface design proposals.

The human-computer interface represents the boundary between functions allocated to operators and the software systems which are designed to support operator tasks. As such, it influences not only *what* information is presented to the operator, but also *how* it is presented, in addition to providing mechanisms for *taking actions* based upon decisions made about the information presented.

Figure 3 depicts the many relationships between the human-computer interface and the many surveillance systems available in process control settings. As can be seen, the systems or Instrumentation and Control (I&C) vehicles- do not exist in isolation, but interact in complex ways both with each other, and with the operator. The key to a properly functioning facility requires that all vital I&C vehicles operates effectively with

each other, and that they are compatible with and support information processing, action planning, selection and execution by the operator.

For further description of these COSSs, including systems for intelligent alarm handling, model-based early fault detection and diagnosis, core surveillance for operation planning and optimisation, and computerised procedure implementation, reference is made to a separate paper to this conference (8).

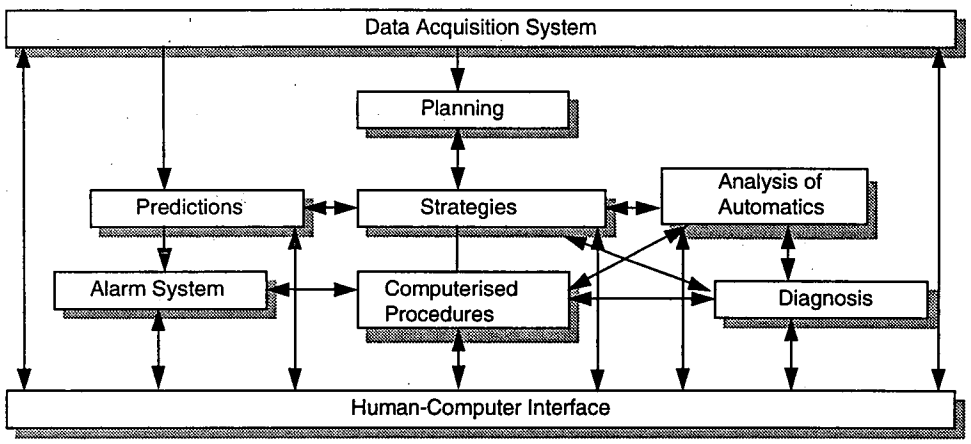


Fig. 3 Relationships between the man-machine interface and the surveillance systems

6. Control Room Development

The aim of the control room development work is relevant for retrofitting of today's control rooms as well as for development of future advanced control rooms. The main vehicle in this work is the Halden Man-Machine Laboratory (HAMMLAB) incorporating the NORS full-scale PWR simulator and the associated experimental control room. In 1991, the first version of the Integrated Surveillance And Control System, ISACS-1, was implemented in the experimental control room, and has during 1992-93 been stepwise improved and upgraded. The ISACS-1 system offers an integrated and flexible interface to the operators and allows extensive studies and demonstrations of features considered important in retrofitting of today's and development of future control rooms.

The ISACS control room concept (9, 10) includes features like integration of a large number of COSSs, co-ordination and prioritisation of information from the process and the COSSs through the intelligent Information Co-ordinator, IC, generation of new high-level information by the IC, and development of a uniform Man-Machine Interface, MMI. The MMI of ISACS-1 can easily be modified with respect to which information to display, how to display it, and the way manual process control is performed. Furthermore, the IC as well as any of the COSSs can be decoupled from the overall system. Utilising the flexibility, a wide range of control room set-ups can be simulated by the ISACS system. In this way, experience is gained on items like which information is important to

the operator, how should overview displays be designed, which information should they contain, etc.

The ISACS research programme also provides information regarding requirements to hardware/software structures when computerised tools are introduced in the control room. Through the ISACS implementation in HAMMLAB, experience with use of networks, expert systems and database management systems in a real-time environment is continuously being accumulated.

7. Concluding Remarks

Backfitting of nuclear power plant control rooms is a continuing process, introducing computer-based solutions for surveillance and control as well as for improving the human-computer interface. At the same time designs for tomorrow's reactors are developed, characterised by fully digital instrumentation and control systems, and advanced, computer-based control rooms. Research and development efforts are needed to ensure that the new technology gives the expected improvements in operational safety and efficiency.

The research programme at the Halden Project addresses the research needs of the nuclear industry in connection with introduction of digital I&C systems in NPPs. The programme provides information supporting design and licensing of upgraded, computer-based control room systems, and demonstrates the benefits of such systems through validation experiments in the simulator-based experimental control room facility at Halden.

At the Halden Project an internationally sponsored research programme is carried out which addresses these research issues. The Halden Man-Machine Laboratory represents a unique test-bed for investigating new, computer-based solutions for nuclear power plant control rooms. The research programme draws upon competence built up through more than 20 years work in the field of computer-based operator support and digital control room solutions, and the close contact with licensing authorities, utilities and reactor vendors in the 15 countries participating in the Halden Project ensures that the work is addressing the real research needs of the nuclear industry.

8. References

1. D. Wilkinson, L. Wray (editors): *"Integrated Instrumentation and Control Upgrade Plan"*. EPRI Report NP-7343, 1992.

2. M. Peyrton, M. Pirus: *"Progress on N4 I&C Architecture"*. ANS Topical Meeting on Nuclear Plant Instrumentation, Control and Man-Machine Interface Technologies, Oak Ridge, Tennessee, April 1993.

3. M. Makino, H. Nishiyama: *"Toshiba Advanced Instrumentation and Control System for Nuclear Power Plants"*. ANS Topical Meeting on Nuclear Plant Instrumentation, Control and Man-Machine Interface Technologies, Oak Ridge, Tennessee, April 1993.

4. Q.B. Chon, P.N. Acchione, R.J. Hohendorf: *"Digital Technology in Nuclear Power Plants: White Knight or Black Hole?"* ANS Topical Meeting on Nuclear Plant Instrumentation, Control and Man-Machine Interface Technologies, Oak Ridge, Tennessee, April 1993.

5. M. Peyrton, M. Pirus: *"Progress on N4 I&C Architecture"*. ANS Topical Meeting on Nuclear Plant Instrumentation, Control and Man-Machine Interface Technologies, Oak Ridge, Tennessee, April 1993

6. G. Dahll, T. Sivertsen: *"Halden Project Activities on Software Dependability"*. International Workshop FLINS'94, Mol, Belgium, September 1994.

7. G. Dahll, J.E. Sjøberg: *"SOSAT - A Set of Tools for Software Safety Assessment"*. Second European Conference on Software Quality Assurance, May 1990.

8. Ø. Berg, T.J. Bjørlo, F. Øwre: *"Computer-Based Operator Support Systems"*. International Workshop FLINS'94, Mol, Belgium, September 1994.

9. K. Haugset, N.T. Førdestrømmen: *"Realisation of the Integrated Control Room Concept ISACS"*. IEEE Fifth Conference on Human Factors and Power Plants, Monterey, June 1992.

10. J. Kvalem, R.-E. Grini, K. Haugset: *"ISACS. An Integrated Surveillance and Control System"*. 2nd International Conference on Database and Expert Systems Applications DEXA'91, Berlin, August 1991.

COMPUTER-BASED OPERATOR SUPPORT SYSTEMS

T.J. Bjørlo, Ø. Berg, F. Øwre
OECD Halden Reactor Project
P.O. Box 173 - N-1751 Halden

Norway
Phone: +47 69-183100
Fax: +47 69-187109

ABSTRACT

This paper presents functional descriptions of a number of computer-based operator support systems (COSSs) developed at the Halden Project. These include systems for intelligent alarm handling, model-based early fault detection and diagnosis, accident management support, core surveillance for operation planning and optimisation and computerised procedure implementation. In addition the Picasso-3 user interface management system and its application in development of COSSs are described.

1. Introduction

Through backfitting of nuclear power plant control rooms computer-based solutions for instrumentation and control systems replace old analogue equipment and CRT-based human-computer interfaces replace conventional control and instrument panels. At the same time designs for tomorrow's reactors are developed characterised by fully digital instrumentation and control systems, and advanced, computer-based control rooms. These trends open possibilities for improving the support given to the operators in their cognitive tasks. At the Halden Reactor Project efforts have been placed on exploring these possibilities through design, development and validation of Computer-based Operator Support Systems (COSSs) which can assist and support the operators in different operational situations, ranging from normal operation to disturbance and accident conditions.

The COSSs developed at the Halden Project are tested and evaluated through experiments in the simulator-based experimental control room at Halden (HAMMLAB) using operators from the Halden Reactor as test subjects. In this way the systems are developed to such a state that they easily can be taken over by member organisations and put into use in their NPP control rooms or simulators. However, since there are many different types of plants in the member countries, the systems developed at Halden are not tailor-made for any particular plant, but are developed as general tools which easily can be adapted to a specific plant through co-operative, bilateral projects with member organisations.

2. Surveillance Systems

2.1 Model-based Early Fault Detection

Early detection of faults and plant disturbances in nuclear power plants reduces the risk of disturbances developing into severe plant conditions (shutdown or accidents) since the operators have more time for diagnosis and counteractions. Further, early detection of the disturbance usually means better localisation of the problem area in the plant, thereby facilitating the diagnostic task. The traditional way of informing operators about possible problems is through alarm systems based on limit checking of process variables, which should stay within prescribed limits. In many cases a disturbance in a plant subsystem may propagate into neighbouring subsystems before the operator is alerted by the alarm systems. Therefore, the operator is confronted with a large number of alarms within a short period of time which makes the diagnostic task difficult. Alarm filtering techniques may reduce this problem to some extent by focussing on essential alarms (1,2).

An alternative method for fault detection is illustrated in Fig. 1. The method is based on mathematical reference models describing the dynamic behaviour of the process in normal operating conditions (no disturbances or faults in the process). By comparing measured process variables with corresponding calculated variables from the reference models in real-time, the time to detect disturbances can be reduced compared to traditional alarm systems. By splitting the reference models into a number of submodels where the input variables to each individual submodel are *measured* output variables from the preceding subprocess (Fig. 1), a good localisation of the problem area in the plant is obtained. By this technique, propagation of faults in the detection algorithms outside the particular subsystem containing the fault, is avoided thus reducing the diagnostic task (3). However, also this method requires additional rules for detailed diagnosis in order to discriminate among various possible failures within a subsystem which may cause an observed deviation between reference models and measurements. For instance, errors in the control system or instrumentation may turn out to be the real problem, but this type of failure should also be detected as early as possible.

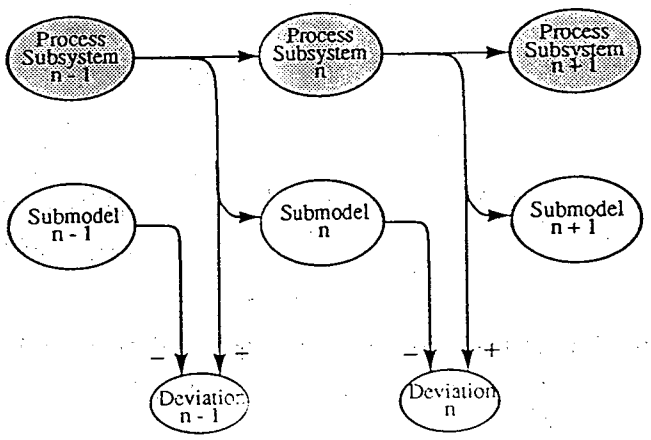


Fig. 1. The principle of model-based early fault detection

At the Halden Project Early Fault Detection (EFD) systems based on the method described above have been developed. Two pilot installations have been made at the Loviisa Nuclear Power Plants in Finland, one for leakage detection and one for signal validation of flow sensors. The systems have proved successful through detecting internal leakages in preheaters in the feedwater system and degradation of feedwater flow instruments (4).

