CA7803406

AECL-5916

ATOMIC ENERGY
OF CANADA LIMITED

L'ÉNERGIE ATOMIQUE
DU CANADA LIMITÉE

DIGITAL COMPUTER CONTROL ON CANADIAN NUCLEAR POWER PLANTS - EXPERIENCE TO DATE AND THE FUTURE OUTLOOK

by

A. PEARSON

Paper presented at the World Electrotechnical Congress

Moscow, USSR, June 21, 1977

Chalk River Nuclear Laboratories

Chalk River, Ontario

October 1977

ATOMIC ENERGY OF CANADA LIMITED

DIGITAL COMPUTER CONTROL ON CANADIAN NUCLEAR POWER PLANTS - EXPERIENCE TO DATE AND THE FUTURE OUTLOOK*

by

A. Pearson

* *Paper presented at the World Electrotechnical Congress, Moscow, USSR, June 21, 1977*

Chalk River Nuclear Laboratories
Chalk River, Ontario
October 1977

AECL-5916

Contrôle par ordinateur numérique des centrales CANDU - expérience acquise à ce jour et perspectives d'avenir*

par

A. Pearson

Résumé

Ce rapport passe en revue la performance du système de contrôle par ordinateur numérique de Pickering durant les années écoulées de 1973 à 1976. Cette évaluation est fondée sur l'étude des archives de fonctionnement de la centrale Pickering. On envisage l'architecture d'avenir des ordinateurs et les avantages pouvant découler d'une approche par système distribué. On donne également un aperçu des mesures prises actuellement pour développer ces idées plus avant dans le contexte de deux projets de Chalk River - REDNET, système avancé d'acquisition des données actuellement installé pour traiter l'information provenant d'expériences d'ingénierie effectuées dans les réacteurs NRX et NRU, et CRIP, un réseau de communications prototype utilisant la technologie de la télévision par câble.

* Rapport présenté au Congrès électrotechnique mondial tenu à Moscou, URSS, le 21 juin 1977.

L'Energie Atomique du Canada, Limitée
Laboratoires Nucléaires de Chalk River
Chalk River, Ontario

Octobre 1977

AECL-5916

ATOMIC ENERGY OF CANADA LIMITED

DIGITAL COMPUTER CONTROL ON CANADIAN NUCLEAR POWER PLANTS - EXPERIENCE TO DATE AND THE FUTURE OUTLOOK*

by

A. Pearson

ABSTRACT

This paper discusses the performance of the digital computer control system at Pickering through the years 1973 to 1976. This evaluation is based on a study of the Pickering Generating Station operating records. The paper goes on to explore future computer architectures and the advantages that could accrue from a distributed system approach. Also outlined are the steps being taken to develop these ideas further in the context of two Chalk River projects - REDNET, an advanced data acquisition system being installed to process information from engineering experiments in NRX and NRU reactors, and CRIP, a prototype communications network using cable television technology.

* *Paper presented at the World Electrotechnical Congress, Moscow, USSR, June 21, 1977*

Electronics, Instrumentation & Control Division
Chalk River Nuclear Laboratories
Chalk River, Ontario
October 1977

AECL-5916

INTRODUCTION

Digital computers have been a part of Canadian control and instrumentation philosophy since the beginning of the country's commercial nuclear program, and all our nuclear power generating units rely heavily on on-line digital computation for control and monitoring functions.

In the early sixties it was appreciated that the medium size digital computer then beginning to appear in data handling systems might be well suited for the data processing and control tasks facing nuclear power plant designers.

The manipulation of nuclear power plant data and the generation of alarm and operating records seemed to be a natural evolution, but the idea of using software to take part in the direct control of reactivity devices was controversial and in many countries remains so today.

Three steps were taken to introduce this new technology into the nuclear power industry; experimentation on a research reactor, use on a prototype nuclear power plant, and finally complete integration into the CANDU* system.

