3099

Department of Energy
Idaho Operations Office
550 Second Street
Idaho Falls, Idaho 83401

JUN 19 1979

TO: M. R. Hayes, Chief, Budget and Contracts Management Branch
Division of Reactor Safety Research, NRC
Silver Spring, MD - Mail Stop 1130SS

FROM: R. E. Tiller, Director
Reactor Operations and Programs Division, ID

R. E. Tiller

SUBJECT: TRIP REPORT - G. R. BURDICK

In accordance with your March 11, 1977 memorandum, enclosed are four copies of the trip report for G. R. Burdick's travel to Halden, Norway, May 29-30, 1979.

Enclosure:
Trip Report (4)

cc: R. W. Barber, DOE-EV/NSC, Germantown, MD

EG&G Idaho

INTEROFFICE CORRESPONDENCE

date June 13, 1979

to Distribution

from J. L. Tylee MC-H for J. L. Tylee

subject TRIP REPORT ON VISIT TO OECD HALDEN REACTOR PROJECT - JLT-14-79

Attached is a copy of the trip report documenting a visit to the OECD Halden Reactor Project, Halden, Norway on April 23 through April 29, 1979. The trip was taken to obtain details on their utilization of digital computers in the control and supervision of nuclear power plants.

If further information is desired, please contact me.

pp

Attachment:
As Stated

DISTRIBUTION

A. N. Anderson
J. E. Baston
G. R. Burdick
T. M. Clemo
J. J. Feeley
R. T. French
J. M. Griffith
[redacted]
J. W. Henscheid
W. R. Nelson
J. W. Sielinsky
C. R. Toole
J. O. Zane
Central File
J. L. Tylee File

FORM EG&G-954
(Rev 2-77)

REPORT ON TRIP TO OECD HALDEN REACTOR PROJECT

SUMMARY

Traveler: J. L. Tylee, Senior Research Engineer, Systems Identification Section, Systems Analysis Branch, EG&G Idaho, Inc.

Date of Report: June 11, 1979

Destination: Institutt for Atomenergi; OECD Halden Reactor Project, Halden, Norway

Date of Trip: April 23 through April 29, 1979

Personnel Contacted: M. Øvreeide, Computer Applications
T. Bjørlo, Fuel and Core Performance
D. Miller, EG&G Idaho, Inc.

Purpose: To obtain information and design details on the utilization of digital computers in the protective, operator communications, control and alarm systems on the Halden reactor.

Abstract: Advanced operator communications systems based on color CRT systems are described and evaluated. Early work involving the application of modern control theory to power and pressure control of the Halden reactor is discussed. Work being performed using state variable feedback control of PWR core power distribution control is examined. Areas of possible interaction between the OECD Halden Project and EG&G are presented.

REPORT ON TRIP TO OECD HALDEN REACTOR PROJECT

The Systems Analysis Branch of EG&G Idaho is currently involved in a DOE-funded project to investigate the applicability of advanced control and estimation theory to the operation of nuclear power reactors. Initial scoping studies made for this project developed the approach of implementing the plant control, estimation, and protection algorithms on digital computers, and providing operator output via CRT color graphics. The OECD Halden Project is a recognized leader in the applications of digital computers and color graphics to the protection, operator communications, control, and alarm systems of nuclear power plants. The information and details obtained in discussions with the cognizant Halden engineers will expedite the work being performed in the DOE project by greatly reducing the required design and programming efforts.

The Halden Boiling Heavy Water Reactor (HBWR) went critical on June 25, 1959, and has been in regular operation with stops only for regular maintenance and fuel changes since then. The plant has three heat removal systems, the primary being a closed heavy water circuit, the secondary a high purity light water circuit, and the tertiary an open light water circuit with the steam being used as process steam at a nearby paper plant. The plant is primarily controlled from a conventional control room. The first attempt at developing advanced control rooms was in 1969 and resulted in the OPCOM (OPerator COMmunications) system. The system consists of a set of three color graphics terminals with a central operator console connected through a set of digital computers to the plant. The operator can access via the console various trend plots, plant circuit diagrams, and status information. The HBWR has been operated for a period of months through OPCOM, which in a modified version is being installed in several Swedish-built nuclear power stations. From operator feedback, limitations of the OPCOM system were identified, primarily inability to display more colors (only four colors are available on OPCOM) and the restriction of a single operator console. The OPCOM system is currently inactive and effort is being applied to developing the next generation of communications consoles.

The new system, CONSUP (CONtrol and SUPervision) is being intended as a main communication system in computer controlled plants. A prototype version of the new system is set up in an experimental control room at the Institutt for Atomenergi near the Halden plant. CONSUP is interfaced with a real-time nuclear power plant simulator, enabling experimental investigation of communication and control procedures under realistic conditions. The simulator, STUDS, describes the power production in a general Westinghouse PWR plant with any number of steam generators and turbines. Outstanding characteristics of STUDS are a sixteen-node axial core simulation, the ability to model more than one steam generator loop, and the real-time capability. The model is coded in FORTRAN IV and at Halden is implemented on a Norwegian-made NORD-10/NORD-50 computer system. It requires 24K of memory and one execution of the program requires 36 msec of CPU time, easily allowing a 200 msec time step in updating the various process variables. In turn, the graphic displays of the CONSUP system are updated every five seconds.

Compared to OPCOM, CONSUP is a vast improvement. The system consists of three studio quality color monitors each with its own access console. From a console, the operator has the option to select numerous displays. Typical displays available provide information on the reactor core, primary cooling loop, the steam generator feedwater system, and the turbine-generator set. System overviews or detailed schematics of a single pump or generator can be called up. Each display provides dynamic values of system temperatures, pressure, levels, and power outputs. Colors are used to indicate whether a flow path is open, valve position, and whether a particular variable is within an acceptable range. A feature of the system that is particularly useful is the ability to display up to four trend plots of various parameters. The operator may select one of three time scales, 12 minutes, one hour, or 24 hours, and the system will generate dynamic plots (updated every five seconds) of the selected parameters. These trend plots essentially replace the conventional strip charts. Tests using actual operators have been made with CONSUP to determine suitability of colors, keyboard layouts, and display requirements.

The software driving CONSUP was developed at Halden and is written in FORTRAN. Terminal hardware, including keyboards and CRT display generators, are made and designed by Halden technicians. A useful software package developed is an on-line editing feature. This feature allows the user to "draw a picture" on the CRT via a few simple commands. A selection of 256 characters is available or the user can develop any character possible in an 8 x 7 matrix of dots. There are 4096 color combinations available although studies show the operators would desire a maximum of about 15 colors for actual implementation. Besides application to the nuclear field, various versions of the CONSUP system are currently is use for process control at oil drilling rigs and paper mills and for navigation control in the Norwegian fjords.

A primary purpose of the trip to Halden was to learn of their experience in the application of modern control theory to the HBWR. A modern control scheme was implemented on the HBWR in 1971 as a demonstration of the theory and was primarily for steady state control of reactor power and pressure. The final control algorithms developed were found to perform satisfactorily, however it was observed that a properly tuned PID-control algorithm for the same variables as controlled with the modern algorithms provided comparable performance. The general conclusion from this work was that the coupling between the power control loop and the pressure control loop in the HBWR is fairly weak, and that a greatly improved control performance using modern control theory could not be observed. The PWR is felt to be a more likely candidate for such modern control applications.

The only current work being performed at Halden relating to the applications of modern multivariable control theory to nuclear plants is in the area of PWR core power distribution control. The aim of this work is to obtain maximum core maneuverability within constraints derived primarily from the limited ability of the fuel to endure power shocks. Three control algorithms have been developed and are presently being subjected to realistic tests in extensive simulation studies. The algorithm of primary interest is that referred to as state variable feedback (SVF). This technique involves a straightforward application of modern control theory. The measured power distribution (13 axial nodes), including noise, is processed by a steady state Kalman filter, which includes the known noise characteristics and a linearized 3-D core model, to make estimates of the unmeasurable states, the iodine and xenon concentrations in each axial node. The full state vector, i.e., the power and iodine and xenon concentrations in each node, is then multiplied by an optimal, steady state feedback gain matrix to provide the control inputs: rod bank position and boron concentration. This optimal control is obtained by minimizing a standard quadratic performance index. All of the required computations are done on a Cyber 74 computer and follow the program sequence: (1) 3-D core model (COSMIC), (2) model linearization (COREP), (3) normalization (PROVA),, (4) discretization, Kalman filter and control gains (MULTEC), and (5) simulation (OPTCOR). It is envisioned that for actual implementation on a plant, a time step of one hour would be sufficient to perform the needed calculations. A future modification to this scheme is to include core coolant temperature as a control input.

