IMPACT OF OPERATOR AIDS ON HUMAN FACTORS AND ORGANIZATIONAL STRUCTURE

by

Wm.J. Garland, System Analytics

and

W.F.S. Poehlman, BNF Consulting

A research report prepared for the
Atomic Energy Control Board
Ottawa, Canada

1992

IMPACT OF OPERATOR AIDS ON HUMAN FACTORS AND ORGANIZATIONAL STRUCTURE

A report prepared by Wm. J. Garland, System Analytics and W.F.S. Poehlman, B.N.F Consulting under contract to the Atomic Energy Control Board

ABSTRACT

This document reports on a recent survey of operator aiding expert systems which are in any stage of development within the Canadian nuclear industry. These operator aids have the goal of helping to create an environment where the operator can perform at the optimum capacity. This is to be accomplished by providing tools and techniques which reduce operator involvement in low level tasks (freeing up time for higher level cognitive tasks) and assist in information and knowledge manipulation so that high level tasks can be performed more efficiently.

Relevant attributes have been identified so that some measure can be made of the various attempts at building operator aids. These attributes are:

- Real-time data acquisition
- Real-time analysis
- Asynchronous activities
- Distributed architecture
- Inferencing capability
- Disparate knowledge bases
- Multidisciplinary agents
- Different mental models
- Overall control strategy.

The APACS project, funded by PRECARN (a PRE-Competitive Applied Research Network funded by industrial partners and the federal government) is a large project to provide an operator aid for the feedwater system. It will be generalized for other nuclear and non-nuclear systems in the future. It is largely traditional in approach (bottom up and detailed). The project has many good features but the one word that comes to mind to describe it is `ponderous'. Little if any consideration of human factors is being built into the schema; it is based on the engineer's functional approach to systems. APACS is not slated for station implementation; rather, it will be installed at a simulator.

AECL CANDU has no active projects of note at the moment. However, the control room design team is playing an important role in vetting R&D ideas coming out of Chalk River Laboratories (CRL) and other COG players. Their focus on CANDU 3 places them squarely where the action will be when the next station is designed. Some of CRL's current thinking on the Operator Companion came from work done at AECL CANDU in the 1980's.

CRL has developed the SES prototype Operator Companion but the prototype is not currently being pursued. CRL has no architecture under development since they are currently focusing on the HF aspects that are implementation independent. Clearly, this is a leading group in the HF area and in COG related Instrumentation and Control work in general. This group has pulled together the main thrusts of the literature and brought it to a focus with the Functional Design Methodology (FDM). So far, much of the work is in the `ideas' stage. CRL ideas are based on a top down approach and are comprehensive but, in our opinion, could stand to be more closely linked to the stations and designers. The Operator Companion includes disparate Knowledge Bases (KB) and inferencing.

Pt. Lepreau NGS personnel have installed a Gateway system to provide real-time station data to plant personnel. The setup uses ethernet but there is no blackboard (BB) or any attempt to provide a coordinated intelligence. The key words are incremental, methodical, and practical. Useful things are being done today to help the technical support teams conduct routine and tedious tasks more efficiently and effectively. Operator aids are limited to enhancing functionality in displays and related devices in the control room.

McMaster University is poised to move along with Pt. Lepreau. Some interesting non-nuclear ES's have been successfully prototyped and a cohesive group of researchers has been assembled.

The University of New Brunswick has an active AI group with a number of relevant ongoing projects in AI topics related to nuclear power but no Human Factors focus and no `systems' per se have been attempted.

Maritime Nuclear has developed an excellent architecture for real-time distributed control. They are working closely with Pt. Lepreau.

Indications are that, at the Ontario Hydro nuclear stations, no projects are ongoing or planned except for those conducted through COG. Most nuclear plants are moving towards improved data handling in general and operating procedure assistance in particular. CRL and Pickering NGS are working on a COG funded critical safety parameter advisor system (CSPAS). It appears to be a very localized system but human factors are being considered.

In addition to the APACS project, PRECARN is involved in the IRIS / IGI / IntelCAD groups based for the most part at Simon Fraser University. These works are in a different sphere altogether (autonomous robots). There seems to be no near or medium term overlap with the nuclear industry. The problem of interfacing between the operator's model and the physical processes (the basis for the engineer's mental model) is being directly addressed by the IGI group.