2.2 *Surveillance of Critical Safety Functions*

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

These problems have resulted in a *function-oriented* approach to nuclear power plant monitoring for disturbances which potentially may develop into accidents. From systematic studies of scenarios that may lead to accidents a set of *critical safety functions* is defined. These functions have to be maintained to prevent serious consequences of the disturbance, like staff injuries and plant damage.

This function-oriented approach to plant monitoring has lead to development of so-called Safety Parameter Display Systems (SPDSs, also denoted Critical Function Monitoring Systems) which alarm the operators when critical safety functions are threatened. The emergency operating procedures (EOPs) have been restructured accordingly, the EOPs of nuclear power plants are now all *symptom-based* (i.e. function oriented) and aims at checking the status and maintaining the integrity of the critical safety functions.

The Halden Project has explored the concept of critical safety function monitoring through development and evaluation of different SPDS-types of systems. Together with Combustion Engineering the Halden Project evaluated the Critical Function Monitoring System (CFMS) and the Success Path Monitoring System (SPMS) in HAMMLAB (5). The SPMS system augments the monitoring of the critical safety functions through presenting to the operator the status of alternative success paths for maintaining a particular critical function in case it is threatened or lost. The experiments in HAMMLAB showed clear advantageous effects of supporting the operator with success path monitoring with respect to his performance during simulated accident scenarios .

In a co-operation between Vattenfall and its unit 2 at the Forsmark NPP, the Swedish Nuclear Inspectorate, the vendor ABB Atom, and the Halden Project a computerised operator support system (denoted SAS-II) has been developed.

The Forsmark 2 plant is designed in such a way that initiation and execution of safety measures take place automatically. The intention is to bring the plant to a safe state without human intervention during the first 30 minutes. These automatic measures are called *safety sequences*.

The main purpose of the SAS-II system is to monitor the critical safety functions and to provide through the display system the necessary information to the shift supervisor such that he can handle the symptom-oriented EOPs when these safety functions *have or should have* been initiated, most often after a scram of the reactor.

The monitoring of the critical safety functions is performed according to the following principles.

- SAS-II monitors and presents on a continuous basis the plant status with respect to whether or not any critical safety function is threatened. This is called the *symptom supervision*. Symptoms are mainly one or more important process values per critical safety function which indicate the status, the *health*, of this function.
- After a scram SAS-II automatically evaluates and presents whether or not the automatically initiated safety sequences have achieved the expected results. This is called *system supervision*.

The SAS-II software system is designed and structured to support the above described concepts. One part of the system is developed and executed under control of the real-time expert system G2. A knowledge-base has been constructed that represents non-successful behaviour of the plant automatics and control systems in terms of the defined critical safety functions. The other part of SAS-II consists of the man-machine interface for the shift supervisor developed and executed under control of the Picasso graphic display system developed at the Halden Project (8).

The SAS-II system has been integrated with the compact simulator at the Forsmark NPP where an extensive validation programme with 11 shift supervisors and senior reactor operators from Forsmark NPP unit 2 has been carried out (6).

A revision of the SAS-II system to bring it in accordance with the revised EOPs of Forsmark unit 2, and installation of the system in the full-scope training simulator for further validation experiments prior to installation in the Forsmark-2 control room is being considered. A decision is expected during 1994.

2.3 Intelligent Alarm Handling

One of the main tasks for operators in nuclear power plants is to identify the status of the process when unexpected or unplanned situations occur. The alarm system is the main information source to detect disturbances in the process, and alarm handling has received much attention after the TMI accident in 1979. It was realized that conventional alarm systems created cognitive overload for the operators during heavy transients.

Over the years the Halden Project has explored different approaches to alarm handling, like alarm filtering techniques, model-based alarm systems (see chapter 2.1) and function oriented approaches like critical safety function monitoring as described in chapter 2.2.

The experience gained from the work with these different alarm systems has shown that there is a need for a generic tool for configurating more intelligent alarm systems where different alarm handling techniques can be integrated. Therefore, the Halden Project is developing an alarm system toolbox, called COAST, which makes it possible to build integrated alarm systems through mechanisms for addressing different principles for alarm generation, structuring and presentation.

COAST will contain facilities for building specific alarm systems as well as facilities for alarm system execution. It will be an integral part of the final alarm system, and not only act as a tool for building dedicated systems. COAST is shown in its final environment in Fig. 2.

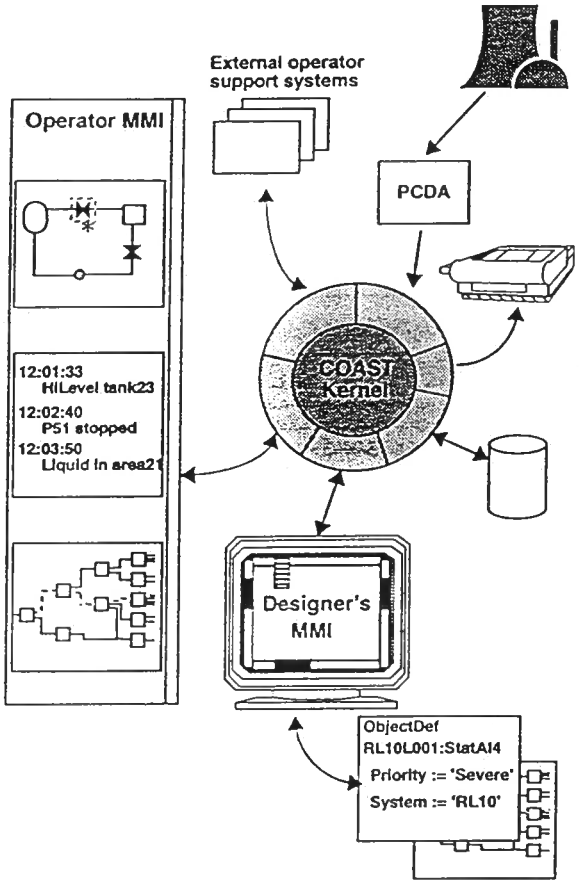


Fig. 2 The Computerised Alarm System Toolbox, COAST with interfaces to external systems

COAST is meant to be an add-on possibility to conventional process control systems. As shown in Fig. 2, it receives process measurements from the process computer

(PCDA - Process Control & Data Acquisition), updates all necessary statuses, and sends updated alarm information to the display system for the operators in the control room. COAST itself does not possess graphic capabilities, but will be easy to couple to different graphical systems. It has been coupled to the Picasso-3 user interface management system developed in Halden. Coupling to all external systems is done through an application programmer's interface, which includes simple functions to get data in and out of COAST, e.g., process data must be provided as input to the alarm objects.

The designer's MMI will be designed as an alarm editor, but it will also be possible to operate COAST through text-files.

COAST will be tested in a full scope training simulator in HAMMLAB. In this application the number of potential alarm signals is almost 5000, and Picasso-3 is used for graphical interfaces.

2.4 Diagnosis Systems

At the Halden Project prototypes of diagnostic systems have been developed to investigate their merits for NPP operation. DISKET is a rule-based expert system where information on patterns of the actual alarms and other process variables are matched with precalculated patterns from known disturbances to arrive at hypotheses for the cause of the alarms. The system was originally developed by JAERI (Japan) and further developed at Halden. DISKET has been validated in HAMMLAB, and the results show improved operator performance when the operators have access to DISKET during disturbances (9).

Detailed Diagnosis (DD) has been developed to perform diagnosis of alarms originating from the Early Fault Detection (EFD) system (chapter 2.1). The diagnosis is based on knowledge based techniques. Typically the results will be identification of failed components, control system failure or instrument malfunctions.

Currently the Halden Project is working on an Integrated Diagnosis System (IDS) aiming at utilisation of the experience from already developed diagnosis systems to make a general framework for diagnostic systems, incorporating important qualities of the previously developed systems. In this way, more robust systems will be obtainable due to the diversity in diagnostic methods and knowledge (10).

2.5 Core Surveillance Systems

The Core Surveillance System SCORPIO has been developed by the Halden Project to provide NPP reactor physicists and control room operators with a practical tool for improved on-line monitoring of core status and optimisation of control strategies for planned power changes. This is achieved through better surveillance of core instrumentation and application of powerful on-line core physics simulators (11).

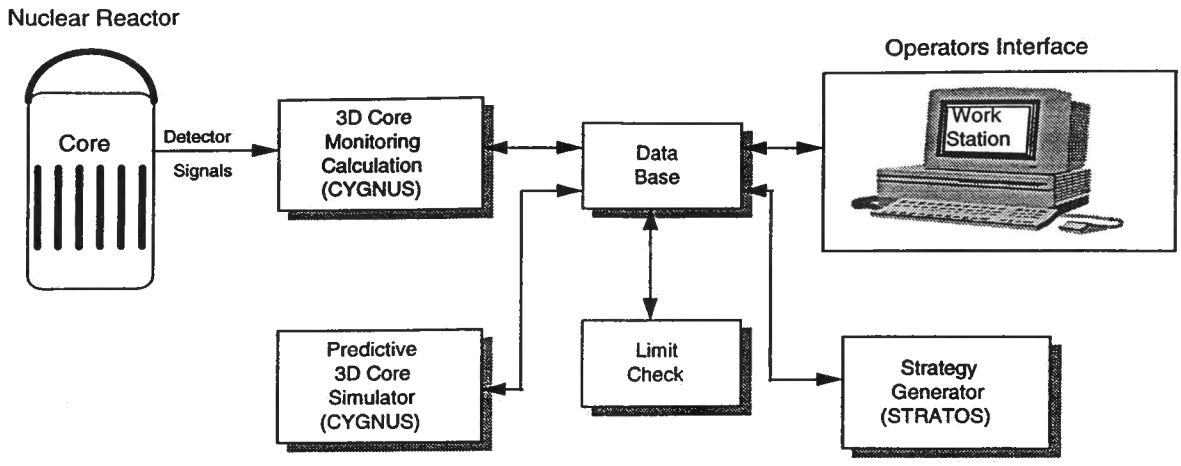


Fig. 3 Simplified block diagram of the SCORPIO system

The structure of the system is shown in Fig. 3. SCORPIO operates in two modes: monitoring mode, and predictive mode. In the Monitoring Mode, the system produces a realistic estimate of the core status based on instrument readings and calculations with CYGNUS, a 3-dimensional physics model including xenon dynamics. As soon as the core state data are available, the system checks and displays the margins to operating limits.

In the Predictive Mode, the system calculates the core behaviour during a planned power transient. This is of great help for reactor operation in dynamic core state situations where xenon variations often have a complex influence on power distribution.

Thus, the operator can avoid control strategies that are unacceptable due to operational constraints, by inspecting the predicted margins to these limits for different strategies.

Usually, a predictive calculation is made by simply specifying the planned power manoeuvre through drawing the power as a function of time using the mouse device, and then starting the strategy generator, STRATOS. When the strategy generator has been run, a 3D-calculation with CYGNUS is started using the controller settings provided by STRATOS as input.

The results of the predictive calculations can be viewed during the simulator run, on a picture showing margins to operational limits. More detailed information on the forecast can be visualised on demand as trend curves or spatial core distributions in a number of pictures.