Related to this core power distribution control is work being done in the field of core surveillance. Here the emphasis is on the use of core simulators on-site to obtain information about the dynamic behavior of the core in response to proposed control inputs. Such simulators can be used to ascertain that local fuel heat ratings stay below operational limits during load maneuvers or to compute the axial power distribution required in the SVF feedback scheme.

Other core control strategies that have been developed use multistage mathematical programming (MMP) and multivariable frequency response (MFR) methods. The MMP is primarily a predictive technique based on nonlinear programming that allows the plant to follow a predefined load curve subject to some minimization function and a set of constraints. The MFR technique is an extension of classical control theory to allow application to multivariable systems and was not of much interest.

The program used in the SVF method for computation of the Kalman filter and controller gains, MULTEC, offers many desirable features including: discretization of continuous systems, calculation of Kalman gains in continuous and discrete domains, calculation of optimal control gains in continuous and discrete domains, eigenvalue calculations, calculation of observability and controllability, and simulation of process control systems. EG&G should pursue the acquisition of such a code for its work in control applications.

This covers the primary topics discussed during the Halden trip. Other areas addressed included computer architecture, human interface, microprocessor applications, noise analysis, software reliability, and on-line maintenance assistance. Papers concerning these and previously mentioned topics were obtained and are listed in the appendix to this report. A presentation concerning the Systems Analysis Branch and how it fits into EG&G Idaho and the INEL was made at the Institutt for Atomenergi and was well received. Particular surprise was expressed at the number of operating reactors at the INEL.

Interest was expressed by Magnus Øvreeide, Manager, Computer Applications, in the possibility of initiating a joint research program between the OECD Halden Project and EG&G through the NRC. Areas identified as possible candidates for a cooperative effort included: (1) operator communications, (2) disturbance analysis system development, (3) on-site core simulators, and (4) microprocessor applications. In addition, Mr. Øvreeide stated that all computer routines at Halden are to be converted from FORTRAN to PEARL, a German-developed real-time process control language. This new language could be of help in the current DOE project. A request for information on PEARL was sent to Norskdata, a Norwegian computer firm.

The information gained in this trip to the OECD Halden Reactor Project will provide major progress in the advanced control work currently being pursued at EG&G Idaho.

APPENDIX

ITINERARY AND PERSONS CONTACTED

4-20-79 through 4-22-79	Travel: Idaho Falls to Oslo, Norway Oslo, Norway to Halden, Norway
4-23-79	OECD Halden Reactor Project: 1. Dick Miller, EG&G Idaho 2. Magnus Øvreeide, Manager, Computer Applications 3. R. Stokke, Operator Communications 4. J. Høl, Halden Reactor 5. K. Netland, Computer Architectures
4-24-79	OECD Halden Reactor Project: 1. M. Øvreeide 2. K. Netland 3. K. Haugset, Core Power Distribution Control 4. R. Moen, Core Power Distribution Control
4-25-79	OECD Halden Reactor Project: 1. T. Bjørlo, Manager, Fuel and Core Perofrmance 2. K. Haugset 3. R. Moen
4-26-79	OECD Halden Reactor Project: 1. M. Øvreeide 2. T. Bjørlo 3. I. Leikkonen, Linear Core Models 4. G. Dahll, Software Reliability 5. R. Oguma, Noise Analysis
4-27-79	OECD Halden Reactor Project: 1. G. Dahll, Disturbance Analysis System 2. K. Haugset 3. M. Øvreeide 4. T. Bjørlo
4-28-79	Halden, Norway
4-29-79	Oslo, Norway: 1. Arild Ek, Institutt for Atomenergi, Kjeller, Norway

4-30-79	Personal Travel: Oslo, Norway to Stockholm, Sweden
5-1-79	Personal Travel: Stockholm, Sweden to Sulkava, Finland
5-2-79 through 5-5-79	Personal Travel: Sulkava, Finland
5-6-79	Personal Travel: Sulkava, Finland to Helsinki, Finland
5-7-79	Travel: Helsinki, Finland to Idaho Falls

BIBLIOGRAPHY OF ACQUIRED LITERATURE

1. B. Fagerstrøm, R. Stokke, B. Blomsnes, et al, Present Status and Planned Use of the Computer Control Experimental Facility at the Halden Project, Enlarged Halden Programme Group Meeting, Loen, Norway, June, 1978.

2. J. Ø. Hol, G. Øhra, K. Netland, Design of Pictures and Use of Colours and Symbols for a CRT Based Supervision System, Enlarged Halden Programme Group Meeting, Loen, Norway, June, 1978.

3. R. Stokke, B. Fagerstrøm, STUDS - A Simulator Tool for Control Development, Enlarged Halden Programme Group Meeting, Fredrikstad, Norway, June, 1977.

4. A. B. Long, editor, Assessment of Technologies Essential to the Application of Advanced Systems for Process Control, EPRI NP-640, Research Project TPS 75-625-1, 2, 3, January, 1978.

5. F. Øwre, L. Felkel, Functional Description of the Disturbance Analysis System for the Grafenrheinfeld Nuclear Power Plant, Enlarged Halden Programme Group Meeting, Loen, Norway, June, 1978.

6. K. Netland, Architectures for Distributed Computer Process Control Systems, Enlarged Halden Programme Group Meeting, Loen, Norway, June, 1978.

7. B. Blomsnes, J. Karppinen, J. Shimazaki, R. Versluis, Core Control by Linear State-Variable Feedback, Enlarged Halden Programme Group Meeting, Sanderstolen, Norway, March, 1976.

8. R. Versluis, B. Blomsnes, J. Karppinen, Can Optimal Core Power Control Reduce the Operating Cost of Nuclear Reactors?, Enlarged Halden Programme Group Meeting, Sanderstolen, Norway, March, 1976.

9. J. Karppinen, R. Versluis, B. Blomsnes, Core Control by Multistage Mathematical Programming, Enlarged Halden Programme Group Meeting, Sanderstolen, Norway, March, 1976.

10. J. Karppinen, B. Blomsnes, An Application of Optimization Methods to Spatial Control of Nuclear Reactor Cores, International Symposium on New Trends in Systems Analysis, Vienna, Austria, December, 1976.

11. K. Haugset, J. Karppinen, B. Blomsnes, E. Robinson, Optimal Core Control Strategies by Multistage Mathematical Programming, Enlarged Halden Programme Group Meeting, Fredrikstad, Norway, June, 1977.

12. T. Busi, K. Haugset, I. Leikkonen, Improvements of the MMP and SVF Core Control Methods, Enlarged Harden Programme Group Meeting, Loen, Norway, June, 1978.

13. T. Busi, K. Haugset, E. Robinson, et al, Core Control Strategies for the Calvert Cliffs PWR Derived from Multistage Mathematical Programming and State Variable Feedback, Enlarged Halden Programme Group Meeting, Loen, Norway, June 1978.

T. Busi, Synthesis of a Power Distribution Control System for Nuclear Reactor Cores by Multivariable Frequency Response Methods, Enlarged Halden Programme Group Meeting, Loen, Norway, June 1978.

15. COREP, A Computer Programme for Calculating Linear Core Models, OECD Halden Reactor Project, March 1976.

16. A. Ek, E. Gran, Program MULTEC-1, Multivariable Estimation and Control, Institutt for Atomenergi, Kjeller, Norway, April 1974.

17. A. Ek, MATFOR Version 2.0 Users Manual, Institutt for Atomenergi, Kjeller, Norway, March 1977.

18. T. Bjørlo, B. Blomsnes, R. Grumbach, et al, Application of Modern Control Theory for Regulation of the Nuclear Power and the Reactor Vessel Pressure of the HBWR, OECD Halden Reactor Project, HPR 131, August 1971.

19. B. Blomsnes, R. Karlsson, K. Sato, et al, A Computer Control Concept for Load-Following Control of a Nuclear Plant, OECD Halden Reactor Project, HPR 164, October 1973.

20. R. Karlsson, K. Sato, E. Schwieger, A Load Follow Control System for a Nuclear Power Plant with Extended Linearization and Filtering Technique, OECD Halden Reactor Project, HPR 179, April 1975.