Preliminary experiments were conducted on the control system of NRU, a high power research reactor at the Chalk River Nuclear Laboratories of Atomic Energy of Canada Limited. The reactor was equipped with a conventional neutron flux controller but it suffered from a well-known shortcoming, the lack of proportionality between measured flux and reactor power. A digital computer was used to solve this problem. The true reactor power was computed from a series of thermal and hydraulic measurements and the error between this power and the required output was used by the computer to adjust the neutron flux setpoint.

*CANDU - Canada Deuterium Uranium

This experience was rewarding and produced an invaluable understanding of dynamic diagnostic programs. Routines were strategically embedded into the software so that any malfunction of the system would be recognized and annunciated and in some cases automatically corrected. Such reliable self recognition of a fault was to become basic to the approach that followed.

In parallel with this work, another step was being taken at the Douglas Point Generating Station, the 200 MW(e) forerunner of the CANDU system. A computer was introduced into the design to deal with a significant portion of the plant monitoring and logging task and also to control power distribution within the reactor core. For this latter function, the computer had several absorber rods under its direct control.

Since this was a pilot installation, it was not thought prudent to have vital control operations depend entirely upon a computer system. Consequently, the design allowed for operator intervention and continued plant operation in the event of a computer breakdown. It was of course recognized that this removed some of the incentive to provide prompt and efficient maintenance and it has been our experience that busy operating staffs have little time for new devices that are not clearly worthwhile. However, the computer was seen to be a powerful and useful operating tool and the necessary effort for its upkeep was forthcoming.

Faced with the design of the Pickering Generating Station, the first full-scale Canadian plant, the major decision to be made was not whether there would be a computer but rather to what extent would it become an integral part of the control and instrumentation system. Several points seemed clear:

- To justify the capital outlay for both hardware and software, the computer would have to deal with as many tasks as possible.

- Complete reliance on a computer system would impose stringent reliability requirements with availability targets approaching 99.95%.

- If critical control functions were included, Canadian reactor safety regulations would impose another requirement. It would be necessary to ensure that any malfunction requiring the action of an independent safety system to bring a process under control would not occur more often than once in three years.

- The provision of alternative backup systems had to be rejected, not only because of equipment costs, but also because of the double design effort.

Traditionally one had used redundancy coupled with majority logic to obtain high reliability and many such systems using analog equipment were giving good performance. However, to follow the same approach with computer-based systems was neither economically nor technically attractive.

PRESENT ARCHITECTURE

The equipment arrangement chosen to meet these requirements uses a dual computer configuration. Each computer contains the control routines for the vital loops and each contains an Operations Monitor, a self-checking feature that continuously surveys the computer's performance. Only one computer is actually controlling at any instant of time but should its

Operations Monitor detect a malfunction that cannot be readily corrected, control is immediately relinquished and the other computer takes over. In the unlikely event that both computers are unavailable at the same time, the plant is shut down.

The computers play a major role in plant control as indicated in Figure 1. Shown here are the Bruce Generating Station control loops and one of the computers. Sampling periods vary from a fraction of a second to several seconds and the loops range in complexity from having a single input and a single output to multivariable loops that control the power distribution throughout the reactor core. These loops can neither be left open for any length of time nor be effectively controlled by hand. Hence each of the control functions must be available in either one or the other of the computers if the plant is to operate.

Some automatic fault correction such as re-writing a program from a drum store to the core is permitted before taking the action to change over, but the number of attempts that can be made is limited.

Closed loop control is not the only task done by the computers. Included also are such utilitarian functions as data logging, generation of data displays, alarm annunciation, trip sequence recording, fuelling machine control and turbine run-up. All may not be completely duplicated since in some cases the degradation in performance that could result from failure of one of the computers can be tolerated until repairs are made.