During the last year SCORPIO has been delivered to Nuclear Electric, Sizewell B NPP in UK; Duke Power, McGuire and Catawba NPPs in USA; and Vattenfall, Ringhals 2 NPP in Sweden.

2.6 Computerised Procedure System

A number of observed and potential problems in the nuclear industry is related to the quality of operating procedures. Especially when it comes to Emergency Operating

Procedures (EOPs), much work has been done in recent years for improving their quality. This applies to most aspects related to procedure production, procedure structure and contents, procedure implementation and procedure maintenance.

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

COPMA-II is a computerised procedure system developed at the Halden Project (12). The system has two main components: *the procedure editor, PED-II*, is a tool designed to be used by the procedure writers during procedure preparation and procedure maintenance. Procedures to be used with COPMA-II must be expressed in a formal, general purpose procedure language, PROLA, developed by the Halden Project. *The COPMA-II On-line procedure following system* is the tool developed for supporting the process operators during retrieval and execution of procedures. The term *on-line* reflects that the system is designed to work with a live data communication link to the process computer, simulator, or any other external software component. Fig. 4 illustrates the relationship between PED-II, COPMA-II On-line and the plant computer or simulator.

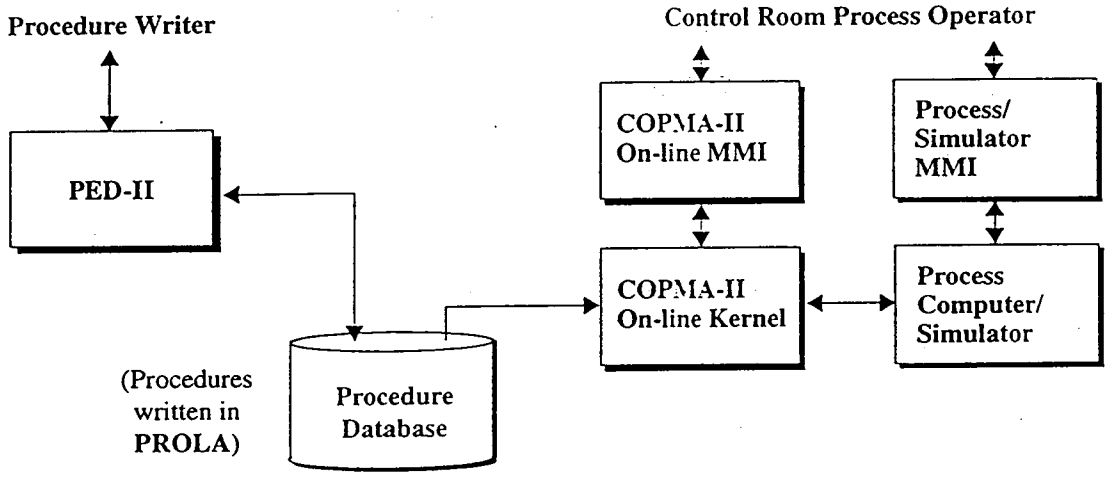


Fig. 4 COPMA-II block diagram

COPMA-II is intended to *replace* the traditional system of paper-based procedures. Existing hard-copy procedures must be transferred to COPMA-II by using the procedure editor. A more or less thorough rewriting of the procedure using the PROLA procedure language is necessary. There are *no* elements of automatic procedure generation or procedure synthesis during on-line operation.

COPMA-II acts as a *shell* for storing procedural information, for access and implementation by the operating crew. As designed, COPMA-II is not supposed to automate the actual execution of procedures. Normally, the operator drives the execution by acknowledging individual instructions within the procedure, making his personal

judgements as much as he did when using hard-copy procedures. COPMA-II may also, if permitted to do so, act as a partial control interface to the process, because certain actions specified in the procedures can be carried out directly through the COPMA-II On-line user interface. The integrated information available in COPMA-II combined with the support functions offered by the system, is intended to improve operator performance when implementing operating procedures compared to when doing the same job with paper procedures.

COPMA has been subjected to human factors evaluation experiments in HAMMLAB using Halden Reactor operators as test subjects and at the Scaled Pressurised Water Reactor Facility at North Carolina State University where 16 licensed NPP operators were test subjects. These studies have shown that operators can increase their performance and reduce their error rates when using COPMA, compared to using paper-based procedures.

2.7 Computerised Accident Management Support

The Halden Project is carrying out a research programme on computerised accident management support (the CAMS-project). The aim is to establish a prototype of a system which can provide support to the control room operators and the staff in the Technical Support Centre during accident situations. The CAMS prototype utilises available simulator codes and the capabilities of computer-based tools to assist in identification of plant state, prediction of future development of the accident, and planning of accident mitigation strategies (13).

The CAMS prototype will consist of a data base and a knowledge base, a tracking-mode simulator, a predictive simulator, a strategy generator and a man-machine interface system, see Fig. 5.

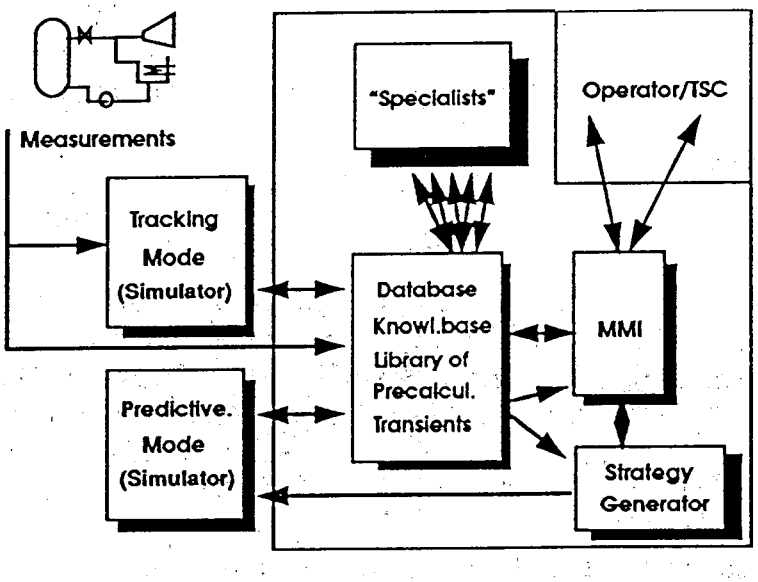


Fig. 5 Block diagram of the CAMS system

The block in the centre of Fig. 5 will have all possible data and knowledge of the plant and different subsystems of CAMS. It includes also a library of precalculated transients. It is exchanging information with all parts of CAMS.

The tracking-mode simulator will be used for signal validation and for state estimation. There are a lot of physical quantities that cannot be measured. If there is enough data available, they can still be calculated. The tracking-mode simulator is supposed to take care of that.

The predictive simulator will predict what will happen in the plant in the future. The future will depend not only of the present state, but also of the planned control actions. Many situations with different control actions can be tested, as well as the proposals from the strategy generator and from the users.

The strategy generator can give control proposals and accident mitigation strategies to operators, shift leaders and to the staff of the technical control centre. The strategy generator must of course contain knowledge about the plant, a model, you cannot propose a strategy without knowing the structure of the plant. The strategy generator shall solve an inverse problem (a question of the type "what shall I do to obtain that..."). Its job is more complicated than the job of the predictive simulator, which shall solve a direct problem (a question of the type "what will happen if..."). Therefore the plant model of the strategy generator has to be simpler than that of the predictive simulator. The strategies generated are therefore to be tested by the predictive simulator with its more detailed model. The predictive simulator can also test out man-made strategies before they are put into action.

The users will interact with the system through the man-machine interface. It is important that this module is as good as possible. Much work will be devoted to finding what information to display in different situations and how this information shall be represented.

A first version of the CAMS prototype is expected ready by the end of 1994.

3. Development Tools

3.1 User Interface Management Systems

User Interface Management Systems (UIMSs) are tools to realize graphic user interfaces (GUIs), i.e., presentation of dynamic process information and handling of operator dialogues. The Picasso system is a UIMS tool developed at the Halden Project which is used in development of the GUIs of most of the COSSs described in this paper.

The latest version, Picasso-3, supports object-oriented definitions of GUIs in a distributed computing environment. The system comprises an interactive graphic editor for drawing pictures, generating class libraries and dialogues, and a C++ inspired programming language for defining advanced picture dynamics (8).

4. Summary

The upgrading of NPP control rooms with introduction of new plant computers and digital I&C systems opens posibilities for assisting the operator through developing computer-based operator support systems (COSSs). At the Halden Project a number of such operator aids have been developed and evaluated through experiments in the HAlden Man-Machine LABoratory, HAMMLAB.

These evaluation studies as well as feedback from installations of COSSs in NPPs and other process industries have shown that benefits with respect to both plant safety and economy can be obtained through introducing COSSs in the control rooms, and development of such systems will therefore continue to be a major activity at the Halden Project in the years to come.

5. References

1. P. Visuri: *"Multivariable Alarm Handling and Display".*
A joint ANS, ENS and JAENS Meeting on Thermal Reactor Safety, Chicago, Illinois, 1982

2. E. C. Marshall, C.S. Reiersen, F. Øwre: *"Operator Performance with HALO-II Advanced Alarm System for Nuclear Power Plants - A Comparative Study".*
ANS Topical Meeting on Artificial Intelligence and Other Innovative Computer Applications in the Nuclear Industry, Snowbird, Utah, 1987

3. T.J. Bjørlo, Ø. Berg, R. E. Grini, M. Yokobayashi: *"Early Detection and Diagnosis of Disturbances in Nuclear Power Plants"*
ANS Topical Meeting on Artificial Intelligence and Other Innovative Computer Applications in the Nuclear Industry, Snowbird, Utah, 1987

4. H. Jokineva, M. Lilja, A. Sørenssen: *"Early Fault Detection in a Real Nuclear Power Plant by Simulation Methods"*
Paper presented at the ENC'90, Lyon, France, September 1990

5. E.C. Marshall, S.M. Baker, C.S. Reiersen, F. Øwre, P.J. Gaudio Jr.: *"The Experimental Evaluation of the Success Path Monitoring System".*
IEEE Fourth Conference on Human Factors and Power Plants, Monterey, June 1988

6. S. Nilsen, F. Øwre, C. B. O. Holmström: *"SAS-II. A Computerised Operator Support System Assisting in Plant Emergency Shutdown".*
NEA Specialist Meeting on Operator Aids for Severe Accident Management and Training, Halden, Norway, June 1993 (NEA/CSNI/R (93) 9)

7. A. Bye, S. Nilsen, F. Handelsby, T. Winsnes: *"COAST - Computerised Alarm System Toolbox"*

2nd IFAC Workshop on Computer Software Structures Integrating AI/KBS Systems in Process Control, Lund, Sweden, August 1994

8. K. A. Barmsnes, Ø. Jakobsen, T. Johnsen, H. O. Randem: *"Developing Graphics Applications in an Interactive Environment"*
1994 SCS Simulation Multiconference, San Diego, California, April 1994

9. C. B. O. Holmström, F. S. Volden, T. Endestad: *"Continued Experimental Evaluations of a Diagnostic Rule-based Expert System for the Nuclear Industry"*
ANP'92 International Conference on Design and Safety of Advanced Nuclear Power Plants, Tokyo, October 1992

10. R. E. Grini, T. Kårstad: *"Integration of Diagnosis Techniques"*
Meeting on Expert Systems and Computer Simulation in Energy Engineering, Erlangen, Germany, March 1992

11. T. Andersson, M. T. Cash, S. Hval: *"Evaluation of SCORPIO by Comparison to Catawba and Ringhals Data"*
ANS 1989 Winter Meeting, San Fransisco, November 1989

12. J. Teigen, E. Ness: *"Computerised Support in the Preparation, Implementation and Maintenance of Operating Procedures"*
2nd IFAC Workshop on Computer Software Structures Integrating AI/KBS Systems in Process Control, Lund, Sweden, August 1994

13. T. J. Bjørlo, A. Sørenssen, Ø. Berg, U. Scot Jørgensen, M. Sirola, F. Øwre, K. A. Ådlandsvik: *"Combining Simulation and Improved Presentation Techniques to Support Accident Management Decisions"*
ANS Topical Meeting on Nuclear Plant Instrumentation and Man-Machine Interface Technologies, Oak Ridge, Tennessee, April 1993

HALDEN PROJECT ACTIVITIES ON SOFTWARE DEPENDABILITY.