None of these projects yet live up to the ideal: a communication highway (like ethernet) which allows peer to peer interaction, involves distributed processing, permits multiple mental models, has no implied or enforced control structure and permits parallel and concurrent problem solving. Development continues.

We found that the people involved in the various projects were interacting with some of the other projects. However, no one is linked to all the projects. The COG Working Party 16 membership provides a forum for most of the nuclear related activity but the PRECARN related work, the COG related work and the university based work are all being conducted in an insular fashion, to everyone's loss. Some mechanism needs to be established to open up communications. That is our key recommendation.

TABLE OF CONTENTS page

LIST OF FIGURES

LIST OF TABLES

A. INTRODUCTION

As energy sources of electric power turned nuclear, the required control technology increased in complexity. Through necessity, straightforward analog systems yielded to the more capable digital circuitry. This allowed improved measurement functionality and remote telemetry. What had originally been, in the first generation, a one-sensor-one indicator philosophy, rapidly grew, forcing the operator into information overload, particularly when the process came under stress conditions. In the second generation, such improvements as attribute-based displays of information and alarm filtering became the norm in an attempt to reduce operator loads. These assistance techniques, however, could not compensate for further increases in sensor density and complexity. Thus, in the third generation, the inclusion of computer-based on-line operator aids is being pursued. Recent findings seem to indicate that, compared to the U.S.A., Canada either leads the way or is rapidly gaining ground in adopting new technology in such areas as technology insertions (retrofit) in existing plants and new enhancements beginning at the design level [BHA91].

The objectives of this work are to explore and assess any current development activities within the Canadian nuclear industry that are focused on operator aids based on expert systems; especially, to identify and assess the practicality of any developments of decision support expert systems for control room operators.

The report takes the following form:

Section B -- The key themes are identified and developed, providing an overall assessment and integration of ideas.

Section C -- Centres of activity involving research projects and programmes are examined and reported with a view to significant operator companion development. This forms the bulk of the material gathered.

Section D -- A summary of selected readings extracted from pertinent papers and books are provided in this section.

Section E -- Concluding remarks are made from the thoughts developed in the previous sections.

References follow.

For assistance in understanding the jargon, a glossary of terms (vocabulary) is included. A list of acronyms and an index are provided for reader convenience.

This report would not be complete without presenting a self-assessment of where the authors feel their knowledge has been advanced in the pursuit of this fact finding mission -- after all, this information is seen and developed through their faculties.

Although we were aware of various "hot-spots" of activity throughout the country (Eg.Federal Centres of Excellence, PRECARN, Simon Fraser University, etc.) where relevant work is being carried out, it was only in discussions with the involved individuals that details provided insights. For instance, it is somewhat obvious, in hindsight, that researchers deeply involved in providing useful operator aids seek to focus on the process operator's view and not the standard engineering view which centres on the process function. Such engineer/operator distinctions and other human factor considerations are extremely germane to developers but have only been appreciated by the authors during the course of this work. We accordingly believe that our original superficial knowledge has actually been a boon to this work as we can say that our approach to information gathering has been totally unbiased. However, our own local efforts at operator companion development [MAH92, LIN92, POE89, BER89a, GAR89, GAR90, GAR92] in microcosm has given us a unique opportunity to appreciate the work of others. Thus, this work has resulted in a steep learning curve for our personal advancement in the field. We believe we are, therefore, uniquely positioned for this work under the categories of competence and objectivity.

The authors wish to report on one prevalent thread that seemed to run adjacent to our investigations. As with most works in progress, the project administrators worry that licensing and safety aspects have not been fully explored, and that partial information could be taken out of context. We hope we have not given substance to their fears. We did find that individuals on the working level to be quite open and forthcoming with answers to our questions. Note, however, that our probes were on the general level, not on technical implementation level.