EXPERIENCE

Considerable experience now exists with the dual computer arrangement. The four 550 MW(e) units at the Pickering Generating Station have accumulated more than 16 reactor years of operation,

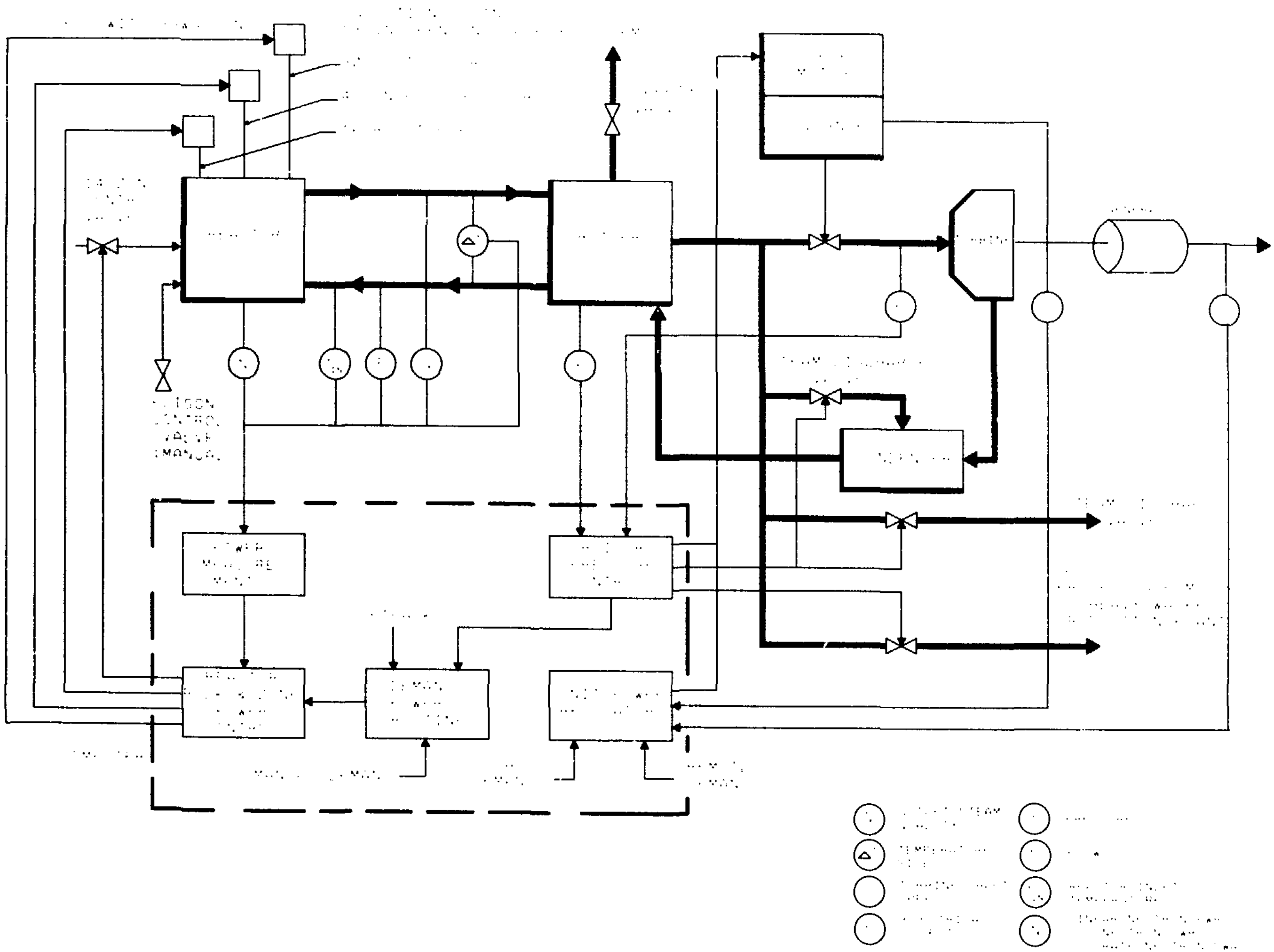

FIGURE 1 - COMPUTER CONTROLLED LOOPS
BRUCE GENERATING STATION

and experience is beginning to build up at the Bruce Generating Station where two of the four 750 MW(e) units have been operating since early in the year. Both Stations are operated by Ontario Hydro, the Utility that supplies electricity for the Province of Ontario.