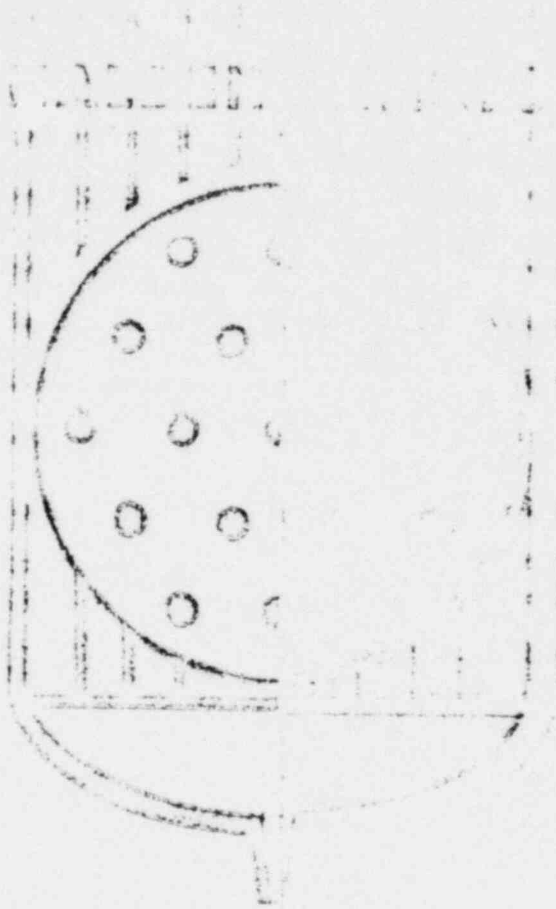
21. Y. Shinohara, R. Oguma, Estimation of Time-Varying Reactivity Using a Method of Nonlinear Filtering, Nuclear Science and Engineering: 52, 76-83, March 1973.

22. K. Matsubara, R. Oguma; A Multivariable Autoregressive Model of the Dynamics of a Boiling Water Reactor, Nuclear Science and Engineering: 65, 1-16, May 1977.

23. R. Oguma, E. Robinson, Evaluation of the Dynamic Behaviour of Fuel Rod Elongation by Noise Analysis, Enlarged Halden Programme Group Meeting, Loen, Norway, June 1978.

24. R. Oguma, Noise Source of the Resonant Power Oscillation in the HBWR, OECD Halden Reactor Project, IDG - Note 2512, June 7, 1978.

HPR-226



OECD HALDEN REACTOR PROJECT QUARTERLY PROGRESS REPORT JANUARY TO MARCH 1979

INSTITUTT FOR ATOMENERGI
OECD HALDEN REACTOR PROJECT
P.O. BOX 173 - HALDEN - NORWAY

Core Surveillance and Control (III.3)

The core simulator QUABOX/CUBBOX, which has been received from Gesellschaft für Reaktorsicherheit (GRS), is at present running on the scientific CYBER computer. Work is continuing on comparisons between this code and the neutronics code CYGNUS.

The work on core surveillance is concentrated on developing a system for display of results from the core simulator COSMIC, using the computer control experimental facility.

In the field of core control methods, several model improvements on the Multistage Mathematical Programming (MMP) method were made during 1978. Comparison between the previous and the newer model has been made through simulation of load cycling of a 2700 MWt PWR core. The model improvements are clearly reflected in the improved quality of the results.

Disturbance Status Analysis (IV.2)

An experiment will be carried out on the Halden Project's experimental facility in the end of May to demonstrate the behaviour of the disturbance analysis system developed for the feedwater circuits of the Grafenrheinfeld PWR plant, and preparations for this experiment are going on.

The process is simulated by an extended version of the PWR simulator. Work is now concentrated on making a programme system to impose disturbances on the process, which then will be analyzed by the disturbance analysis module. The propagation of the disturbances and the results of the analysis will be monitored by the supervisory module and visualized on colour displays.

In the joint project with Österreichische Studiengesellschaft für Atomenergie Ges. m.b.H. (SGAE), Austria, on computerized surveillance of protection systems, a pilot version of a computer programme "Computerized Operation Manual" has now been completed and is presently operating on the Halden experimental facilities. A final report on this programme system is under preparation and will be published as a Halden Project Report. In the continuation of this project it is planned to establish a basis for developing such a system through a more fundamental analysis of protection systems and thereby making it more generally applicable. This work has started with functional analysis and failure mode and effect analysis of a chosen protection system.

A workshop meeting on "Noise Analysis Techniques for Plant Surveillance and Early Failure Detection", attended by twelve experts from organizations participating in the Project, was held in Halden on 22nd March. The activities in this field in the Signatory countries were surveyed, and useful recommendations and proposals concerning planned work at the Project in this area resulted from the discussions in the workshop.

Operator Process Interaction (IV.3)

To investigate the operator's role in current as well as in planned control rooms, questionnaires were sent out to some utilities in the Signatory countries. The responses to the questionnaires are now being compiled and merged with already existing data for further analysis.

Experiments are under preparation to investigate the operator's responses (his thinking and acting) under steady state reactor operation as well as under disturbance situations. The experiments will utilize the experimental facility. For this purpose the experimental facility will comprise the STUDS plant simulator, extended with a model of a detailed PWR feedwater system, but there will not be any modification to the existing control room. The work is now concentrated on preparing the control system for the operation of the simulator.

The communication part of the control system is based on the established philosophy for design of such systems at the Project based on the past years' experience.

Concerning guidelines for use of colours and symbols, work has been concentrated on measuring the physical behaviour of colours emitted from standard CRT monitors to obtain standard CIE colourimetric diagrams for these devices. A state-of-the-art study concerning commercially available colour graphic systems has been undertaken. Features and cost/performance figures have been listed. In general this investigation has revealed that there now are a number of such advanced systems on the market.

In testing of the established high reliability computer structure, efforts are especially centred around the common memory module and its connection to the various computers.

A conceptual study of computer-based control systems has been initiated, with special emphasis on investigations of existing process input/output techniques, including use of microprocessors and fibre optics.

Computer-based control systems for processes with a certain complexity and size need descriptions of all process-parameters, such as measurement points, units, alarm texts, trends, etc. These parameters are a priori information which has to be inserted into tables used by the various control programmes. A conceptual study of an automatic procedure for this work has been initiated, and an existing data base system will be used for this study.

In the joint project between the Technical Research Centre (VTT), Finland, and the Halden Project on software reliability, the data obtained during the analysis and testing period were used as a basis for software reliability assessment. Various methods were applied, but the results were very diverging. One can therefore conclude that none of these methods can be applied with confidence in this specific case. This project is now completed, and a report has been written and will be published as a Halden Project Report in the near future. This cooperation with VTT is continuing, and a new project, aimed at studying methods for the specification of computer programme systems, has been defined. A literature study on this topic has been initiated.

In 1979 the Halden Project has started an activity on the study of high level computer languages. A study of various aspects which are of importance in the evaluation of computer languages, is being made with the intention of applying them on the real time language PEARL.

IMPROVED MULTISTAGE MATHEMATICAL PROGRAMMING CONTROL METHOD TESTED ON A PWR MODEL

The Multistage Mathematical Programming (MMP) method is developed to calculate optimal control strategies for pressurized water reactors. It is based on linear core models and prescribes the controller movement required to minimize some given objective function describing the deviation from a desired power distribution, controller positions, etc. In MMP the same linear models are also used to calculate the power, xenon and iodine distributions resulting from these controller movements. These distributions can then be compared with results from a core simulator, COSMIC, which is assumed to describe the actual reactor very well. Because MMP uses linear models, there is generally some disagreement between MMP and the core simulator. It has been found that in some cases the disagreement is larger than expected. Some modifications in MMP have now been introduced and their effects studied through recalculation of a previously calculated control problem (1).

Modifications

In MMP the so-called core response matrix relates the rod movements to changes in power density. The approximation for the dependence of this core response matrix on the total power level has been slightly changed, as described in (2), which also describes how the method to calculate the feedback matrix has been modified. The feedback arises mainly from the Doppler effect.

The linear models used in MMP are generated from calculations with the core simulator, giving the power distribution, etc., at the linearization point. In the simulator calculations it is desirable to divide the core into many (several thousand in a full core) small nodes (or boxes). On the other hand, in the linear control model used in MMP, it is possible to have only some tens of nodes. The power densities in the nodes are connected to the power densities in the neighbouring nodes through neutron currents across the node boundaries. This coupling is described by coupling coefficients, and these are calculated in the core simulator also for the linear model. If the division of the core into nodes is identical in the simulator and in the control model, then the same coupling coefficients can be used both in the simulator and in the linear model. The method to calculate the coupling coefficeints for the larger nodes in the control model from the coefficients for the small nodes in the simulator has previously been the same as in the so-called coarse mesh rebalancing method (3). This method is used to speed up the eigenvalue calculation in the simulator by combining several small nodes into bigger ones, thus reducing the number of variables. The coefficients describing the coupling between control nodes clearly depend on the size of the small nodes that are combined to the control nodes, and in general the coupling coefficients obtained in this way seem to give a too strong coupling between the control nodes.