B. DISCUSSION

We entered into this investigation with the belief that the relevant issue confronting the operator of a nuclear power plant is information and task overload. This has been confirmed in our discussions and literature survey. The operator is not being properly utilized if the appropriate information (as opposed to data) is not available at the right time or if the operator is overly occupied with mundane tasks. Consequently, the timely and correct response is not assured since information is not readily available in a form conducive to assimilation for the problem at hand and/or the operator is busy implementing procedures that needlessly require far too much of the operator's attention. The operator needs information on alarms, plant state, historical data, diagnostics, design info, station logs, and procedures in a context sensitive manner. And many activities could be automated without the operator losing control.

The goal, then, of the various developers is to rectify the current operator situation by creating an environment where the operator can perform at the optimum capacity. This is to be accomplished by providing tools and techniques which reduce operator involvement in low level tasks (freeing up time for higher level cognitive tasks) and assist in information and knowledge manipulation so that high level tasks can be performed more efficiently. Perhaps new heights could be attained.

In the pursuit of this goal, it is important to identify the relevant attributes of the situation so that some measure can be made of the various attempts being made on operator aids. Our suggested attributes are:

Real-time data acquisition

Any operator aid of value must contain knowledge of the plant that is up to date. `Real-time' can only be defined in terms of the information in question, ie., real-time pressure data probably requires updating every second or so, whereas refuelling history data requires updating only 20 or 30 times a day.

Real-time analysis

Reasoning in real-time and reasoning about real-time data is in its infancy. Yet it is a central element needed in an operator aid. It is not just a question of being fast. Rather, bounding the solution time is the issue. Can a sufficiently good solution be found within the time required? The goal here is to `sufficify' rather than `optimize'. A real-time system is one that reaches its conclusion before the real system does.

Asynchronous activities

Plant operations are diverse and multifaceted. But, in addition, they are asynchronous in nature. It would be to some advantage (modelling fidelity) to emulate this attribute but it is not essential.

Distributed architecture

Again, the breadth and depth of plant operations dictate that no one aid can ever hope to encompass the needs of the operator. Rather, many small aids need to be developed in a coordinated manner. The individual aids are of considerable utility by themselves but the true power of the paradigm comes when the various individual aids cooperate in problem solving (concurrent engineering).

Inferencing Capability

The hallmark of an operator aid that rises above a `tool' is the existence of some level of higher level functioning. This is usually manifested through the presence of an agent that worries about the `how' after being charged with the goal. This is accomplished by consulting a knowledge base. Most AI or ES based systems today distinguish between the knowledge base and the inference engine.

Disparate knowledge bases

In the diverse environment of the nuclear plant, the consultation of many disparate knowledge bases