The performance of the Pickering reactors has been exceptional and in 1976 the Station achieved a gross capacity factor of 87%, i.e. it produced 17,000,000 MW·h out of a possible 19,500,000 MW·h. This attests to the good performance of all systems, but since the purpose here is to get some insight into the operation of the digital computers, a more detailed examination is required to determine the extent to which lost output was attributable to their malfunction.

In view of the type of redundant system used, it is instructive to class failures into two groups:

- Control system malfunction due to simultaneous faults in both computers.

- Control system malfunction due to a fault in the controlling computer that is not detected by the Operations Monitor.

The first category of failures results from faults that in general have been anticipated by the designer; faults such as mechanical failure of peripherals, electronic component failures, parity errors and irrational inputs are in this class and they are detected by the on-line diagnostic procedures. The faults are rarely connected by a common cause but rather occur when one computer has already been shut down by a fault and is undergoing maintenance, and the controlling computer detects a malfunction and relinquishes control to a computer unable to respond.

To keep the probability of simultaneous failure low, i.e. to keep the system availability high, there are essentially only two directions that can be taken. One must keep the failure rate and time to repair as small as possible and one must take care in design and operation to ensure that common mode failures are eliminated.

In an attempt to quantify some of our experience, the Pickering Station's operating record for the past four years has been examined. The number of times both computers were out of service and the lost production charged to each outage were recorded and the results are shown in Table 1.

TABLE 1

PICKERING GENERATING STATION
COMPUTER SYSTEM OUTAGES

YEAR	NO. OF OUTAGES	LOST PRODUCTION MW•h	TOTAL PRODUCTION MW•h
1973	2	1,000	14,000,000
1974	2	21,000	14,000,000
1975	5	65,000	11,000,000
1976	0	0	17,000,000
	9	87,000	56,000,000

Thus the gross station output for the four year period would have been about 0.2% greater if the computer performance had been flawless.

An estimate of the availability of the system can be made if we assume lost production is directly proportional to computer outage time. This yields an availability of 99.89%, i.e.

$$\left(1 - \frac{\text{Lost Production}}{\text{Total Possible Production}}\right) \times 100\%$$

This is not strictly correct since a reactor outage may extend well beyond a computer outage because of xenon poison build-up or because of the scheduling of other maintenance work. However it probably represents a lower limit.

The second category of failures, those caused by faults that escaped the diagnostic procedures, was either not anticipated by the designer or was thought to be too improbable to consider. Redundancy of course, as applied here, does not improve this situation. Further examination of the operating record provides the information shown in Table 2.

TABLE 2

COMPUTER SYSTEM FAULTS
NOT DETECTED BY OPERATIONS MONITOR

YEAR	NO. OF FAULTS	LOST PRODUCTION MW·h
1973	5	7,000
1974	5	1,300
1975	1	0
1976	1	200
	12	8,500

These occurrences were distributed as follows:

- Software - four errors
- Hardware - five faults
- Operating - three errors

It is interesting to note that the rate of occurrence of this type of failure has decreased. This is to be expected since as faults are discovered, steps are taken to ensure that they do not reoccur or that they will come under the surveillance of the Operations Monitor.

It is also worth noting that the generation loss has been less with this category of failure than with the double failure. This is due in part to the rapidity with which the fault was discovered and the standby computer switched into service, and due in part to the fact that some of the software errors occurred during modification and testing and took place when the reactor was at low power.

A final point concerns the number of computer initiated control system failures that had to be terminated by the action of the safety system. This occurred three times.