Gustav Dahll and Terje Sivertsen

OECD Halden Reactor Project

P.O. Box 173, N-1751 Halden, Norway

ABSTRACT

The increasing use of programmable equipment in nuclear power plants, even in safety critical applications, requires an emphasis on the problem of software dependability. The OECD Halden Project, which is an international research institute with member organisations from 15 countries, has worked in this field for more than 15 years, doing research projects together with other member organisations. This paper gives a summary of past and present activities, including the topics Formal development methods, Software diversity, Dynamic testing, Static analysis and Software reliability measures. The benefit the member organisations can have from working actively on this topic within the Halden Project is also emphasised.

1 Introduction

During the recent years there has been a trend to replace conventional electro-mechanical systems for the control of industrial plants with computer based systems. This also includes the use of computers in safety related tasks, e.g. in nuclear power plants and traffic control. There are many clear advantages of using programmable equipment in safety related systems in NPPs, compared to conventional equipment:

- It can provide more accurate trip criteria.
- It has automatic surveillance test capability.
- Calibration and functional testing during operation is simplified.
- The calibration drift is reduced.
- It is more reliable against hardware failures.

There has, in spite of this, been a certain reluctance to use programmable equipment in safety systems. A reason for this has been the complexity of safety assessment and the licensing of these systems, and in particular of the embedded software.

Since 1977 the OECD Halden Reactor Project (HRP) has been actively working in the field of software dependability. Particular emphasis has been placed on software in safety critical systems. The concept *software dependability* includes both safety and availability. However, in safety critical systems, safety should dominate over availability in the sense that if the two goals conflict then availability should be sacrificed in order to maintain safety. However, both safety and availability are closely correlated to the quality and reliability of the software.

There are three complementary principles which should be followed to obtain dependable software. The first principle in this respect is fault avoidance through good software engineering and quality assurance throughout the complete lifecycle of the software. The second principle is fault detection and removal through a thorough validation and

Paper presented at the Flins'94 International Workshop, Sept. 14 - 16, 1994 Mol, Belgium.

verification activity. A third principle, which should also be considered is fault tolerance, i.e. the system should be designed so that a single failure will not jeopardise safety. The Halden Project has made research activities on methods of relevance for all these principles.

Fault avoidance through good software engineering and quality assurance has been addressed through all our projects. A particular effort has, however, in the recent years been put on fault avoidance through the use of formal software development methods, which is discussed in section 5.

Faults inherent in the software should be detected and removed before it is put into operation in a safe system. The goal is to remove as many as possible, preferably all, such faults, and for that purpose it is necessary to develop good fault detection methods. Fault detection methods can conceptually be divided into two main types, viz. static analysis and dynamic testing, and both has been investigated at the Halden Project. In the SOSAT project a set of program tools for analysing safety critical software has been developed (see section 4), and in the STEM project various testing strategies were investigated (see section 2.5).

Fault tolerance can be obtained in different ways. One way is to design the system so that a potential failure has no effect, e.g. through redundancy. Another way is to bring the system into a safe state or a state of reduced risk, in case of a failure. One technique to obtain fault tolerance is through diversity, i.e. that the same function is simultaneously performed by several independent systems, and the result is decided by a voting system. The Halden Project has, through various projects, investigated possible benefits from using software diversity (see section 2).

Even if a system is made highly dependable, one must also be able to show this dependability to get acceptance from the authorities, and confidence with the public, in order to implement such a system in a safety critical system, in particular in the nuclear area. It is in this respect necessary to develop methods which can measure software reliability, and the Halden Project has investigated some such methods (see section 3).

The Halden Project is an international institution with participation from 15 countries. A main objective of the research activities is that the experiences and results from these activities can be utilised by member countries in real applications. One has therefore in the software dependability work put emphasis on close co-operation with member organisations, and many of the research projects were conducted as joint activities with other signatory institutions in UK, Finland, Germany, Japan and Sweden.

The Halden Project is also doing bilateral projects directly for member organisations. A guideline for reviewing and assessing safety critical software has been written for the Swedish Nuclear Power Inspectorate (SKI). It is also assisting SKI in using this guideline in their review of planned implementation of safety critical digital systems in Swedish NPPs.

2. Software Diversity

The PODS (Project On Diverse Software) project was a joint project between the Safety and Reliability Directorate (SRD), Central Electricity Research Laboratory (CERL), The

Tecnical Research Centre (VTT) of Finland and HRP. The main objective of the project was to provide a measure of the relative merits of using diverse programs, as compared with any one of the programs replicated in all channels, in a 2-out-of-3 majority voting protection system. To achieve the objective, an experiment was mounted which simulated a normal software development process to produce three diverse programs to the same requirement. The requirement was for a reactor over-power protection system. After careful independent development and testing the three programs were tested back-to-back against each other to locate residual faults. The three development teams were allowed to discuss problems with the requirement specifiers, but not with each other. All phases of the project were carefully documented for subsequent analysis.

2.1 Experimental Set-up

The structure of the experiment is summarised in fig. 1. The objective of this structure, which also included additional constraints, was to study the effect of diversity in the different program development stages.

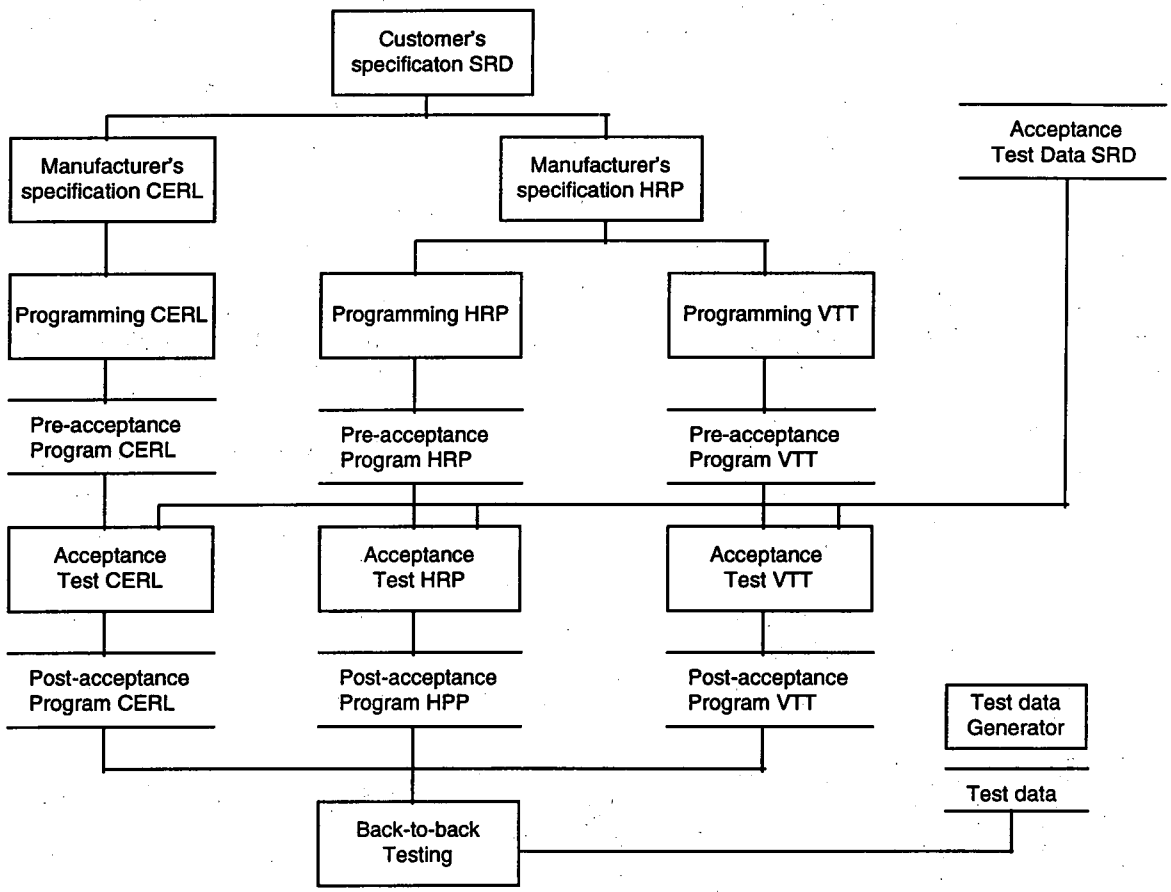


Fig. 1 Experimental set-up

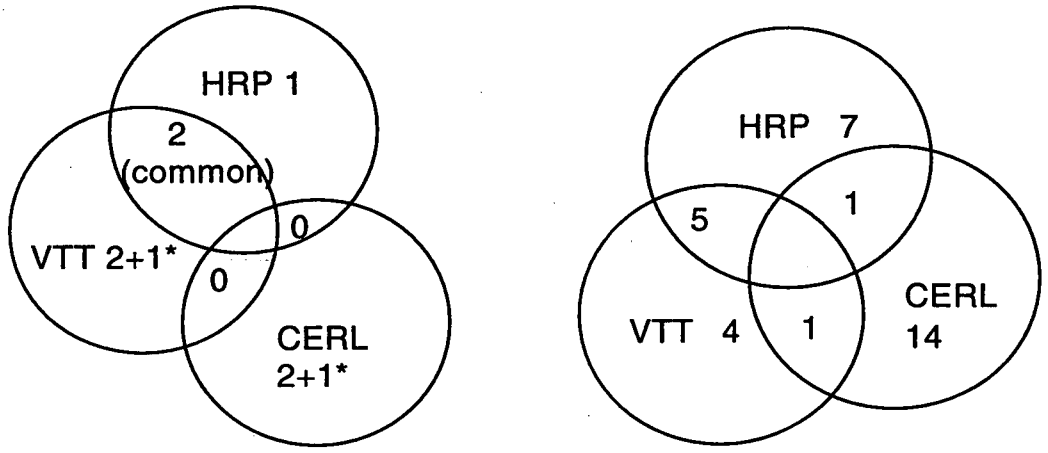
2.2 Back-to-back Testing

These three programs were tested back-to-back, i.e. they were executed simultaneously with the same set of test data and the results were compared. A test harness was developed for this purpose, as well as the test data generators and the systematic test data. The test data which were used as inputs to the trip functions were chosen according to

different strategies:

- Systematic data. 2472 sets of input data were produced manually to cover the various aspects of specification for the trip function
- Random data drawn from different distributions, including uniform and Gaussian distributions. Altogether the test data set consisted of 655288 test cases.
- Data simulating the actual data that are input to the trip algorithm from the plant in the real-life application.