The method to calculate the coupling coefficients for the control model nodes has now been changes. The new method is based on two requirements: The neutron current between the nodes must be correct at the linearization point, and the error in the neutron current must be small when the power distribution changes slightly from the linearization point distribution.

Test Case

The control problem studied after the modifications were introduced, is the same that was presented at the Enlarged Halden Programme Group Meeting at Loen, 1978 (1). The reactor in these studies is a 2700 MWt PWR from Combustion Engineering, Inc., to be controlled over a typical daily load cycle, fourteen hours at full power, six hours at half power with two hours' rise and fall times, see Figure P-1. The

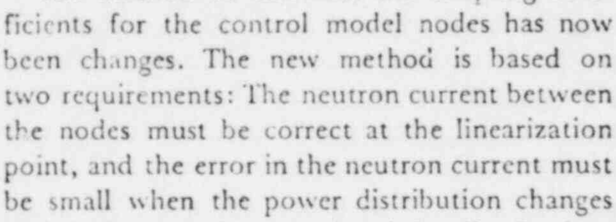


Fig. P-1. Load cycle to be controlled

control objective is to minimize the use of boron, with some emphasis also on the power distribution. Both in the simulator and in the control model one quadrant of the core is calculated. In the simulator, the quadrant is divided into 1240 core nodes, of 20 x 20 x 17.36 cm^3. In the control model these small nodes are combined into totally 36 nodes. The horizontal division into control and simulator nodes is shown in Figure P-2. The axial height of each control node is 86.8 cm. The total twenty-four hours' period to be controlled is divided into three control periods of equal length. The new (test)

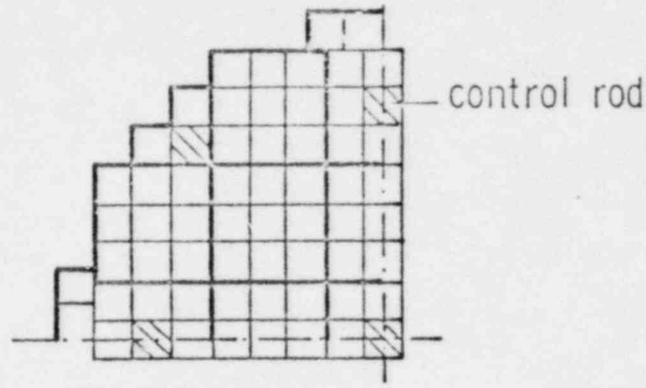


Fig. P-2. The division of the core quadrant into nodes in the simulator and control models. The size of the simulator nodes is 20 x 20 x 17.36 cm^3

and the old (1) calculations are not completely identical. In the new calculations totally four linear models were used, in the old ones only two. In the new calculation also the possibility to change the core response matrix according to the rod movements was used, because the rod movements were rather large. Their non-linear effect on the power distribution therefore became too significant. Also the input data for controller strengths and objective function differ slightly from the old calculations. Thus the differences in the results from the new and old calculations can be attributed partly to the modifications in MMP and partly to the abovementioned differences.

The main results of the MMP test calculations are shown in Figures P-3 - P-6 compared with results from simulating the MMP control strategy with the core simulator COSMIC. The results of the old calculations are also given. The rod movements (Fig. P-3) are basically similar in both calculations, but obviously the weight on the power distribution is larger in the new calculations than in the old ones. In the new calculations the agreement of the MMP calculation and the COSMIC simulations seems to be better than in the old ones for boron and axial power shape index (power in lower half of core minus power in upper half divided by total power), Figures P-4 and P-5, whereas the agreement for power peak (maximum power density in the large nodes normalized to core average), Figure P-5, is about the same. The somewhat strange behaviour of the power peak (visible also in the axial shape index) at about 20 hours may result from the rod tip crossing the node boundary giving rise to a rather strong variation in the power density and thus a strong coupling between adjacent nodes near the rod tips.