The effectiveness of dual computers in improving availability is not known in quantitative terms; that is, there is no detailed record kept of every fault detected by the Operations Monitor. However there is no doubt that a single computer system would be at least an order of magnitude inferior and would not be tolerable.

FUTURE ARCHITECTURES

It is clear that the dual central computer approach has been successful and that it will continue to be installed in CANDU power stations for at least another decade. However advances in integrated circuit technology, minicomputers, microprocessors and peripheral equipment necessitated reappraisal of our concepts. Also becoming available are distributed architectures that promise to enhance further the usefulness of computers in process control applications.

The merits of these advances have yet to be clearly identified let alone realized in practice. Nevertheless these advances are bound to have an impact on future designs in that they will provide the tools most readily available to the designers of the day.

The introduction of novel concepts into a nuclear power system that is performing well is difficult to justify and other opportunities for a realistic trial are rare. We are therefore turning once again to the research reactor environment.

The high power research reactors, NRX and NRU, are used extensively for engineering experiments in support of the Canadian nuclear power program. Most of these experiments are associated with 'reactor loops' which are essentially single power-reactor channels operating under power-reactor conditions.

A centralized computer system installed nearly 15 years ago has been collecting and processing data from these facilities but a combination of increased workload and computer obsolescence is requiring a complete replacement.

The new system named REDNET for REactor Data NETwork will incorporate many advanced concepts providing they are not totally inconsistent with offering the experimenters a reliable data acquisition service. A distributed structure has been chosen for REDNET, the concept of which is shown in Figure 2. The fundamental property of a distributed system is evident. Intelligence or processing power is dispersed throughout a number of processors or throughout a mixture of processors and devices.