The testing continued until a discrepancy between two or more programs occurred. This discrepancy was analysed and the correct answer was agreed. The program(s) was corrected accordingly, and the testing started from the beginning to check for faults induced during the correction. This procedure continued until the three programs agreed on all input data in the test data set. The back-to-back testing was performed both on the pre- and the post- acceptance test versions of the three programs. Fig. 2 shows the distribution of faults found in the three versions during the two back-to-back tests. These faults were all thoroughly documented for later analysis, and the assessment of the benefit of diversity is based on an analysis of this.



Post-acceptancetest programs
(Correction induced faults)*

Pre-acceptancetest programs

Fig 2. Distribution of faults in back-to-back testing

2.3 Reliability Enhancement Achieved by Diversity

One objective of this study was to assess the improvement in performance that was achieved by using a threefold redundant system.

With majority voting on individual outputs, good failure detection/correction was achieved when compared with the overall program failure rates. Failure detection rates in the pre-acceptance programs were greater than 99.7% except for some outputs which are known to be affected by specification-based common mode faults.

During execution of the post-acceptance programs, 100% of failures were detected by discrepancies between the three programs, i.e. there were no cases where all three programs agreed on the incorrect answer caused by distinct faults (possible common faults can of course not be found this way). The outputs on which the failures occurred

tended to be different so it was possible to vote out the incorrect result completely on 5 of the 7 affected outputs. The remaining two outputs are known to be affected by two common-mode faults in the post-acceptance programs. Similar results are not available for the pre-acceptance programs due to insufficient information from the test harness, but it is reason to believe that the failure correction performance is poor, largely because many different outputs were affected on the same cycle.

2.4 Failure Independence

One of the arguments put forward for software diversity is that the faults made in independent programs would be different and therefore the failures are likely to be uncorrelated. If this is true then the probability of two programs A and B failing simultaneously is:

$$P_{ab}=P_a*P_b$$

where P_a and P_b are the failure probabilities of A and B respectively, and P_{ab} is the coincident failure probability. Under this assumption relatively low reliability programs could be put together with voting logic to make a system with much higher reliability.

The following experiment was performed to test this independence hypothesis: Two programs were executed back-to-back with the complete uniform random data set. These programs were all combinations of the correct versions of the three programs, each seeded with one of the faults found during the second back-to-back test. The frequency of failures of each program (P_a and P_b) were measured, as well as the frequency of coincident failures (P_{ab}). All combinations of these faults were used, except those which caused a failure in every cycle, and therefore were uninteresting.

The results showed that there are four main populations of failures:
- Strongly positively correlated failures, mainly due to common faults.
- Relatively independent failures.
- Strongly negatively correlated failures.
- Fault combinations which caused an intermediate degree of dependency.

A potential cause of the latter is error masking. This can be explained in the following way: A binary output value is determined by a logical OR of several logical conditions. A failure to set one condition true can only be seen if all the other conditions in the OR gate are false. So the underlying individual and coincident failure rates should all be reduced by the same factor, viz. the probability that the rest of the OR gate inputs are false. The ratio between P_{ab}/P_a*P_b will therefore be increased by the same factor.

Strong negative correlation effect can also be explained by the masking effect of OR logic, e.g. when two faults fail to opposite values (0 and 1). These failures cannot be observed simultaneously through the OR logic, hence $P_{ab}=0$.

2.5 Test-data Efficiency

One objective of the project was to investigate the efficiency of the test data selection. The different strategies were compared, both with respect to fault finding capacity and to program coverage. All faults which were detected, and corrected, during earlier phases were seeded back into the programs. These were then tested with all data selection strategies (systematic, uniform random etc.).

To compare the fault finding capacity, the number of cycles to failures were measured for the different test data types for all faults. All the faults were revealed by at least one of the test data sets. However, not all faults were found by any single set of test data type. The percentage of not revealed faults for each of the different test data types are shown in table 1. As one can see, the uniform random data selection is very efficient, whereas the use of plant simulation data was not efficient to detect faults.

Table 1. Fault detection performance with different test data

Test data type	%faults not found
systematic data	14.0
systematic data	28.0
random data (Uniform)	4.6
random data (Uniform around boundaries)	13.0
random data (Gaussian)	28.0
random data (Gaussian around boundaries)	13.0
Plant simulation data	55.5

Branch and statement coverage tests were also done for each program, and the results from these also show that the random uniform is very efficient. This, together with the systematic tests reaches almost 100% coverage after around 500 test cycles. The plant simulation data, on the other side had bad coverage.

3. Software Reliability Measures

The data from the PODS/STEM project, as well as from a previous similar project, has been used to evaluate several models for software reliability measures.

3.1 Software Reliability Growth Models

Software reliability growth models are based on the assumption that the reliability of a program grows when a program is tested and discovered faults are corrected. The data from testing or actual operation on when failures occur are then used to compute the parameters in a failure probability function. The data in our case were the number of execution cycles before the programs failed. A variety of such models, using different parametrised distribution functions, were investigated. After each failure the distribution parameter was computed, the next time to failure was computed and estimated, and compared to the real time to next failure. Other types of comparisons were also applied.

The results from this analysis showed that no model represented an adequate fit to the failure data, and that the software reliability estimation differed substantially between the models. Some models gave better fits than other, but this is presumably only arbitrary, depending on the actual data. The problem is that these models require a large amount of failures during test and operation. This is seldom the case for safety critical software.

3.2 Reliability Estimation Based on Detection of Seeded and Real Faults

The number of faults remaining in a program after a certain amount of testing has been made can be estimated on the basis of an error seeding model. A set of artificial faults were seeded into the programs, and then the programs were tested until all the seeded

errors were revealed. When a fault (real or seeded) was revealed, it was corrected before the test continued. The estimation of remaining faults is based on the assumption that the ratio of unrevealed to revealed faults is the same for real and seeded faults.

The estimated and the real number of remaining faults were plotted against the number revealed faults in the test development. A general observation from these diagrams is that the number of remaining faults are clearly underestimated in the beginning, but as the number of faults found are getting larger, the difference starts to oscillate and approach zero. The estimation was found to be quite good when more than half of the seeded faults have been found. The fact that the number of remaining faults seems to be underestimated, particularly in the early phases of the testing, is due to the fact that more artificial than real faults were revealed in the first test cycle. This is because the most obvious real faults were removed during inspection and local testing.

3.3 Complexity Measures

The objective of complexity metrics is to measure the complexity of software modules and programs. If a good correlation between the complexity metric and the number of faults could be established, then the metric could be used as a software reliability measure. There are many different complexity measures, but none of them are generally accepted to be superior to others. To investigate this a set of known software measures (Halstead, McCabe etc.) were correlated with the number of faults in program modules of three test programs.

There was a positive correlation between the complexity metrics and the number of faults in the modules. This correlation can, however, mainly be attributed to the correlation between the size of a module and the other metrics. The relative correlation coefficients, where this effect was removed, showed little correlation. Some of the metrics showed better correlation than others, but not significant. This difference is probably arbitrary.

The reasons for the poor correlation in this experiment may be
- statistical significance of the results is poor due to small error counts
- complexity of the code does not tell enough about the software and its development.
- human perception is not taken into account in the complexity metrics.
- data complexity is not considered.

One should therefore be careful not to draw too firm conclusions on software complexity metrics from this experiment.

4. Static Analysis Tools

The SOSAT (SOftware Safety Tools) project is a joint project between HRP, Technische Überwachungsverein Nord (TüV) and Gesellschaft fur Reaktorsicherheit (GRS). The objective of the project is to develop tools which can assist in the safety analysis of computer programs. Manual routine work is partly automated. This reduces the amount of desk analysis of the programs, and thereby the cost and time to perform it. The reliability of the safety assessment is improved, and the possibility to reproduce the safety analysis is facilitated.

The verification process with the SOSAT tools is based on a memory dump of the host

computer, i.e. the computer where the analysed program is implemented. One reason for basing the analysis on the machine code representation of the program is to reveal potential faults introduced through the compiler and other programming aids. A disassembler extracts the part of the memory content which constitutes the program(s). That part is translated into a processor independent language, CAL, specially designed to facilitate program analysis. CAL is the basis for the further analysis. Disassemblers have till now been made for several Intel and Motorola processors.

The program is divided into routines, and the calling hierarchy between the routines are found. A set of basic information about each routine is produced, as e.g. number of instructions, number of forward and backward jumps, maximum nesting level etc. This information is useful to get an impression of the complexity of the routines, and of the further work needed to perform a safety assessment. It can also be used to detect possible defects in the program, as e.g. code sharing and dead loops.

The further analysis is a decomposition of the routines into units at different levels. There are three types of units: linear pieces of code, single-entry-single-exits, and loops. This decomposition of the program into units on different hierarchical levels, and the connection between these, constitutes the basic results from the control flow analysis.

A path through a program is a possible sequence of statements from start to end. The analyser can identify all paths through a routine and write them in a very compact form. Path information is very useful in the dataflow analysis and the real-time analysis, and also as a basis for test measurements.

The main idea with dataflow analysis is to trace variables forward and backward in the program. One will in this way check that all variables are defined correctly before they are used, and show the influence the variables have on each other. The results from the control flow analysis, in particular the path analysis, are very useful in this respect.

A program which performs symbolic execution of linear pieces of code aids the analysis of the data flow in a program. The variables which are changed in a piece of code are expressed in terms of the value of variables at the entry of the code. This may abbreviate a fairly long piece of code substantially.

5. Formal Development Methods

The Halden Reactor Project has for a number of years been involved in the evaluation and development of formal software development methods. These are methods which provide a mathematically based framework within which specification, development and verification of software systems can be done in a systematic and precise way. The main idea in formal software development is to use mathematical techniques to describe properties of the desired system and proofs to verify the design steps from this description. Formal methods provide an efficient way of developing a system and its proof hand-in-hand, with the proof leading the way. This gives more reliable systems giving their designers and customers more confidence than they otherwise would have.

The use of formal specification and design makes it possible to discover many errors which might otherwise very easily be overlooked. Even if a formal specification may be difficult to understand, its meaning is not ambiguous, i.e. the semantics is well-defined.

Once formally captured, the formal specification gives a precise description of the system to be developed. The final product should be in accordance with this specification, and to achieve this, various methods have been proposed to move from the formal specification to the finished product. The use of these methods disciplines the developer to make a specification clearly express what the customer wants.

This concept of correctness is however not sufficient to ensure that the resulting software system correctly reflects the customer's original requirements. Even if the formalization of these requirements provides a precise and unambiguous description, the correctness of this formalization remains to be demonstrated. One way to achieve this is to make use of executable specifications, which allow validation (by a process called animation) in an early phase of the development project. As a consequence, the software may be made more reliable, while the costs and time needed to develop the software may be reduced. Animation also enhances experimentation of the requirements, a property which may be useful in projects where the requirements can not initially be stated in a complete and precise way. One of the most attractive features of executable specifications is the means they provide for communication between the developer and the customer. Typically, neither the customer nor the users of a quoted system are able to read formal specifications. Animation may therefore be an excellent means for elucidating the specification. Executable specifications may be particularly attractive when combined with an transformational approach. By means of transformations, the specification can gradually be designed into an implementation, while the correctness of the design steps can be proved within the same framework. As long as two design steps are written in the same notation, the intended relationship between them can be expressed by means of so-called abstraction functions.