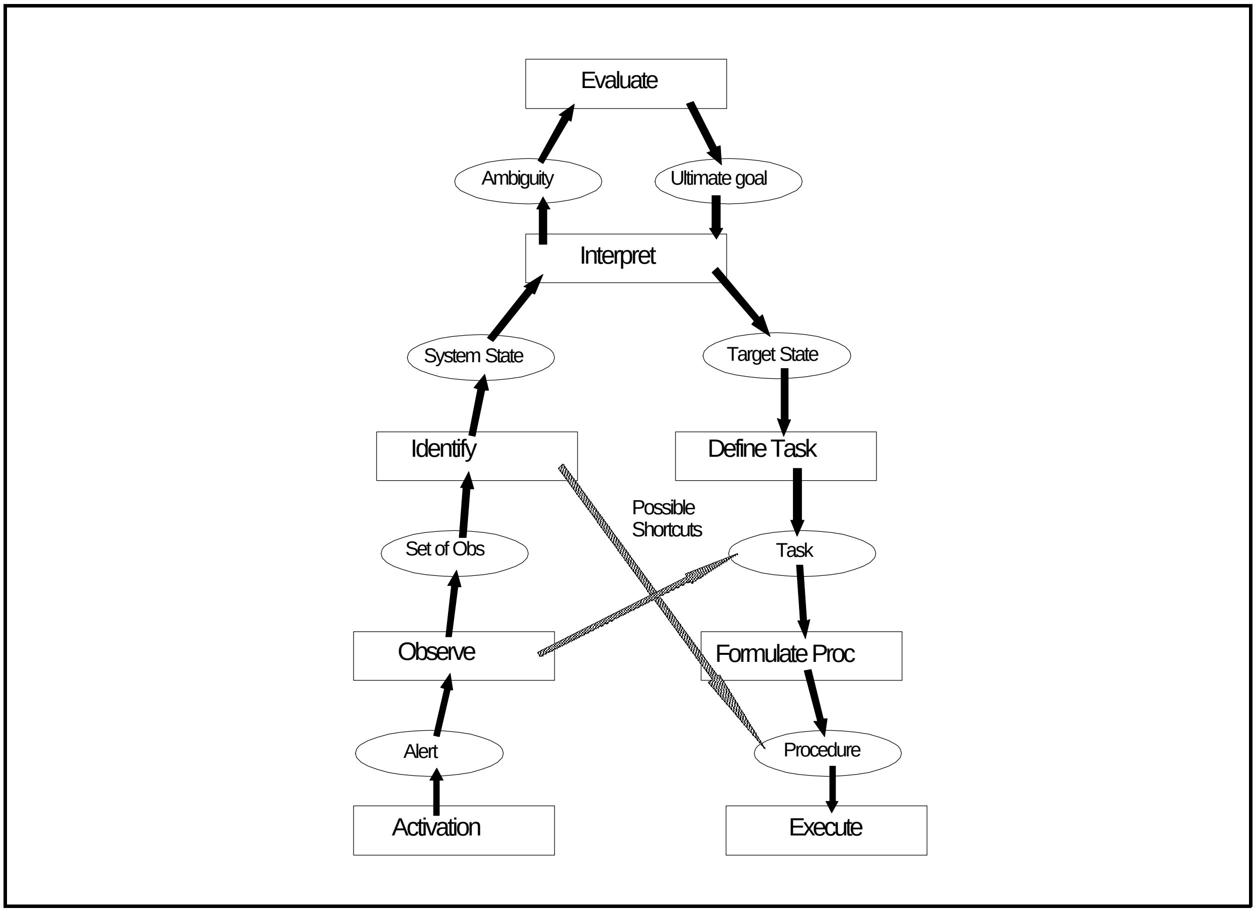

Figure B-1 Rasmussen's Problem Solving Schema (Simplified).

involving the many plant components and plant views is required for problem solving. The various agents will operate (inference) on these knowledge bases in diverse ways.

Multidisciplinary agents

Expertise from many disciplines are brought to bear in the problem solving process. This is another essential feature of a well rounded aid. At the moment, only the human operator is capable of multidisciplinary integration and this will not change in the foreseeable future.

Different mental models

This refers to the different problem solving strategies of the technician / operator vs. the engineer / designer. This is elaborated below.

Overall control strategy.

This refers to the machine-centred approach vs. the human-centred approach. This is discussed next.

Past work has been machine-centred. This is a term used by Bernard [BER92] to describe the overall design philosophy of building tools that put the machine in control, that is, the computer program tells the operator what to do and when to do it. Contrast this to the human-centred approach wherein the operator is the primary source of intelligence and is in control. In the human-centred approach, the operator uses the computer programs as tools. The computer may monitor and annunciate but it is the operator who pilots the operation, using the tools when

necessary and as necessary. The paradigm shift is profound. Bernard notes that the machine-centred approach is now considered inappropriate.
Closely linked to the machine-centred approach is the mental model used based on functional decomposition. That is the mental model of the designer or engineer as developed in Rasmussen's book [RAS86]. The engineer poses: How does the plant work? What is broken? What measurements must be taken? What is the functional decomposition of the plant? How do the parts interact? How can one simulate it? This `mechanology' led to alarm based annunciation, control room displays and controls grouped by system (functional decomposition), sensoritus, and information glut without enhanced knowledge. The view of the plant taken was that of the design engineer - this is how and why it works - here are all the details, etc. Ergonomics was commonplace but limited to `knobology'. Make the knob bigger, use a red light here, etc. This kind of thinking leads to products like the VCR - machines with attractive lines, buttons that `feel' right, on-screen programming and 64 button remote controls - full featured functionality from the comfort of your armchair. And unusable for anyone except a technoid! Problem solving strategies here relies on a deeper than average understanding and use of specific knowledge. Contrast this to the more typical user.