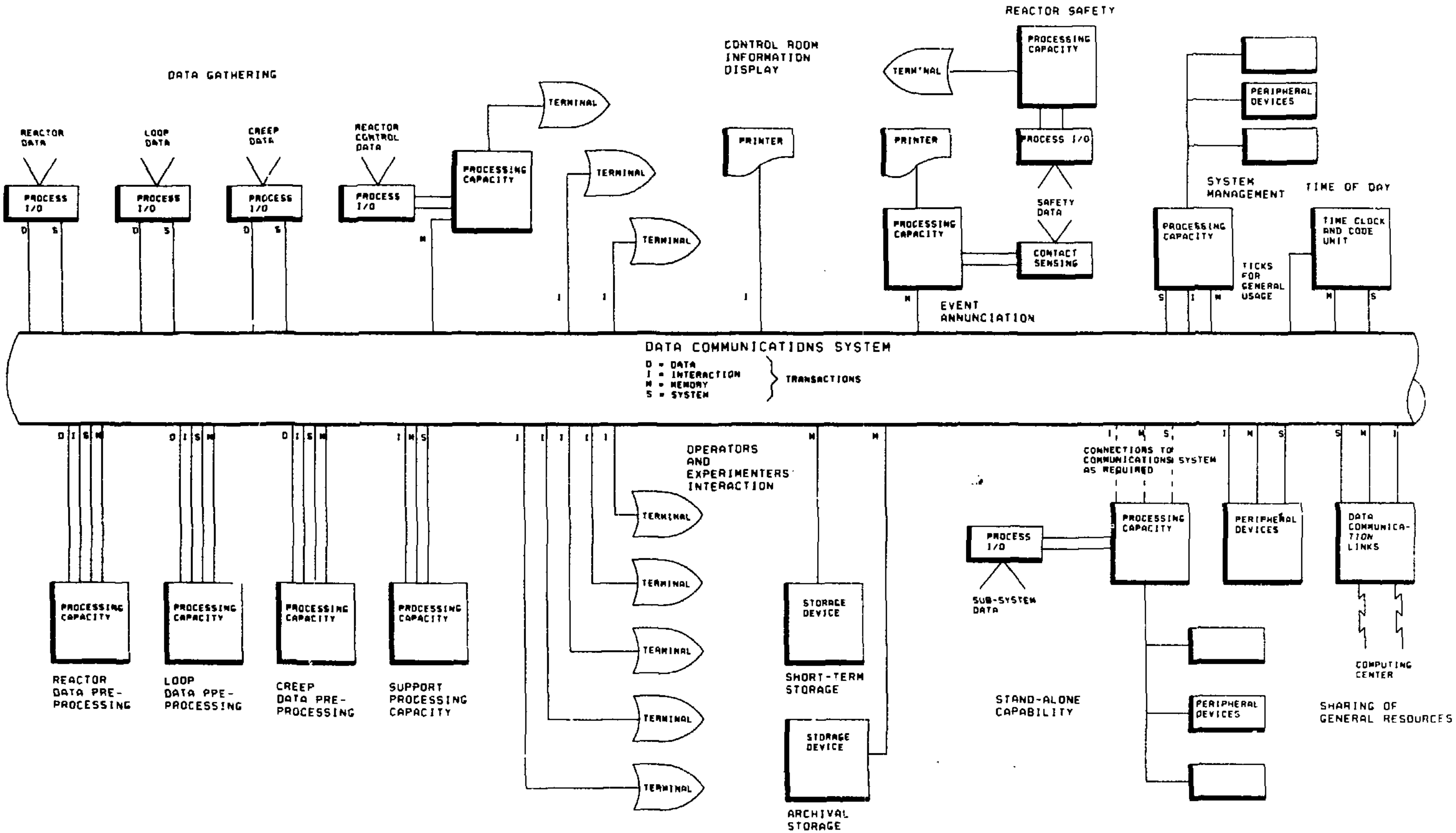

FIGURE 2 - THE REDNET CONCEPT

Several of the reasons for choosing a distributed structure are highly relevant to the design of a nuclear power plant:

- Ability to choose the level and location of intelligence so that an individual match can be made to each task.

- System design can be broken into readily manageable packages.

- Redundancy can be adjusted to meet the needs of a particular function.

- Components can be changed without affecting system operation or concept, thus providing some immunity to obsolescence or technology change.

- Ability to locate intelligence close to the source of data can result in simplified and less costly cabling methods.

The answers to some specific questions will be sought:

- What is the critical intelligence in a field-located device below which improved overall system performance is marginal?

- Can software be structured to permit dynamic system reconfiguration on component failure?

- Can processes communicate with each other transparently across processor boundaries regardless of physical location in the system?

- Can a fully integrated data base be achieved easily and be transparent to users of specific data without sacrificing data protection and integrity?

- Can the use of modern communication technology such as cable television techniques and networking concepts provide the reliable information transfer required in a distributed system?

The REDNET configuration will appear as shown in Figure 3. The following features can be noted:

- A network of five interconnected processors.

- Remotely sited preprocessors and controllers.

- The concept of sensors connected directly to a data bus (implying the development of a sensor interface able to provide address and digital information).

- No central or master processor is required to keep the system operational (the management system is for program development and upkeep).

- A multipurpose communication medium to handle the various transactions.

When a distributed system was first being considered as an alternative to our existing structure, it was realized that a reliable communications medium would be a key ingredient. A study of the communications market indicated that the manufacturers of cable television (CATV) equipment were concentrating on short-haul two-way digital communications systems for industrial use and had products suitable for the power plant environment.