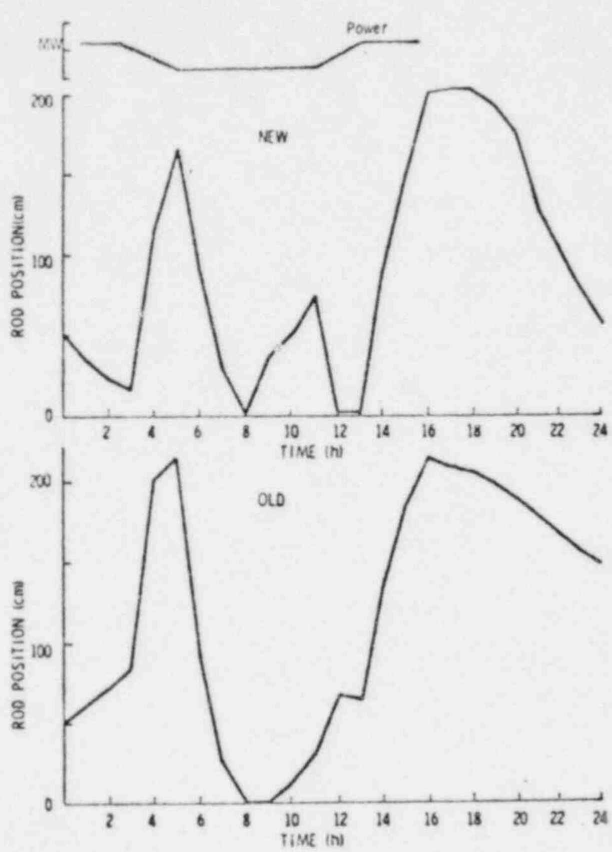


Fig. P-3. The control rod movements in the new and old (1) calculations

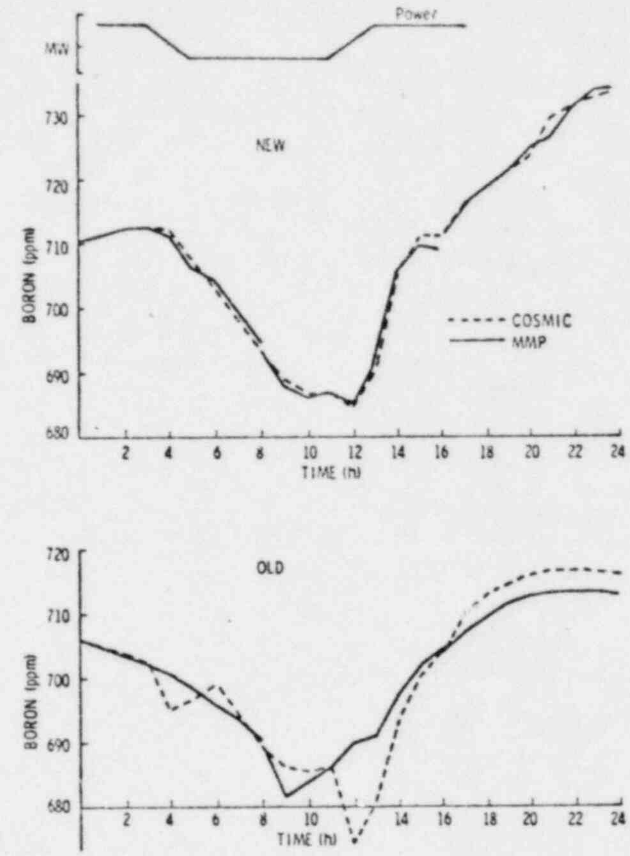


Fig. P-4. The boron concentration in the "minimum boron" control

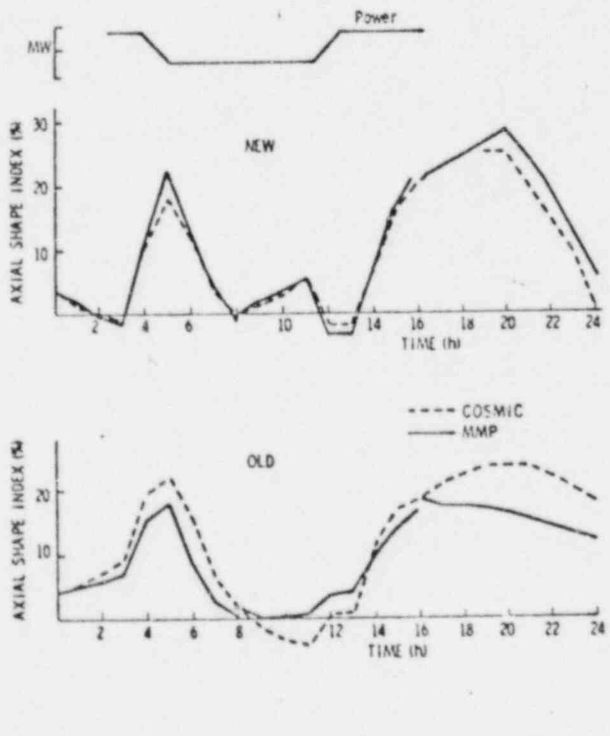


Fig. P-5. Axial shape index in the "minimum boron" control

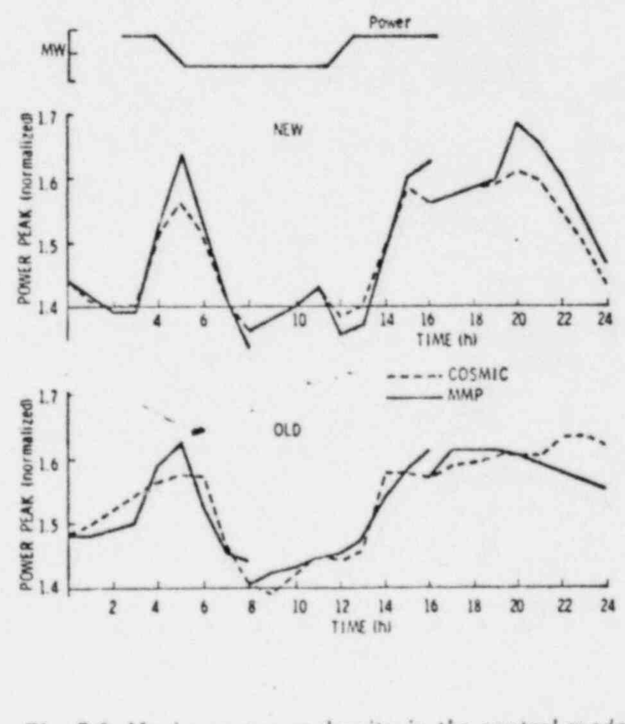


Fig. P-6. Maximum power density in the control model nodes. It is normalized to the average power density

SOFTWARE RELIABILITY – INVESTIGATION OF SPECIFICATION METHODS

Introduction

A joint project between the Technical Research Centre (VTT), Finland, and the Halden Project on an investigation of methods for developing and testing reliable software has just been completed. An experience from this project was that weaknesses in the specification were frequent sources of misconceptions and errors in the programming. The cooperation between VTT and the Halden Project will therefore continue in a project on an investigation and development of methods for the specification of computer programme systems. It was also confirmed in a workshop on software reliability held in Halden in October 1978, that this is an area of common interest to the Signatory organizations of the Halden Project.

The work made within this area during the last quarter has been devoted to an investigation of various specification methods found in the literature. It has been attempted to define the aspects which may be used to classify the various methods, and which further may be of importance for the selection of the specification methods for a specific problem. In the following some of these aspects will be shortly described.

Aspects and Concepts

One aspect is the *level of generality*. A high level of generality means that the specification method can be applied on a large variety of problems. A typical example of a specification method with a high level of generality is the DELTA language (4) which can be used to describe all kinds of processes and systems, and not only to specify programme systems. A slightly less general specification is SADT (5). This is a method suited to describe the information flow of processes of any kind, but not suited to describe static systems.

On the opposite side there is a method (6) for the specification of data structures by defining them as data abstraction with the use of algebraic axioms.

Another aspect is the question of *functional versus design specifications*. There is no clear division between these concepts, as the design of one step in the development process will constitute the functional specification of the next step. The specification process can thus be viewed as a scale starting with the most "functional" of the steps sliding over the most "designly".

An important point concerning specification is *comprehensibility*. This is not a uniquely defined concept, as there are many aspects connected to this concept. One is the question to whom the specification should be comprehensible. It might e.g. be necessary to make the specification comprehensible for a non-technician. A hierarchic build-up of the specification will in general enhance the comprehensibility. This aspect is stressed in e.g. SADT, and is obtainable in a variety of specification methods. At a more detailed level the specification should be understood by both a non-programming process engineer and by a programmer with no knowledge of the process. Another aspect concerning the comprehensibility is whether the method is *easy to use* for the specifier, i.e., whether the specification method in itself is easy to comprehend and apply. The hierarchic method seems a good way of attacking the problem, but it requires a certain dicipline by the specifier who might be unaccustomed to the method.

The *format* of the specification is a concept which is related to the comprehensibility. The format of the various methods can in general be grouped into three classes: the graphical format, the pseudocode format and the mathematical/logical format. The first one, using directed graphs to show the information flow (e.g. SADT), makes the specification easy to grasp visually. The second one, using ordinary language written in a way resembling a computer language, is easier to write and to be handled by a possible computer aided specification. The last one, comprising various methods, like the use of decision tables (7), has its advantage for the verification of the programming system.

Another concept is the *conciseness* of the specification method. This is enhanced through a well defined syntax, but this is not enough because a well defined semantics is also needed. Syntaxes seem to be defined for most specification methods, whereas the semantics are defined to a variable degree within these methods. As it will be virtually impossible to define a semantics covering all possible areas of specification, it is evident that the more general specification methods will have a rather loosely defined semantics, i.e., the specifier will have to define his own semantics at a more detailed level. The more special specification methods may, on the other side, have a more well defined semantics.

A concept which is, in a way, related to the preceeding ... the *level of abstraction*. Methods at a high abstraction level can be used to express details of the specification very precisely, whereas more straight forward methods must often rely on the amount of preciseness that ordinary language can give. Methods at a high abstraction level may seem rather incomprehensible, but that will to some degree depend on who is going to use it.

As conciseness and abstraction level are concepts concerning the specification method, the concepts of *completeness* and *consistency* are concerning the specification as such. By completeness is meant that the specification defines an action for all possible input combinations and situations, whereas consistency means that the specification does not contain internal contradictions or deadlocks. A goal for a specification method is to prevent incompleteness and inconsistency in the specification. This leads us to the next important concept of the specification procedure, viz., the *verification* of the specification. There are various aspects of such a verification. One is to verify that the specification fulfils the intention of the specifier. This aspect is difficult to perform by a general method. Another aspect is to verify the completeness of the specification.

For a graphic specification, the Petri net analysis might be useful to check that the specification fulfils certain criteria, like safeness and liveness. One way of verifying the specification is by way of *simulation*. It is difficult to include a simulation in a general specification method, as that goes beyond the scope of the specifications. But the method should encourage the use of simulation, and Petri nets are suitable tools for a partial simulation.

The specification procedure is only a part of the total programme development procedure, and for a verification of the total programme it is necessary to verify the programme versus the specification. An aspect of the specification which is also of interest, is therefore its suitableness as a *basis for programme* verification. The use of axiomatic specifications seems suitable for such techniques.

In addition to the general characteristics of specification procedures, there are other specific aspects which should also be considered during the specification, like the synchronisation of non-deterministic processes and the restart conditions for real-time systems in case of a computer stop etc.

Conclusion

The intention of this work has been to focus the attention on various aspects and concepts which are of importance for the specification procedure. It has also been pointed out that these aspects and concepts are managed differently in the different specification methods. It is therefore our conclusion that the choice of a specification method should depend on the problem to be specified and also on the goals one wants to achieve (for instance on software reliability). It is, however, not said that one should use one method for the whole specification procedure. One may, for instance, combine the more general methods with the more specific method for details. But one may also apply two or more methods in parallel for the whole problem to obtain a complete and correct specification. This might be a good procedure in projects where dual programming is recommended to gain a high software reliability. It would be useful to perform an experiment in this direction.

OPERATORS' PERFORMANCE EXPERIMENTS

Experiments are being prepared for the analysis of the safety problems related to operating personnel in nuclear power plants as regards the design of information presentation, the work situation and the training of the operators. A cooperation between some of the participating organizations (within the Nordic countries) has during the past years resulted in data on the function of the operator. These data have led to the formation, planning, and design of a series of experiments to study ergonomic evaluations and human reliability related to computer based control rooms with colour CRT's as one of the main man/process interfaces. Initially it will be investigated how various designs of CRT displays influence the perceived support given to the operator in his task performance. Ultimately, the experiments should provide knowledge about the operator's performance related to the information presentation, aiming at reducing the potential of operation errors. Figure P-7 below tries to illustrate the factors influencing his performance.