The user, it is now recognized, is the operator, not the design engineer. The operator's mental model of the plant is closer to that of a technician - the plant is a collection of many systems, most of which are treated with generic algorithms for fault diagnosis and treatment of event symptoms, irrespective of the system in question. Rasmussen's figure (reproduced in part in Figure B-1) illustrates this generic algorithm. In fact, ALL problem solving is covered by this figure but the technician employs strategies and tactics that do not rely heavily on a detailed knowledge of system and component behaviour. That is, short cuts to Rasmussen's full solution path are taken. This is a form of shallow reasoning and is good most of the time. This is not to say that the operator does not have a detailed knowledge of the systems and components. He or she indeed does. It is simply that the problem solving scheme is not as system dependent as for the engineer. We have a hint here of why typical AI implementations haven't worked as well as hoped. Past AI models have tried to emulate the engineer. But these models are largely based on IF-THEN rules, ie, heuristics. The mapping from the engineering mental model to the rule base is so bad as to be termed inappropriate since typical AI does not involve significant high level integration. The operator's mental model (short cuts and heuristics) map to the AI paradigms very well. This emphasis on the difference in mental models between operators and engineers overstates the case. Operators are perfectly capable of using the full strategy when needed and engineers often use shortcuts. However, the caricatures of the engineers mental model and the operators mental model are useful for argument's sake.