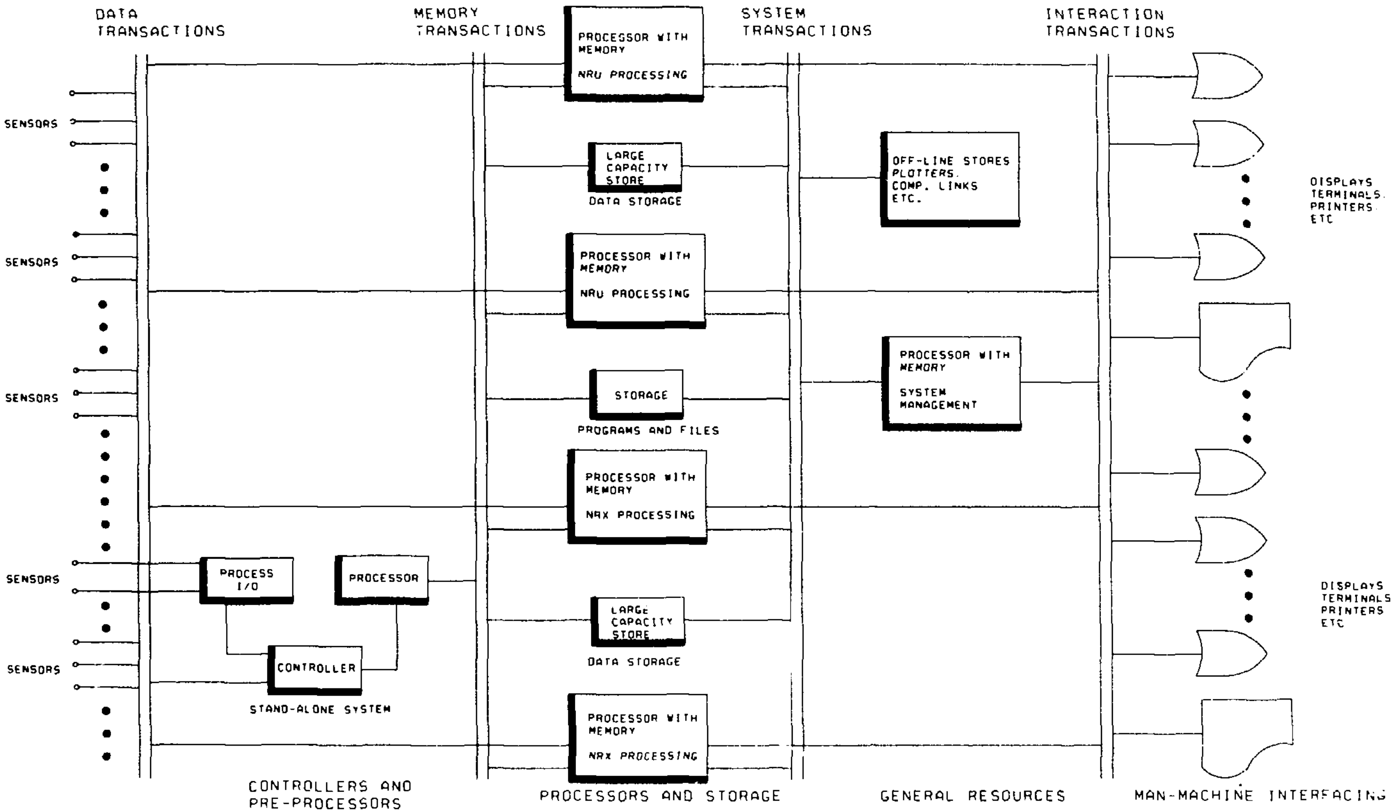

FIGURE 3 - THE REDNET CONFIGURATION

In order to obtain experience with this technology and to develop the protocols needed for dealing with a distributed data base, an experimental network was installed in our electronics laboratory. It links together several computer systems and fulfills a utilitarian role as well as being a development vehicle.

To simplify design, a concept of Levels and Channels was formulated to provide a modular solution adaptable to specific system needs.

A Level can have several Channels and is defined by a set of rules corresponding to a range of capabilities as follows:

- Level 1 is used for terminal support and for the control of information transport.

- Level 2 is used for batch transport of information files in the order of 10^5 characters. Transmission between system components is in bursts lasting less that 30 seconds each.

- Level 3 accommodates direct real-time interactions between system components by assigning Channels for several days.