Even if animation is useful, it has the same limitations as traditional program testing, in that only a small number of walk-throughs are conducted, and serious errors may easily be overlooked. This limitation is especially unsatisfactory when validating the specification of safety critical software. Fortunately, this shortcoming of animation can to a large extent be met by formal proofs of properties of the specification. When modelling the state of a system there are often some intended relationships between the state variables. An important part of the specification of the system, is to make these relationships explicit and prove that they are maintained by the functions modifying the system state. One important class of properties are so-called safety invariants, which are specifically defined to ensure certain safety conditions hold true. Given the requirements to the system, the safety invariants are expressed in the notation used in the formal specification of the system. The verification of these invariants constitutes an important part of the analysis/validation of the specification.

5.1 Algebraic Specification

Following the principles behind formal software development, the Halden Project has developed a methodology based on algebraic specification and a proof tool, the ***HRP Prover***. One of the virtues of this methodology is that the same language, tool and proof techniques can be used both in specification and design, even down to a "concrete" specification which can be automatically translated into code. In the specification phase, the theorem prover is used to verify and validate the specification, while in the design phase the same tool is used to verify the correctness of the design steps. The final

implementation can be performed by an automatic translator, tailor-made for the specific implementation language. All together, this gives a framework which not only makes it feasible to develop highly reliable software, but which also allows for substantial reductions in the development costs. A guiding principle in the development of the method has been to try remove some of the obstacles that make the use of formal methods difficult. This is reflected both in the implementation in the specification language, in the tool support, and in the principles of the method. In spite of these simplifications, the tool support has been made sophisticated enough to allow a smooth use of the method. This involves automation of animation, proofs of correctness of specifications, and proofs of correctness of design steps.

An algebraic specification of a data type is a representation-independent formal definition of each function (operation) of a data type. The purpose of such a specification is to capture the requirements to this data type, without otherwise putting restrictions to the possible implementations. Algebraic specifications have proved to be a powerful tool for writing hierarchical, modular, and implementation-independent specifications. Because the specifications are based on interpreting the equational axioms as rewrite rules, they have also proved to form an appropriate basis for rapid prototyping and environments for verification and validation. One important motivation for using abstract data types is that the object types natural to the problem domain usually are not available as primitive types in the implementation language. A model of the systems behaviour in terms of these primitive types can therefore not possibly be optimal, in terms of efficiency. Data abstraction makes it possible to specify data types reflecting the natural object types, and to use these types in modelling the system behaviour. Algebraic specification is a language for specifying such data types. A formal software development method based on algebraic specification purposes to support the design of an efficient computer program from this model.

The extensive use of a "mathematical tool-kit" of predefined data types makes it possible to specify a software system in a very concise way. In the design and implementation of the specification we can utilize exisiting designs and implementations of these data types and thereby gain several benefits:

Cost-effectiveness: Types and functions specified in the mathematical tool-kit need not be designed and implemented over again. As a consequence, the use of the tool-kit not only gives more concise specifications; it also reduces the effort which must be invested in design and implementation.

Reliability: The functionality of the mathematical tool-kit can be understood separately from its context, and corresponds to familiar mathematical concepts. This increases comprehensibility and reduces the risk of writing an erroneous specification. Furthermore, the mathematical tool-kit has already been designed and implemented, and the correctness of this implementation removes the source of errors that would otherwise be involved in the design and implementation of the corresponding parts of the specification.

Modularity: The implementation of the mathematical tool-kit can be used as a library of related types and functions which can be understood separately from its context.

5.2 The SAP Project

The Halden Project's activities on the evaluation of formal methods started with the Safety Assessment of Programs (SAP) Project, in co-operation with SRD and CERL. A subtask of this project addressed techniques and methods to ensure that safety critical software is developed and assessed in a safe manner. One of the objectives was to gain practical insight into formal software development, and to assess its performance compared with conventional approaches. The investigations focused on the Def-Stan-0055 standard for procurement of safety critical software. According to this standard, formal development should include a mathematically formal specification and specification validation. Further a rigourous development of software in a syntactically and semantically well-defined high-level language is required, with verification during development using static analysis tools. The investigations included the complete development of a small software system in accordance to the proposed standard.

Phase 1 of the SAP project demonstrated that tool support is essential during any formal development. It was therefore decided to establish and maintain a document which could assist in the choice of methods and tools applicable to formal software development. It was also decided to initiate a second phase of the SAP project concentrating on the evaluation of different approaches to formal development with respect to applicability and implications on safety and reliability. Three different methods (Z, Larch, and CSP) were evaluated using a suitable small but realistic case example. This approach enabled a comparison of the different methods in order to provide advice on the advantages and drawbacks of the different methods and approaches. All the methods evaluated appear to be useful for specification and verification of process-oriented systems, even if the parts of the systems which can be adequately described may be too limited for many applications. Nevertheless, the fact that proofs of important safety properties can be carried out suggests that the methods evaluated have relevance in this context. The selection between them must be guided by the characteristics of the target system and its behaviour which are of particular interest.

5.3 The EvalFM Project

The EvalFM (Evaluation of Formal Methods) project was established in order to investigate the applicability of formal methods in the development of safety-critical software based systems. In particular, the EvalFM project has focused on the evaluation of the formal software development method based on algebraic specification and the HRP Prover. This method has been used in a case study on the applicability of formal methods in the development of a protection system for a nuclear power plant. The example is based on the computer-based power range monitoring (PRM) system installed at Barseback NPP in Sweden. The purpose of the PRM system which is of particular interest in this project is the monitoring of the average power emission of the core, the average PRM (APRM) value. When high power emission is monitored, the system must trip the high level alarms.

The method has been used to formally specify and design one out of four similar subsystems of the PRM system. Based on the requirements document, a formal algebraic specification has been written, utilizing the mathematical tool-kit defined in /HWR-331/. Using the design and implementation techniques discussed in /HWR-363/, the subsystem has been designed and implemented in a safe subset of Pascal. The project has also

investigated how the design can be varied to allow implementation in other languages and to put stronger emphasis on efficiency. Finally, the project has investigated the applicability of algebraic specification for aspects relating to timing, communication and diversity. The overall purpose of these investigations has been to contribute to an understanding of the role and applicability of formal methods for these and other aspects of relevance to V&V.

When writing a formal specification based on a requirements specification like the one given for the PRM system, it is important to ensure that any implementation satisfying the formal specification must also satisfy the requirements specification. Fortunately, the formal development of the implementation from the formal specification makes it possible to demonstrate *a priori* that the implementation satisfies the formal specification. The concern about the satisfaction of the requirements specification therefore reduces to a validation of the formal specification against the requirements specification.

It is expected that the investigations in the EvalFM project will contribute to a clarification of the role and limitations of formal methods when applied on the development of safety-critical software systems. In particular, licensing authorities want to see representative applications of existing formal methods to make decisions on whether the use of formal methods should be required, which formal methods should be used and what is the appropriate way to use them, and what to require to be formally verified. For the development of such guidelines the licensing authorities are not primarily interested in the development of new methods but in the application of existing methods.

6. Concluding Remarks

A main objective of the Halden Project is to act as a focal point for research on topic of interest for the nuclear power society in the member countries. This includes vendors, power companies, licensing organisations and research institutes. The conclusions and recommendations from the research projects constitute information which is useful to these organisations. In this respect a topical report on lessons learned from all software dependability work at Halden has been made, with emphasis on conclusions and recommendations. Tools which are developed within the Project are freely available also to members which have not directly participated in the development. However, the best way to utilise the results from the Halden Project is to actively participate in joint projects and utilise the results, as e.g TüV, which is a licensing advisor, uses the SOSAT tools in their assessment of safety critical and safety relevant software, and AEA/SRD has benefited from the work on software diversity.

References.

HWR-331:T. Sivertsen, "Algebraic Specification Used in Formal Software Development Part 1: Specification". Halden Work Report 331, Nov. 1992

HWR-363: T. Sivertsen, "Algebraic Specification Used in Formal Software Development Part 2: Design and Implementation",Halden Work Report 331, Aug. 1993.

RETROFITTING OF NPP COMPUTER SYSTEMS

Geir Pettersen
OECD Halden Reactor Project
P.O. Box 173
N-1751 Halden, Norway
Phone: 47 69 183100
Fax: 47 69 183103
E-mail: Geir.Pettersen@hrp.no

ABSTRACT

Retrofitting of nuclear power plant control rooms is a continuing process for most utilities. This involves introducing and/or extending computer-based solutions for surveillance and control as well as improving the human-computer interface. The paper describes typical requirements when retrofitting NPP process computer systems, and focuses on the activities of Institutt for energiteknikk, OECD Halden Reactor project with respect to such retrofitting, using examples from actual delivery projects. In particular, a project carried out for Forsmarksverket in Sweden comprising upgrade of the operator system in the control rooms of units 1 and 2 is described. Possible multi-stage upgrade paths for the process computer system are also described. As many of the problems of retrofitting NPP process computer systems are similar to such work in other kinds of process industries, an examples from a non-nuclear application area is also given.

1. Introduction

As industrial plants get older, it will often be required to replace certain kinds of equipment, or install new equipment to be able to continue to run the plant in a secure and efficient manner, or even improve operation with respect to safety, quality and economy. Modern technology typically offers more powerful solutions than what is supported by the equipment originally installed. In particular, the rapid technological evolution in the computer area has lead to powerful and flexible computers being available at a reasonable low cost. These are important factors when discussing how the process computer system of Nuclear Power Plants can be upgraded or retrofitted.

The degree of computerization varies a lot between different NPPs, from the oldest ones being fully based on conventional instrumentation and control, to the most modern plants which can be fully digitalized using computer-based solutions for all kinds of I&C. This diversity in the current situation leads to challenges and specific requirements for the retrofitting process, as the new equipment must typically be interfaced to and work with more or less of the old equipment that are not changed during the upgrade. In some situations it may also be required that the new equipment can be installed while the old equipment are still in operation, and even work in parallel with the old equipment for a certain period.

2. Main requirements in NPP Process Computer System Upgrade

For most utilities it is of vital importance to have the highest possible figures for plant availability and thus reduce the shutdown periods as much as possible. This implies that changes of all or parts of the process computer system must either be performed during short time frames in an already tight shutdown period, or the upgrade must be performed by introducing new equipment in parallel with the old equipment and thus providing a smooth change during normal operation.

Another important issue is that the new equipment must be possible to connect to and communicate with existing equipment on the plant. This means e.g. that it must be possible for the new process computer system to use existing signals, or more or less of the total data acquisition system. Another example is that it must still be possible for higher-level administrative related systems to communicate with the new process computer system to extract e.g. production data.

Using standard communication methods for inter-system communication helps solving communication problems in multi-vendor environments. Common interface packages (APIs) implemented on the various process-related computers in the total process computer structure make it possible to standardize data transfer between various subsystems to a high extent. This is possible independent of the underlying hardware and operating system on the process computers involved, as long as they comply to basic standards with respect to communication capabilities, e.g. TCP/IP, OSI etc.

To have a unified control room, it is also important that the operator system part of the process computer system is implemented in compliance with utility guidelines with respect to the man-machine interface. As the control rooms often contain several individual systems, standardizing use of colours, symbols, operation sequences etc. between the different systems is important to secure correct operator actions, in particular in abnormal plant operation situations. Introducing new systems will also require a certain degree of operator training. If the new system follows established guidelines and standards well-known to the operators, the required amount of training can be reduced.

As process computer systems are often important in daily plant operation, it is important to have the highest possible (and reasonable) availability figures for these systems. This means that time required for maintenance should be as little as possible, and that it should be easy to exchange parts of the system in case of system failure. This brings forward the need for a reliable, modular system. Modularity is also important when discussing the possibilities for future extensions of the system.