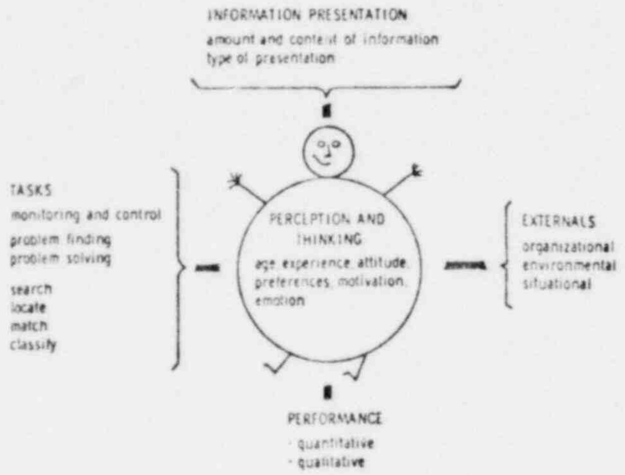


Fig. P-7. Factors influencing the operators' performance

The equipment required for the experimental series is mostly already at hand in the computer laboratory facilities of the Halden Project. This consists, besides the required computing capacity, of a computer based control room with necessary operator interfaces. The hardware and software already developed for man/process communication via CRT displays, function- and alphanumeric keyboards and tracker ball will be employed. The process, as it will be seen by the operator(s), is provided by a PWR simulator (STUDS-20) to a rather realistic detail level.

The experimental methods to be tested in a commissioning test planned for June 1979 may be identified as a so-called "Confrontation Method". In the present set-up this implies that an operator will act through a predefined operational task, e.g., to bring the plant from criticality to full power. During this performance the experimentalist may introduce predefined plant malfunctioning, which should be corrected by the operator. All plant data, operator's actions and man/process communication are logged on file. Some main plant parameters and all operator's actions are additionally listed on-line on hard-copy units. From the data logged on file a complete replication of the performance can be replayed, including the process history, the operator's actions and the man/process communication. Thus the experimentalist can confront the operator with every action done and their consequences, and inquire why he acted as he did in the various situations. In this way it is intended that the operator will reveal the structure of his mental model of the process, and the success of his performance will indicate how well the type of displays used matched his model.

STATE-OF-THE-ART STUDY OF COLOUR GRAPHIC SYSTEMS

At this stage a search on the market for existing colour graphic systems has been carried out. The search revealed sixteen serious manufacturers producing altogether a total of fifty different models, all possessing multi-colour capacity. These models were subject to a closer study, and the following list contains some of the parameters considered to be of importance:

- stand alone capacity
- resolution
- image refresh memory
- image refresh frequency
- colours
- semi/full graphic
- computer interface
- linkable peripherals
- available software
- special features
- available options.

All fifty models mentioned above make use of the raster scan technique. Colours typically range in number from 8 to 4096, where some models are capable of displaying all 4096 colours at the same time. At the extreme, other models can back up with 2^{24} (16,8 mill.) colours.

The trend is towards full graphic capacity, i.e., ability to address and process each picture element in the display. This combined with higher screen resolution – 1024 x 1024 picture elements – and possibilities for generating matrices, say 5 x 7 picture elements, will offer more flexibility in generating and displaying pictures.

Certainly, microprocessor-technology has also made its way into graphical display systems where devices like Z-80, Intel 8085, and Intel 8086 are often encountered. The microprocessors perform tasks like display control, serial and parallel interfacing, interrupt processing, and instruction decoding. More and more functions are incorporated which together with the microprocessor architecture makes the display units more powerful and less dependent on the host computer

The following items are some of the special features available today:

- hardware roll and scroll (roll is rolling by lines while scroll is rolling page by page)
- hardware zoom and pan (panning makes it possible to move symbols around in the display while zooming has the effect of magnifying a selected area)
- hardware graphics generator for plots, histograms, area outlines, special symbols, etc.
- hardware character and pixel (picture element) selective blink
- digitizers able to digitize video signals
- all kinds of programming features when a higher language package is implemented
- use of high resolution monitors.

A comparison of all fifty models was made, and with the technical aspect in mind, two or three models seemed to take the lead. With the performance of these units in mind, thinking of available software packages, available hardware options, and flexibility in design, they look like meeting not only the display requirements of today, but also those that can be envisioned for years to come.

AN ASSESSMENT OF A NEW DATA ACQUISITION AND CONTROL SYSTEM

Introduction

During the last years several concepts have been worked out to study high reliability computer structure. Based on the experience obtained from these studies and facing the need for replacing our existing data acquisition system, an assessment of a new system has been initiated. This study is also carried out with reference to point IV.3 in the 1979 Halden Project programme: "Development of a Revised Concept for Distributed Process Control Based on Micro Processors and Fibre Optics Technology".

For eleven years the IBM 1800 computer has rendered good support in data collection, computing and presentation of results from the various test fuel experiments. In addition, the computer has monitored a number of signals from the reactor plant, including the power of individual instrumented fuel assemblies.

With the development as seen today the experimental programme seems to increase both in complexity and sophistication which result in higher demands on the computing capabilities.

The requirements today are different from when the IBM 1800 was installed, because the functions are better defined and the users' needs are better known.

As a starting point in considering a new system, the main function blocks, as Fast Scan, Calib, etc., running on IBM 1800 are partitioned as shown in Figure P-8. The different signals are read by the different blocks to different areas either in core, on disc, or magnetic tape. The only coupling between the blocks is when one block needs data scanned by another block, and this is normally performed through the presentation programme. This indicates that it should be easy to specialize, or to separate the different function blocks on IBM 1800 among several microcomputers in a decentralized or distributed architecture, as indicated in Figure P-9. This method has a number of advantages, such as flexibility, expandability, simpler software, and higher reliability than a centralized computer system, but it has also typical drawbacks, as data communication and data integration become a necessary and perhaps a critical function.

The purpose is to achieve a gradual reduction of the IBM 1800 functions by implementing small submodels (task oriented computers) which ultimately will be integrated in a total test fuel experimental and plant supervision facility.

Future Requirements

The main function of the new system will be data acquisition, i.e., reading signals from the instrumented fuel assemblies, the special test rigs and the reactor plant, at different intervals as required by the experimental programme. However, the system will also be designed for control of test fuel experiments and provide possibilities for operator communication, simple at the lower level and more advanced at higher levels by using high resolution colour graphics.