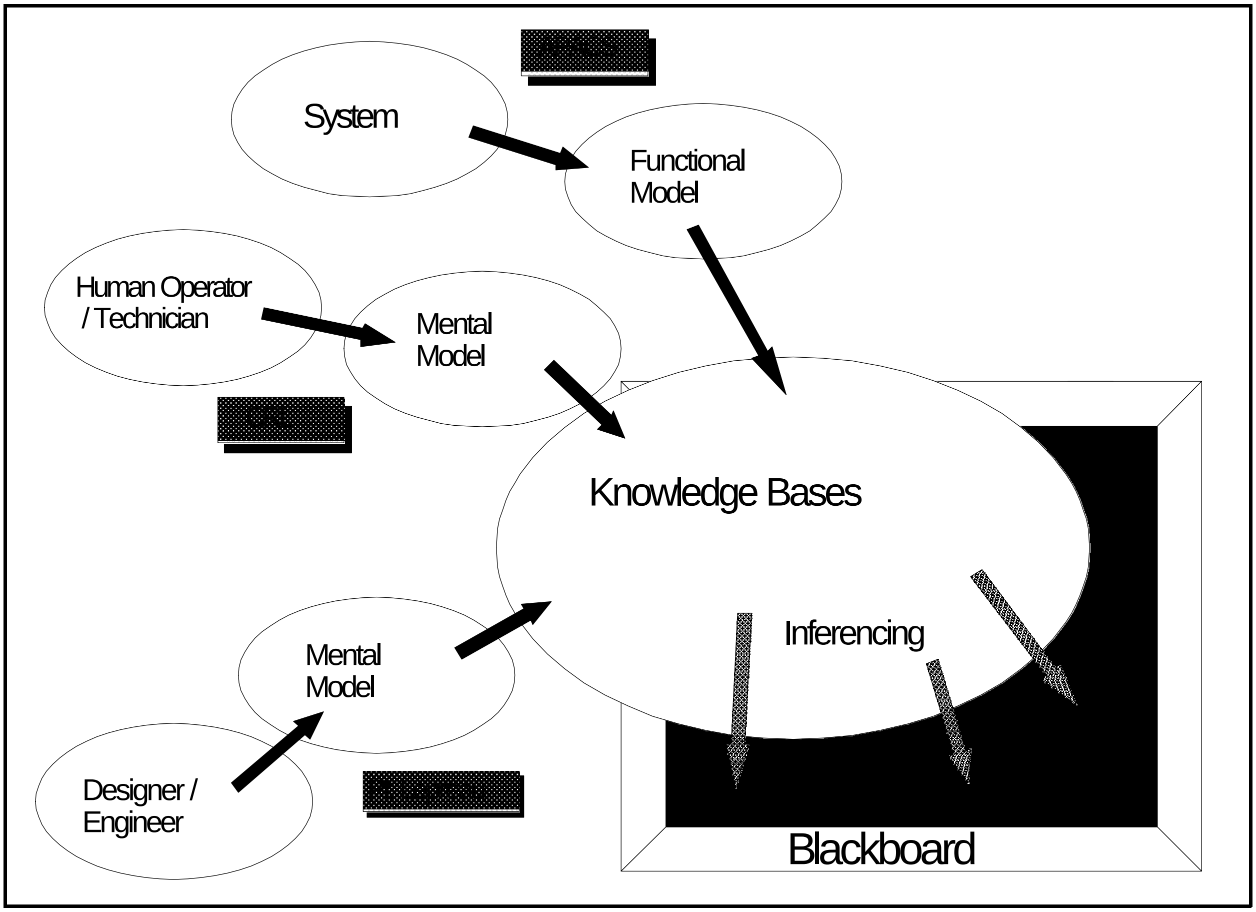

Figure B-2 Various Mental and Physical Models.

Another point of note is the fact that expertise is composed of both knowledge and the ability to manipulate that knowledge. It has been observed and is widely recognized in the literature that it is the vast knowledge-base that exemplifies the expert rather than raw inferencing capability. Take an expert and place him or her in novel territory and you get decidedly non-expert behaviour. Take a genius and place him or her in the expert's territory and you do not get expert behaviour. The reactor environment is a case in point; operator actions require mostly procedural knowledge and moderate inferencing capability. The knowledge-base (composed of facts and heuristics) is then very important. The knowledge-base is necessarily system or component specific and it is unlikely that a general knowledge-base can ever be conceived. This leads to the paradigm of message passing via a blackboard or some other mail handling system as a means of allowing disparate agents (models or codes or humans, etc.) to interact. Knowledge-base design is, then, more about the design of the blackboard - the format and content of the messages being processed. It is at this level that one is concerned about how the operator or engineer interacts with the system being controlled. The result of this is that the objects being manipulated (the knowledge base) need to be defined before they can be manipulated (by the inferencing or procedural engine). But how we define these objects will depend on the mental model chosen. This leads to a dilemma: the system needs to be functionally decomposed along the lines of the physical or engineers mental model, whereas, this is an inappropriate model for the operator. No-one to date has demonstrated a schema to solve this dilemma. Figure B-2 illustrates this point and shows where the various projects are with respect to this particular characterization.