To summarize, the following requirements must be considered as mandatory when performing a process computer system upgrade:

1) short installation time, possibilities for parallel operation
2) interconnection possibilities to other systems
3) standard communication capabilities
4) operator interface standardization
5) easy maintenance and extensibility

3. Multi-stage NPP Process Computer System Upgrades

Process computer system upgrades can be performed as a multi-stage operation, in which the different system modules are upgraded individually and in sequence. This will often be interesting in order to comply with the first requirement described above. To reduce the need for a longer shut-down period in order to perform a total upgrade of the process computer system can give major advantages with respect to plant operational availability. However, to perform such a multi-stage upgrade requires detailed planning and proper definition of all interfaces.

Open systems are getting wide-spread and popular in the computer industry. It is therefore interesting to bring attention to such systems also when retrofitting NPP process computer systems. Using standard hardware and software based on common, international standards as basic building blocks in the process computer system makes the utility less dependent on specific vendors, and makes it possible to integrate the best products from different vendors to form the desired total system. It will also be easier to perform the installation in several phases, as the inter-system interfaces will be based on common standards. This functionality is in direct compliance with both the second, third and fifth requirement described above.

As flexibility is a typical property of modern open systems, it will often be possible to configure these systems in a way making them fit smoothly into the rest of the control room and process control area. If proper actions are performed, also the fourth requirement can be fulfilled.

A multi-stage upgrade path for the process computer system can thus satisfy the main requirements described in the previous section. Such a philosophy will often prove being a good solution, both with respect to technical issues and total life-cycle costs.

4. Forsmark Operator System Upgrade

4.1. General

As an example of how a NPP process computer system upgrade can be performed, taking advantage of modern technology, common industrial standards etc., and providing a basis for step-wise continuation of the upgrading process, a project performed by Institutt for energiteknikk (IFE), OECD Halden Reactor Project, will be described.

4.2. Description of original system

Forsmarksverket is one of Sweden's four NPPs, and consists of three units, all BWRs. Unit 1 and 2 (F1 and F2) are identical, and were delivered by ASEA-ATOM and put into operation in 1980 and 1981. The control rooms of these units are based on a combination of conventional panel/desk instrumentation and computer screens. However, control actions towards the plant are only performed through conventional instrumentation.

The original process computer system consisted of a DS-8 data acquisition system connected to three Norsk Data ND-100 16-bits minicomputers, one taking care of analogue data processing, one taking care of digital signals and one being the main plant computer. Four low-resolution semigraphic operator stations with keyboards were connected to the main plant computer.

All displays were implemented as conventionally coded program segments, and it was difficult to add new displays and functions to the system. The displays mainly consisted of group displays with bargraphs and trend curves, detail displays showing all parameters, e.g. measuring range, alarm limits, filter constant etc. for a variable, alarm and event lists, in addition to some special-purpose displays, e.g. for detector calibration, core follow result presentation, showing operational point in a power/cooling flow diagram etc. No process mimic diagrams were available for the operators in the original system.

The original system configuration is shown in figure 1.

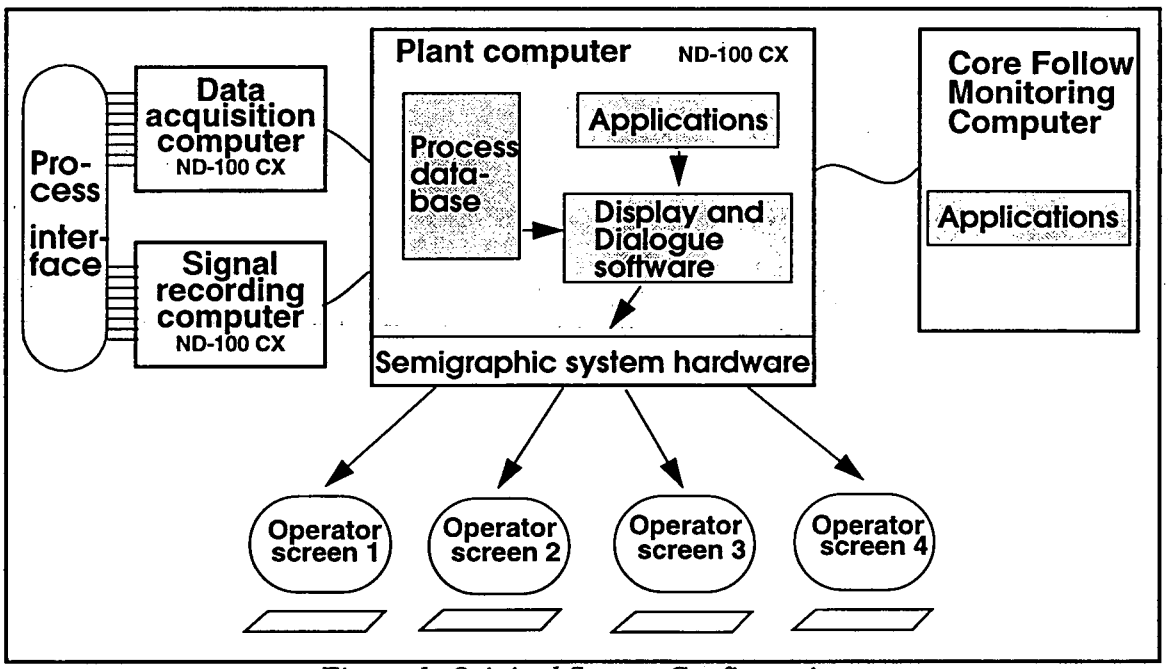


Figure 1 Original System Configuration

4.3. Requirements for new system

This system did not fulfil the requirements of a modern operator interface with respect to display content, colours, resolution etc. Hardware maintenance of the operator system was also getting difficult and expensive due to lack of spare parts and service engineers for such an old system. It was thus in 1989 decided to perform a retrofitting of the process computer system involving upgrading the central ND minicomputers and installing high-resolution colour graphic screens for the operator interface.

A working group at Forsmarksverket was established and developed the following basic requirements for the new operator system:

- Each operator station should be based on stand-alone hardware and should be able to communicate with at least 5 separate plant computers using Ethernet and the TCP/IP protocol.
- The operator stations should have a 19" colour graphic VDU with more than 16 different colours and a minimum resolution of 640*480 pixels.
- Input devices should be a standard alphanumeric keyboard, a function keyboard with about 30 keys, and mouse or trackball.
- A colour hardcopy printer common to a group of 4 operator stations should be connected.
- The operator system should be able to handle at least 100 different graphic displays. It should be possible to have at least 25 analogue values and 25 indicators in one picture, all dynamically updated.
- The system should be able to handle 1600 digital values and 900 analogue values that are updated on a cyclic basis. 50% contingency should be added to these figures.
- Display times should be less than 2 seconds for static part, less than 3 seconds for a picture with about 15 dynamic values and less than 5 seconds for a display with historical trend curves.
- Complete system start-up time should be less than 5 minutes.
- It should be possible to use the existing operator system in parallel with the new system in a transitional phase.
- It should be possible to realise the existing operator interface look and feel.
- Window capabilities should be available.
- It should be possible for the customer to develop the displays and dialogues without restrictions of using fixed format layouts. Future expansions should be possible.

After an evaluation of the offers from several possible vendors, IFE was chosen for the retrofitting project. IFE has been working with development of computer-based solutions for control room applications for twenty-five years and has substantial experience in different process control related fields such as user interfaces, support systems, computer technology etc. This basic knowledge, together with the ability to configure and integrate a system matching Forsmarkverket's requirements were important issues in the vendor selection phase.

4.4. Description of new system

The new operator system installed in each of the F1 and F2 control rooms consists of four Hewlett-Packard 340 workstations with 19" colour CRTs with a resolution of 1024x768 pixels. Each workstation has 16 Mb primary memory and two of the stations are equipped with a 323 Mb SCSI disk.The operator input devices are a standard workstation keyboard, a 32 button function keyboard and a track ball. The workstations are standard configuration equipment and are running the HP-UX operating system. This configuration is shown in figure 2.

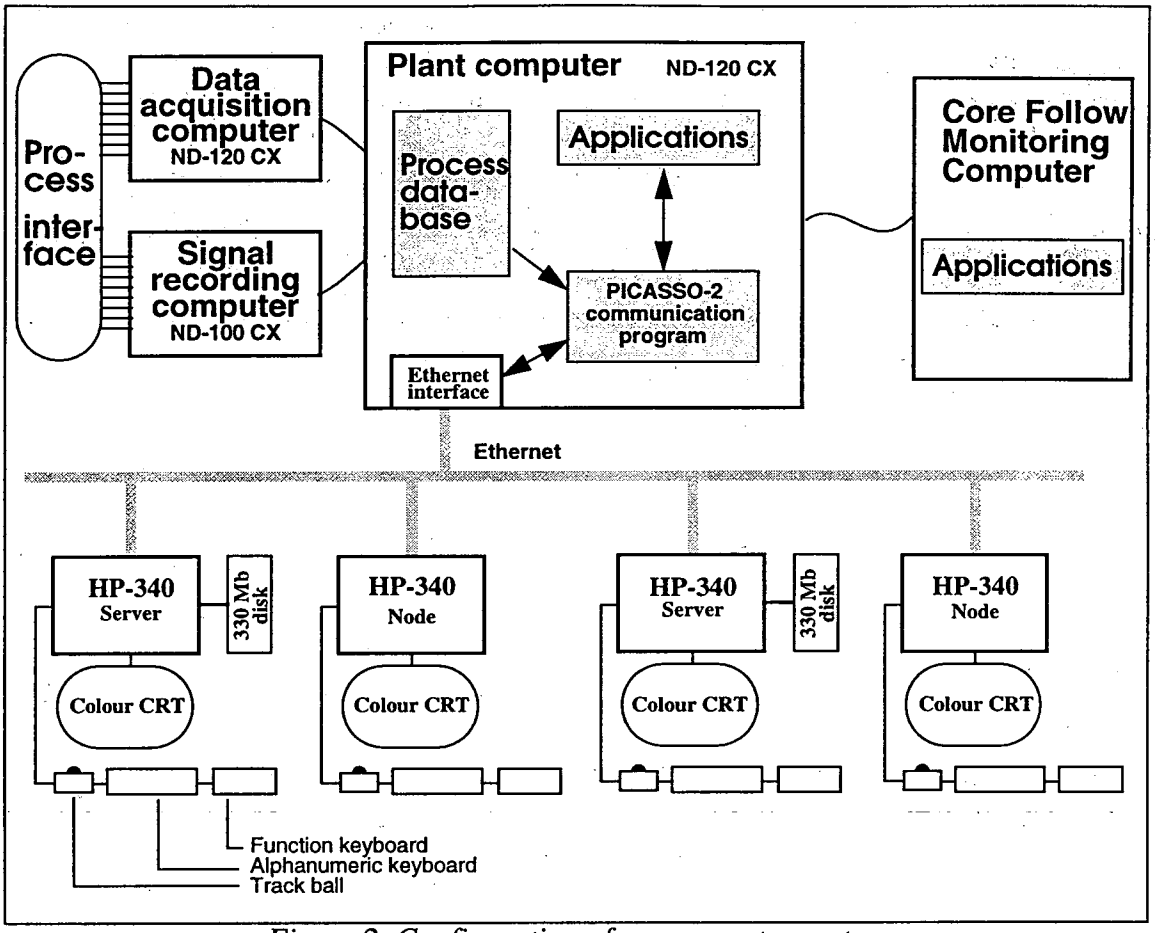


Figure 2 Configuration of new operator system

The operator interface is implemented using the PICASSO-2 User Interface Management System (UIMS), which has been developed by OECD Halden Reactor Project during the last seven years. This system is designed using the criteria of handling the Man-Machine Interaction for an application separated from the application itself. PICASSO-2 has been developed with special focus on the requirements set by process control applications to a UIMS.