Table P-1 shows the number of signals required

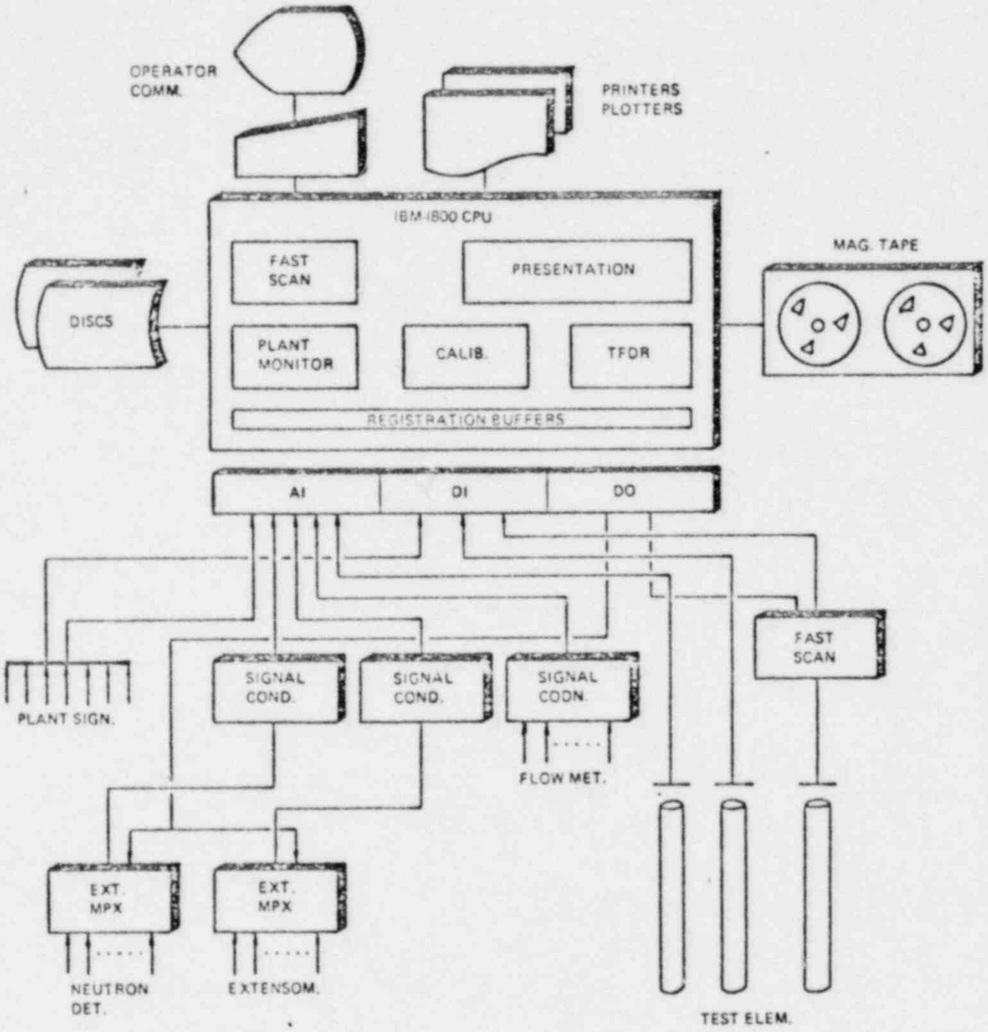


Fig. P-8. The IBM-1800 structure

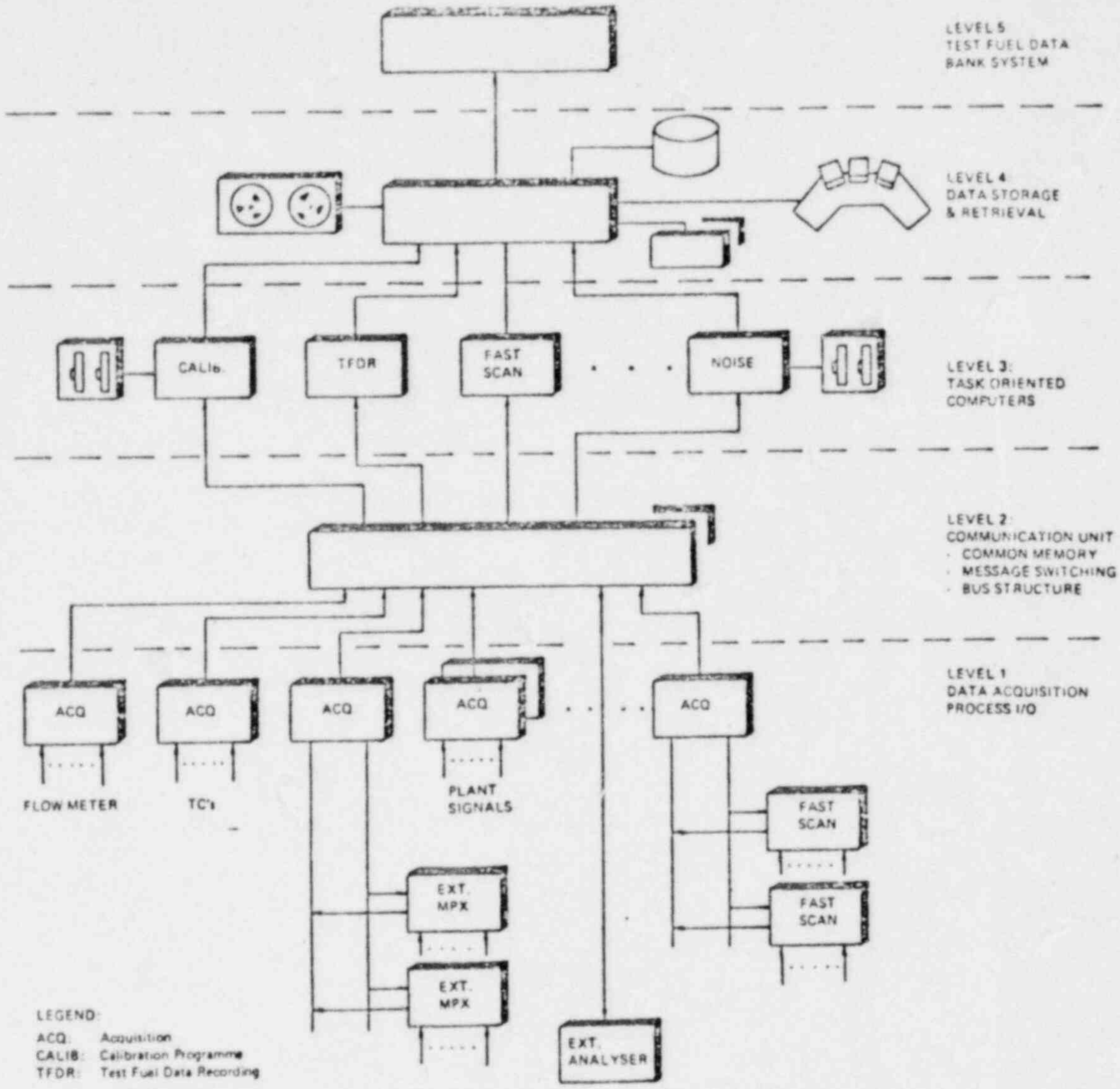


Fig. P-9. Function levels in a distributed data acquisition system

Table P-I. Signals Required for Each Main Function Block

Function	Number of Signals	Interval	Data Rate/Interval Bytes/Sec.
Test Fuel Data Recording	1,500 - 3,000	5 - 15 min.	2 - 20
Calibration Programmes	100 - 500	1 sec. - 5 min.	1 - 1,000
Fast Scan	100 - 150	20 msec.	10,000 - 15,000
Noise	5 - 15	10 msec.	1,000 - 3,000
Plant Data	100 - 200	10 sec. - 1 min.	3 - 40

for each function block, the interval and the calculated data rates per interval. The peak data rates are not estimated.

In addition to the above listed requirements the new system should simplify signal checking with different degrees of sophistication. Also alternative methods for scanning AC-signals directly into the computer without expensive conditioning electronics should be investigated.

It is supposed that serial communication links will be used between units on the different levels, and one should utilize fiber optics cables, which give a number of advantages compared with wires.

Assessment of Computer Structure

The multilevel structure as indicated in Figure P-9 must only be considered as a starting point. The units on level 1 can be located in a central computer room or they can be geographically distributed and located near the instrumentation to save cable and reduce installation costs. A "communication unit" on level 2 should perform the data transmission between units on level 1 and units on level 3 at a data rate required by the system. Considering the physical distances involved, a series transmission system with sufficient capacity seems most attractive.

The units on level 3 are task oriented computers, normally with limited storage capacity and simple operator communication. The units get their data from the "communication unit" at a rate required by the different tasks. Historical data are transferred to level 4, data storage and retrieval. Historical data can by request be transferred to the test fuel data bank system on level 5 either by batch transfer or by physical transport of magnetic tape reels.

Level 1 – Data Acquisition

The function modules on this level will be based on micro-computers equipped with necessary interface for process communication. All units on this level will mainly perform the same tasks which can be organized by a simple operating system (monitor). The intention is that each unit only will handle one type of signal transducer or an external device, as indicated in Figure P-9. Units on this level can also be used for control of loop experiments, diameter rig operation, power ramp function, etc. Each unit will have sufficient memory capacity for intermediate storage of scanned data.

Level 2 – Communication Unit

The unit(s) on this level will handle the communication between level 1 and level 3 with a throughput required by the total system. The selection of method will influence the structure of the whole system. There will not only be a matter of technical performance but also what is available on the market and to what price it can be implemented. Three different methods will be considered:

- the common memory
- message switching
- the bus structure.

The use of common memory as a "communication unit" in data acquisition and process control system has been studied and used at the Halden Project for several years. The system has several advantages, but also disadvantages, as all communication between level 1 and 3 (and vice versa) must go through "mailboxes" in common memory which present direct communication between units on different levels. To achieve the required high throughput, the existing common memory design must be modified, and since this also is a common resource high reliability technique must be implemented.

A message switching system (MSS) may consist of one or several dedicated computers, only used for handling the communication between units on level 1 and level 3. It is called a message switching system because e.g. a unit on level 3 only sends a telegram to the MSS and then forgets all about it. The MSS interprets the content, organizes the procedures for communication with units on level 1 and respond to the unit on level 3 when requested data are ready for transfer. The MSS itself may consist of several micro-computers in a bus structure, and if equipped with a shared memory, the advantages of the common memory structure is implemented in this structure too.

A bus structure may not differ much from the message switching system. Any unit connected to the bus can send messages to all the others, but since the bus is a shared resource, only one unit can use the bus at a time. The throughput in the system may be a problem, but with the technology developed today the bandwidth of several megabytes is usual, which is sufficient capacity for our purpose.