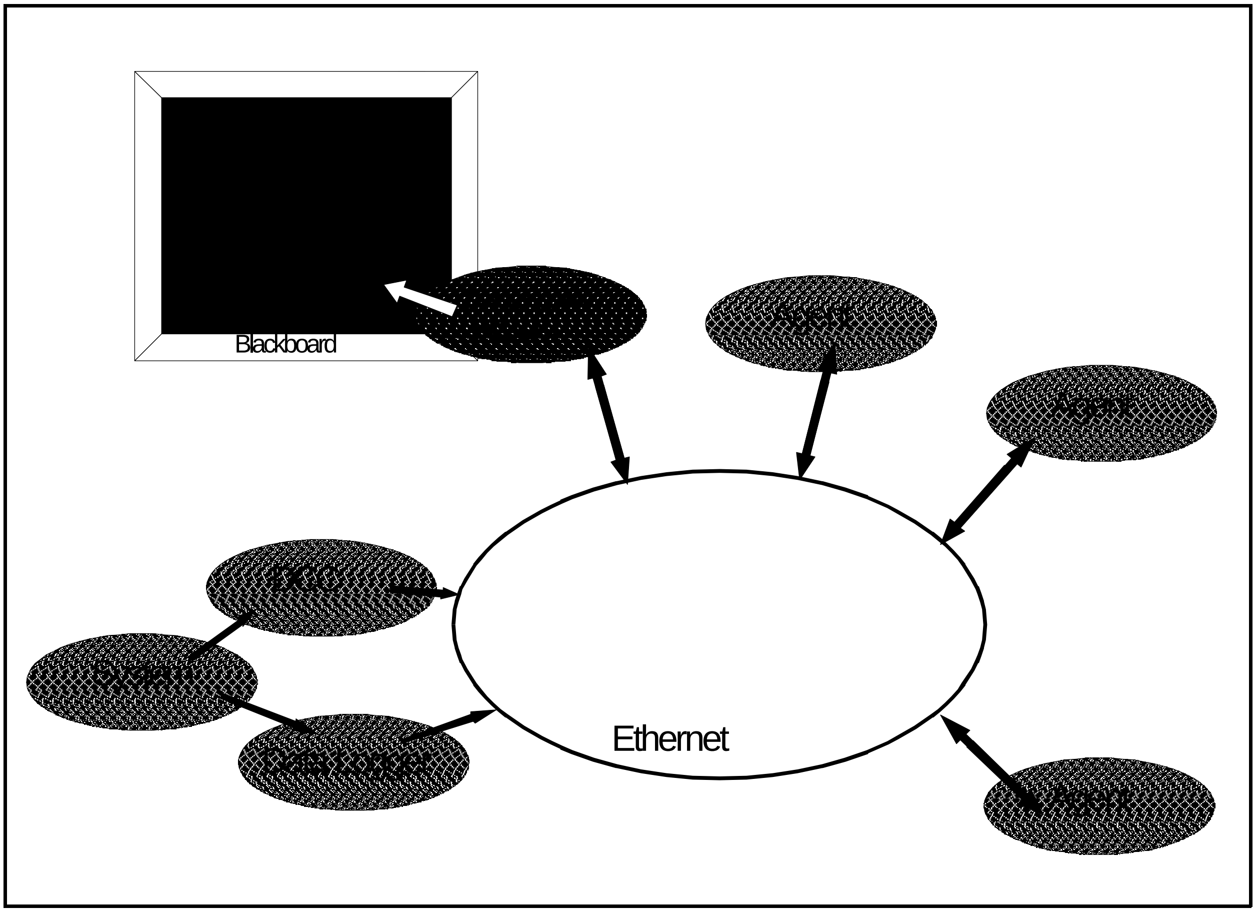

Figure B-3 A Generic and Idealized System.

The ideal environment would include a communication highway (like ethernet) to allow peer to peer interaction, involve distributed processing, permit short circuit heuristics (as per Rasmussen), have no implied or enforced control structure (orthogonal to the control plane) and permit parallel and concurrent problem solving. Figure B-3 illustrates an implementation that has the required generality and flexibility. No specific control structure is implied; it is simply a fast, inexpensive message passing medium that is available today. Note that incoming plant data is broadcast to all agents but the primary direct users of the plant data are the data acquisition agents and the BB. All agents are free to interact with other agents. (the BB and the DA's are just specific instances of agents).

Table B-1 Current status of the projects surveyed.

CENTRES of ACTIVITY	R-T DA	R-T ANAL	ASYNCH	DIST'E D	INF CAP	DISP KB	MULTI DISP	DIFF MENTAL	HUMAN CENT
APACS	√	√	√	√	√	X	X	X	X
CRL	√	X	√	√	√	X	X	√	√
NB POWER	√	X	√	√	√	√	X	X	√
OADCS	√	X	√	√	X	X	X	X	X
PICKERING	√	X	X	X	X	X	X	X	√
OPCOP	X	X	√	√	√	√	X	√	√
IGI	X	X	X	X	√	√	X	√	√

LEGEND:

R-T DA: Real-time data acquisition
R-T ANAL: Real-time analysis
ASYNCH: Asynchronous activities
DIST'ED: Distributed architecture
INF CAP: Inferencing capability
DISP KB: Disparate knowledge bases
MULTI DISP: Multidisciplinary agents
DIFF MENTAL: Different mental models
HUMAN CENT: Human-centred or Machine-centred

A capsule summary of the main projects on operator aids is given in Table B-1. It is clear from the table that no one project does it all. Nevertheless, each project has something to offer. In the following we take a look at each project, addressing each of the attributes mentioned earlier and try to put each project into some overall perspective.