- Level 4 is used to meet specific point-to-point hard-wired data link requirements. Channels are permanently assigned.

A broad-band two-way coaxial cable is used to distribute data between processors.

Sharing of the cable between Channels is accomplished by using Frequency Division Multiplexing (FDM). Separate 100 MHz bands are used for transmission in each direction on the cable. The bands are subdivided into sixteen 6 MHz "sub-bands" and each of these is in turn subdivided into twenty 200 kHz Channels. Thus 320 Channels may be installed in each direction. Currently each Channel operates at 48 kilo bits per second.

Access to the cable is gained by a tap and a FDM modulator-demodulator (i.e. a modem). The transmitter-receiver sections use phase shift keying and except for frequency assignments, are identical for all levels.

Except for Level 4 where linking is 'direct', all transmissions are routed through a controller installed at the head end of the cable.

Experience with this communication system has been good and uncorrected bit error rates better than 1×10^{-10} are attainable. Field experience will be forthcoming when similar systems are installed as part of the REDNET project.

SUMMARY

The digital computer has been fully established as an integral part of the control and instrumentation of the CANDU system. The dual central computer approach is performing well and will continue to be installed in CANDUs for at least another decade. The applicability of distributed systems to process control is not yet fully ascertained and the extent to which these new architectures will take over will depend to a large extent upon the success of the pilot systems that have been described here.

ACKNOWLEDGMENTS

I wish to thank Ontario Hydro for permission to use information extracted from the Pickering Generating Station operating records.

BIBLIOGRAPHY

A. Pearson, E. Siddall and P.R. Tunnicliffe, "The Control of Canadian Nuclear Reactors", 2nd U.N. International Conference on Peaceful Uses of Atomic Energy, Geneva, 1958, Vol. 11, p.372.

A. Pearson, "The NRU Computer-Control Experiment", Proceedings of a Symposium on Use of Computers in Analysis of Experimental Data and the Control of Nuclear Facilities, at Argonne National Laboratory, Argonne, Illinois, 1966, U.S. Atomic Energy Commission, 1967, p.21.

A. Pearson, "Computer Control on Canadian Nuclear Reactors", Atomic Energy of Canada Limited report AECL-3452, 1969.

E. Siddall and J.E. Smith, "Computer Controller in the Douglas Point Nuclear Power Station", IAEA Symposium on Heavy Water Power Reactors, Vienna, 1967.

J.E. Smith, "Digital Computer Control System Planned for Pickering Nuclear Station", Electrical News and Engineering, March, 1967, p.39.

E.M. Yaremy and D.E. Anderson, "Application of Pickering Experience to Future Canadian Nuclear Power Stations", Proceedings of a Symposium on Nuclear Power Plant Control and Instrumentation held in Prague, 1973, International Atomic Energy Agency, Vienna, 1973, p.187.

J.V.R. L'Archevêque and G. Yan, "On the Selection of Architectures for Distributed Computer Systems in Real Time Applications", Atomic Energy of Canada Limited report AECL-5583, presented at the Nuclear Science Symposium, New Orleans, October 1976.

A.C. Capel and G. Yan, "An Experimental Distributed System Development Facility", Atomic Energy of Canada Limited report AECL-5584, presented at the Nuclear Science Symposium, New Orleans, October 1976.

A.J. Stirling and J.V.R. L'Archevêque, "Potential of Remote Multiplexing Systems in Reducing Cabling Cost and Complexity in Nuclear Power Stations", Atomic Energy of Canada Limited report AECL-5700, 1977.

The International Standard Serial Number

ISSN 0067–0367

has been assigned to this series of reports.

To identify individual documents in the series
we have assigned an AECL– number.

Please refer to the AECL- number when
requesting additional copies of this document
from

Scientific Document Distribution Office
Atomic Energy of Canada Limited
Chalk River, Ontario, Canada
K0J 1J0

Price $3.00 per copy