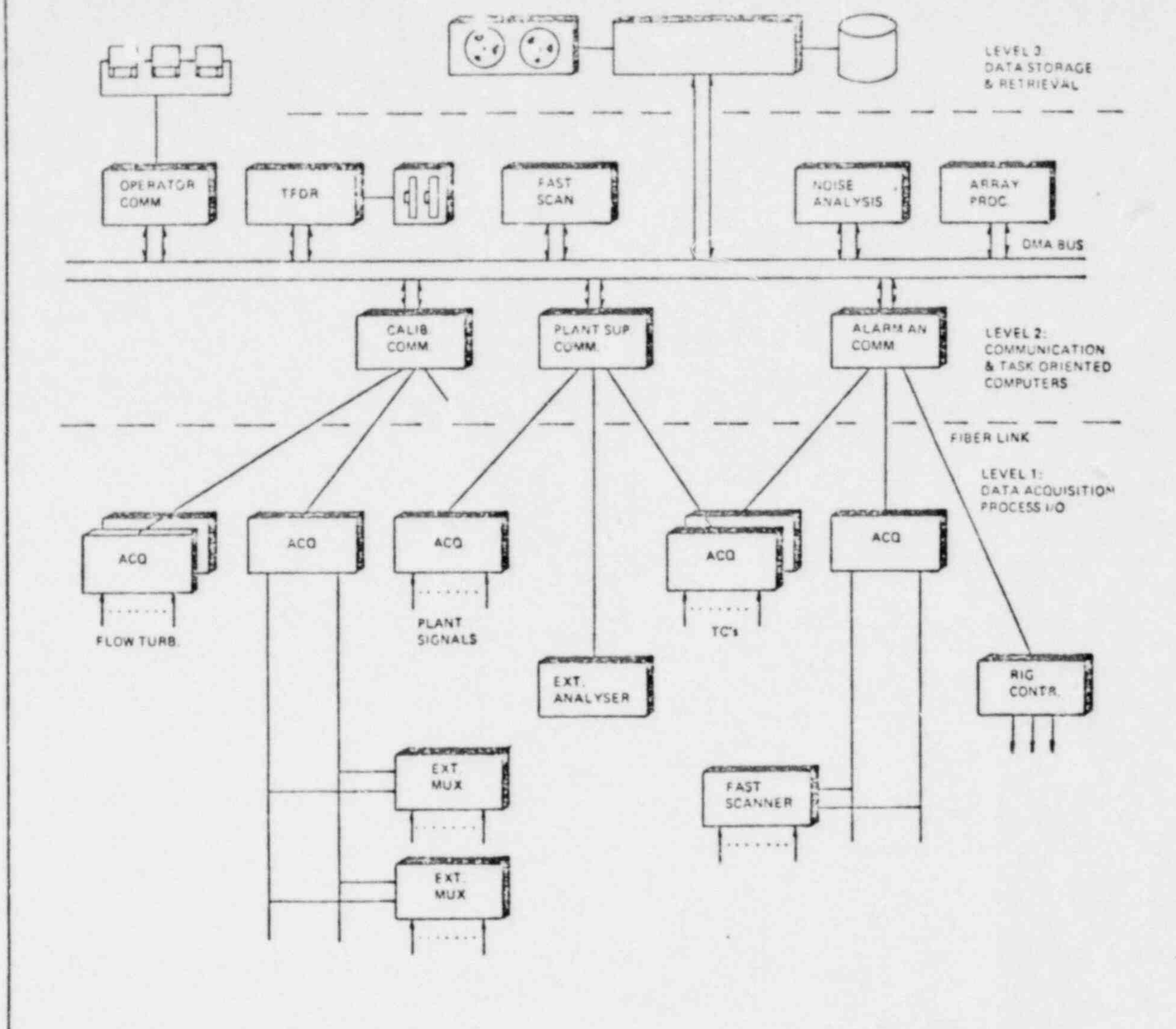


Fig. P-10. Proposed system for data acquisition and control

Alternative Structure

An attractive solution is proposed in Figure P-10. The communication units are integrated into level 2 and consist of microcomputers with two buses, a local bus and a global bus. All I/O-functions use the local bus, while high bandwidth communication between intelligent units is performed through the global bus. From the local bus, communication ports utilizing standardized protocols (HDLC, SLDC, etc.) and with bandwidth of 5 - 10 kbytes/sec., will be used for communication with level 1.

Level 1 – Data Acquisition

The function modules on this level will perform data acquisition as described above.

Level 2 – Communication and Task Oriented Computers

The computers on this level may also be based on 16-bits microcomputers and will to a certain extent be dedicated to perform special functions, as communication with level 1, Test Fuel Data Recording, (TFDR), Fast Scan, etc. Flexibility is obtained by loading other functions via diskettes. The unit which perform the Test Fuel Data Recording function, will request transfer of all test fuel signals at intervals of 5 - 15 minutes. Today the recording is signal oriented, but the intention with the new system is to make the recording oriented to each individual instrumented fuel assembly. The Fast Scan function requires a different number of signals (100 - 150) connected to various units on level 1, but with a repetition frequency of up to

50 Hz. Modules with special arithmetic processors used for noise analyses may be implemented.

A certain level of operator communication is necessary on this level. The degree of sophistication is dependent on the selected structure. With the bus structure as indicated Figure P-10, each unit can perform simple operator communication via the local bus, while more sophisticated operator communication covering the total system can be performed through a function module connected to the global bus.

Level 3 – Data Storage and Retrieval

The computer on this level must be equipped with a large storage capacity, magnetic tape stations, and equipment for presentation purposes. Historical data will be stored on discs or magnetic tape. Depending on the selected computer capacity, the Test Fuel Data Bank System may be implemented on this level, which in this case makes this level the highest in the hierarchy.

RGB – COMPUTERIZED OPERATION MANUAL FOR NUCLEAR POWER PLANTS. TWO APPROACHES

Introduction

The main goal of a reactor protection system is to actuate subsystems at the appropriate time and in the appropriate manner to perform protective actions in the case of an accident. Because of the great hazard-potential which a nuclear power plant represents, the ability to perform protective actions has to be available at any time. To achieve this high availability, reactor protection systems apply special design criteria like redundancy, diversity, etc.

The problem now is to know how failures in the safety system affect the overall availability and which measures are to be taken by the operator. The structure of a reactor protection system permits at least the occurrence of a single failure. Depending on the failure combination second failures may be tolerated for a limited time or not at all.

The Table of Second Failures. Approach No. 1

It has turned out that the operator of a nuclear power plant will not be able to estimate correctly the effect of a second failure to the safety system. He will not be able to do this task in an appropriate time without special aids.

All possible second failure combinations within the safety system (reactor protection system and connected systems) and the respective repair times ranging from unlimited to zero are listed in the so-called Table of Second Failures. This table is part of the Operation Manual and is voluminous because of the complexity of the safety system.

The RGB (Rechnergestütztes Betriebshandbuch)

As a first step of a joint project between the Österreichische Studiengesellschaft für Atomenergie Ges.m.b.H. (SGAE) and the Halden Project, a computerized operation manual for nuclear power plants has been developed. This RGB is based on the Table of Second Failures of a real nuclear power plant and has just been finished. It is now available as a pilot version which includes all essential features of the real system:

The operator communicates with the RGB by means of a keyboard to give in any changes of the status (devices failed or repaired) of the safety system. The RGB displays messages and information:

- permitted total repair time
- remaining repair time
- list of all actual failures
- system diagram with failed devices
- status of the safety system (survey table).

This RGB will also be very helpful for any chemical or industrial process which very often need safety and protection measures in addition to the operating control system.

Probabilistic Reliability Assessment. Approach No. 2

In continuation of the joint project between SGAE and the Halden Project, a new step has been done:

A "general RGB" using probabilistic reliability assessment methods is now in development and should later on be part of an overall operator process communcation system, not only for nuclear power plants.

This development is being done with a real reactor protection system as a case study. The completed items are as follows:

- A thorough literature search was done.
- A Design Basis Accident (DBA) was chosen: Loss of Coolant Accident (LOCA) inside the containment. LOCA is a very important DBA, and it requires five different protective actions, it represents well the entire safety system (reactor protection system and connected systems).
- The involved part of the reactor protection system was described by means of logic-diagrams thus defining the interfaces clearly.
- The involved electronic devices (pressure transmitters, alarm units, etc.) were identified and a functional description was given.
- A failure mode and effect analysis were performed, if there was no suitable information about a special device.
- The failure rates for different failure modes were evaluated, respectively estimated.
- The identification method of each failure mode was indicated.
- The down-time (identification time plus actual repair time) was estimated.

Outlook

The next step will be the application of the device-related data to the entire safety system. This will be done through fault tree analysis.

The result of the development, which will take account of software reliability criteria, should be an interactive reliability analysis of a safety system. This reliability analysis should consider the actual system status and display relevant data to the operator: identification of critical devices, permissible repair times, changed inspection times.