The workstations running the PICASSO-2 system communicate with the main plant computer on Ethernet, using standard TCP/IP and Berkeley Sockets interface. Data traffic is mainly transfer of current states of analogue and digital process variables to be mirrored into the internal database of the PICASSO-2 system for display on the operator screens or for logging and trending.

To reduce the requirements for extensive operator training, it was considered important that the main user interface guidelines for the old operator system should be maintained in the first version of the new system. However, new functionality, e.g. windowing, supported by the new technology was utilized to a certain degree.

The system was installed into the control rooms of units 1 and 2 early 1991, and was well received by the operators. After installation, the system has been upgraded with new displays etc. which have been developed by or in close cooperation with the operators themselves.

The modularity of the system, with four independent workstations and a main plant computer communicating across standard interfaces, makes it possible to continue the upgrading process. This can e.g. be a change of the main plant computer, further upgrades to more powerful workstations in the operator system, adding more operator stations etc.

5. Non-nuclear Process Computer System Upgrades

Many of the same issues important for NPP process computer system upgrades also applies to similar upgrades in other industry areas. IFE has together with the Norwegian company Kongsberg Offshore a.s performed a similar task on a monitoring system for the PEMEX oil company in Mexico. This project was a replacement of an earlier system with graphic terminals and minicomputers.

The new system, which was installed in 1993, is based on a dual ND120/CX minicomputer system and a number of operator stations implemented on 386/486 based PC's running SCO UNIX. The operator interface is implemented using the PICASSO-2 UIMS system. Additional modules were developed for communication, alarm handling, reporting etc. The operator stations are installed both locally connected to a LAN, and also on remote locations using serial modem lines for communication with the central process computer and data acquisition subsystem.

Da Ruan

Da Ruan gained a BSc degree in Applied Mathematics from Fudan University, Shanghai, in 1983, a Certificate in Management from the Katholieke Universiteit of Leuven, Belgium, in 1990, and a PhD degree in Mathematics from the Rijksuniversiteit Gent, Belgium, in 1990. He was a teaching research assistant at Fudan University in 1983–86, a PhD researcher at the Rijksuniversiteit Gent in 1987–90, a researcher at SCK•CEN in 1991–93, and since 1994, a postdoctoral researcher at SCK•CEN and the project leader of FLINS (Fuzzy Logic and Intelligent Technologies in Nuclear Science) at SCK•CEN. His interests and scientific expertise include computational methods, numerical algorithms, simulation modelling, artificial intelligence, fuzzy logic and its applications, and applied mathematics.

He is the author of numerous professional publications, including "A Critical Study of Widely Used Fuzzy Implication Operators and their Influence on the Inference Rules in Fuzzy Expert Systems" (1990), "Fuzzy Logic in Approximate Reasoning" (1991), "Fuzzy Sets and Decision Theory" (1992), "Decision Making in Nuclear Science" and "Fuzzy Systems in Nuclear Applications" (1993), and "Basic Concepts in Nuclear Research—Core Activities at the Belgian Nuclear Research Centre" and "Fuzzy Logic and Intelligent Technologies in Nuclear Science" (1994).

Dr Ruan is a member of the International Fuzzy Systems Association and the chair of FLINS in Belgium. He was selected to appear in *Five Hundred Leaders on Influence* (honoring achievements during the last quarter of the twentieth century) by the American Biographical Institute in 1994 and in *International Who's Who of Intellectuals, 11th Edition* by the International Biographical Centre, Cambridge, England, in 1994. He is currently leading the new international forum FLINS, linking industrials and academics for international projects of common interest.

Authors' biographies

Marc Vankeerberghen

Marc Vankeerberghen obtained his engineering degree from the Katholieke Universiteit of Leuven in 1983. After some postgraduate research at the University of the Witwatersrand (South-Africa), he worked in the research departments of large South-African corporations (Boart International, Atlas Aircraft, and De Beers). In the meantime, he obtained a postgraduate degree in control engineering and was trained in middle management. The main thread throughout his career has been the modelling of equipment and processes. He joined SCK•CEN in 1993 and is involved with nuclear plant decommissioning. He will be seconded to the Halden Reactor Project as from January 1995.

Frans Moons

Frans Moons obtained his electromechanical engineering degree from the Katholieke Universiteit of Leuven in 1973. He held the position of project engineer at SCK•CEN, designing rigs for fuel and materials study at the BR2 materials testing reactor and evaluating irradiation results. He was seconded to the design team of the Next European Torus (thermonuclear fusion) at Garching near Munich, Germany, for the period 1983–89. Since 1989, he has been the senior scientist working on candidate materials for next fusion machines, the coordinator of the thermonuclear fusion programme at SCK•CEN, the scientific secretary to the scientific advisory board, and a member of the Halden Project Programme Group (vice-president in 1994).

Fridtjov Øwre

Fridtjov Øwre obtained a MSc in Physics, department of Cybernetics, from the University of Oslo, Norway, in 1975. His main study focused on the registration, transformation, and presentation of signals propagating in *real* neural networks (shrimps).

In 1975, he joined the Institutt for Energiteknikk, Halden, Norway (OECD Halden Reactor Project). He has a wide experience in the application of computers to real-time processing, in computerized operator support as well as in topics related to human factors engineering. His main interest has been the development of new and efficient computerized alarm systems.

Presently, he is deputy project manager at the OECD Halden Reactor Project with the overall responsibility for the man-machine system research activities and the coordination of the bilateral contract work at the Project.

Mr Øwre is the author of many reports and papers within the above-mentioned research topics.

Thorbjørn J. Bjørlo

Thorbjørn J. Bjørlo obtained a MSc in Engineering Physics from the Norwegian Institute of Technology (NTH), Trondheim, Norway, in 1964 and a MSc & DIC in Control Engineering from the Imperial College of Science and Technology, London, UK, in 1969.

In 1964–65, he was assigned to the Norwegian Defence Research Establishment during his military service, working with design and integration of rocket pay-load instrumentation for investigation of auroral particles.

In 1965, he joined the Institutt for Atomenergi (presently Institutt for Energiteknikk), OECD Halden Reactor Project. Except for a study year at the Imperial College of Science and Technology in London, UK, in 1968–69 and a two-year period in 1972–73 when he was employed as a lecturer at the Electrical Engineering Department, University of Nairobi, Kenya through the Norwegian Agency for International Development, he has since then had different assignments at the OECD Halden Reactor Project. He has experience in a wide variety of disciplines within

nuclear research and development, including reactor physics and dynamics, two-phase flow dynamics, reactor and plant control systems, fuel performance modelling, core surveillance, and operator support systems. Presently, he is head of the Control Room Systems Development division at the Halden Reactor Project with overall responsibility for the development of operator support systems for nuclear power plant control rooms.

Mr Bjørlo is the author of numerous reports and papers within the above research disciplines and has served in programme committees and as chairman in international conferences in the nuclear field.

Kjell Haugset

Kjell Haugset obtained a MSc in physics from the University of Oslo, Norway, in 1965. In 1967–68, he was visiting scholar at the Nuclear Engineering Department of the Massachusetts Institute of Technology.

In 1965, he joined the Institutt for Atomenergi (presently Institutt for Energiteknikk) at Kjeller, where he worked in the area of reactor physics with emphasis on reactor dynamics.

Since 1976, Mr Haugset has been employed at the Institutt for Energiteknikk, Halden, mainly working within the OECD Halden Reactor Project research programme. He was responsible for developing the first version of the core surveillance system SCORPIO. Later, he was heading the project on development of the integrated surveillance and control system ISACS, which is presently in operation in the Halden Man-Machine Laboratory.

Mr Haugset is presently head of the Man-Machine Systems Research division and has the overall responsibility for the Halden Project research programme on software reliability, human factors, and advanced control room development. In addition, the division is engaged in bilateral work towards Norwegian and foreign industries. Mr Haugset has written a number of reports and papers, and is active in international committees in the nuclear field.

Øivind Berg

Øivind Berg graduated from the Norwegian Institute of Technology, NTH Trondheim, Norway, in 1977, where he studied solid state and theoretical physics. His main thesis was on the use of X-ray diffraction to study the electron structure of single crystals.

In the period 1977–80, he was employed at the Norwegian Defence Research Establishment in Horten, working with underwater acoustics, digital signal processing, real-time systems, and array processors.

He has been with the Institutt for Energiteknikk, OECD Halden Reactor Project, since 1980. His main responsibilities have been to develop and deliver the Core Surveillance system SCORPIO to a number of utilities. The research activities have covered areas like Optimal Predictive Control, system engineering, and user-interface design.

Mr Berg is the section head of modelling and simulation within the Control Room Systems Development (CRSD) division at the Halden Project. In addition to core surveillance, the section develops systems for early fault detection, alarm analysis, and accident management support. Mr Berg also acts as the deputy division head of CRSD.

Gustav Dahll

Gustav Dahll obtained a MSc in nuclear physics from the University of Oslo in 1964.

Between 1964 and 1970, he received various scholarships in theoretical physics: Western Reserve University in the USA, NORDITA-Niels Bohr Institute in Denmark, and Oslo University.

In 1970, he joined the OECD Halden Reactor Project, where his work has consisted in research in and development of computerized operator support systems (alarm and disturbance analysis) and reliability analysis. The latter has included plant reliability and safety and human reliability, but the main emphasis has been put on software dependability. He is now leader of a section on software verification and validation at the Halden Project, and is the author of numerous reports and papers on this subject.

He has also actively taken part in international work on developing standards and guidelines for developing and validating safety-related computer systems.

Terje Sivertsen

Terje Sivertsen obtained a MSc in Computer Science from the University of Oslo, Norway, in 1988. He graduated with a thesis on the use of logic programming in formal verification. Since 1988, he has been assigned to the Institutt for Energiteknikk, OECD Halden Reactor Project, where he has been central in establishing several research activities on formal methods in software engineering. One of his main contributions has been the development of a formal software development method based on algebraic specification, including an experimental theorem prover called the HRP Prover. Recently, he has been using this method in a case study on the formal development of a reactor safety system. His research activities on algebraic specification have been performed in parallel with the evaluation of formal methods on a broader scale. His research activities have also included the applicability of formal methods to the verification of the correctness of discrete event control systems and to qualitative reasoning about physical systems.

Mr Sivertsen is the author of several reports and papers on formal methods. Presently, he is working as a research scientist in the Software Verification an Validation Section of the Man-Machine Systems Research Division (OECD Halden Reactor Project).

Geir Pettersen

Geir Pettersen obtained a MSc in Computer Science from the Norwegian Institute of Technology (NTH), Trondheim, Norway, in 1988. His main thesis was performed at the Institutt for Energiteknikk and covered the configuration of operator interfaces in computerized control rooms.

He has since 1988 been employed at the Institutt for Energiteknikk, OECD Halden Reactor Project, as a research scientist. During this time, he has been working on several tasks related to user interfaces in real-time process control environments. Main activities include developing User Interface Management Systems, emulating various control systems for training simulator applications, retrofitting plant computer systems, and developing tools for simulator configuration and execution.