C. CENTRES OF ACTIVITY

1. PRECARN Consortium

PRECARN Associates Inc. is a PRE-Competitive Applied Research Network funded by industrial partners and the federal government. The intent is to provide a means of conducting applied research at the pre-competitive stage, that is, at a stage and level that industry normally could not maintain because the lead times are too long to be considered profitable. The industrial orientation also makes the research untenable for the normal university avenues. Some 30 industrial partners are currently associated with PRECARN. Yearly funding is roughly $20 million. PRECARN was formed in 1987 and opened a competition in 1988. Of the 30 or so submissions, 6 projects were funded. These are (from the information kit received from PRECARN in May, 1992):

APACS - discussed elsewhere in this document

IGI - discussed elsewhere in this document

ARK - Autonomous Robot for a Known Environment - for the nuclear industry but not an operator aid.

TDS - Telerobotics Development System - robotics project - not an operator aid

KAD - Knowledge-Aided Design - design oriented - not an operator aid

CORFFA - Control of Robots for Future Applications - another robotics project that is not an operator aid.

In addition, PRECARN manages one of the Federal Centres of Excellence, IRIS, the Institute for Robotics and Intelligent Systems. There are 22 projects within 3 areas within IRIS. Please refer to the IRIS section for further details.

Contact:

JEAN-CLAUDE GAVREL (613)727-9576 FAX: 727-5672
PRECARN GAVREL%A1.AT0TT2.NRC.CA@VM.NRC.CA
30 COLONNADE ROAD
NEPEAN, ONTARIO
K2E 7J6

2. Advanced Process Analysis and Control System Project (APACS):

Project: APACS
Sponsor: PRECARN
Participants: Ontario Hydro, CAE Electronics Ltd., University of Toronto (U of T), Shell, Stelco, Hatch Associates.
Site: Ontario Hydro (Toronto), CAE Electronics Ltd. (Montreal).
Time Frame: Phase I May 90 - December 91, Phase II underway.
Project Scale: $9.5M total over 5 years.
Objectives: Phase I Proof of concept prototype, Phase II Expansion of Prototype.
Methodology: Monitor, interpret, simulate and diagnose plant operations.

Attribute Summary:

Real-time data acquisition: This is one of the strong points of APACS.
Real-time analysis: The diagnosis agent is novel and is still in the early stages of development. There is good potential here.
Asynchronous activities: Yes, but no attempt is made at using new solution paradigms like blackboards or concurrent problem solving. Rather, a traditional approach is used wherein proper sequencing must be observed.
Distributed architecture: Yes, the problem domain is appropriately decomposed in a manner amenable to their distributed architecture.
Intelligent inferencing: Yes, the agents employ high level reasoning, especially the Diagnosis agent.
Disparate knowledge bases and inferencing: Because only one view is taken (the engineer's view) and because the knowledge bases are likely little more than databases, diversity in form and function is not evident here. There seems to be only one database per se although multiple copies can exist at any one time. The diagnosis agent is distinct in form from the other agents but it too lives off the common database.
Multidisciplinary agents: No, the focus of the current project is a relatively simple fluid system (fluids plus control). As such, it does not require a multidisciplinary approach. There is nothing in the model to prevent extension when it is warranted.
Different mental models: No, only the engineer's viewpoint is considered. See the comments below.
Overall control strategy: For the most part, a machine-centred approach is taken. Little thought has been given, apparently, to human factor concerns. This is slated for the distant future.

Contacts:

```
MIKE BENJAMIN                592-1997
ELECTRICAL & CONTROLS ENGIN. FAX:592-2009
ONTARIO HYDRO
700 UNIVERSITY AVE
TORONTO, ONTARIO
M5G 1X6

JOHN MYLOPOULOS
DEPT OF COMPUTER SCIENCE
UNIVERSITY OF TORONTO
TORONTO, ONTARIO
```

BRYAN KRAMER 978-7330
DEPT. OF COMPUTER SCIENCE FAX: 978-1455
UNIVERSITY OF TORONTO EMAIL: KRAMER@AI.TORONTO.EDU
6 KING'S COLLEGE ROAD
TORONTO, ONTARIO
M5S 1A4

Comments:

Ontario Hydro is the primary investigator in a PRECARN project called Advanced Process Analysis and Control System Project (APACS). They are teamed up with CAE in Montreal and the University of Toronto.

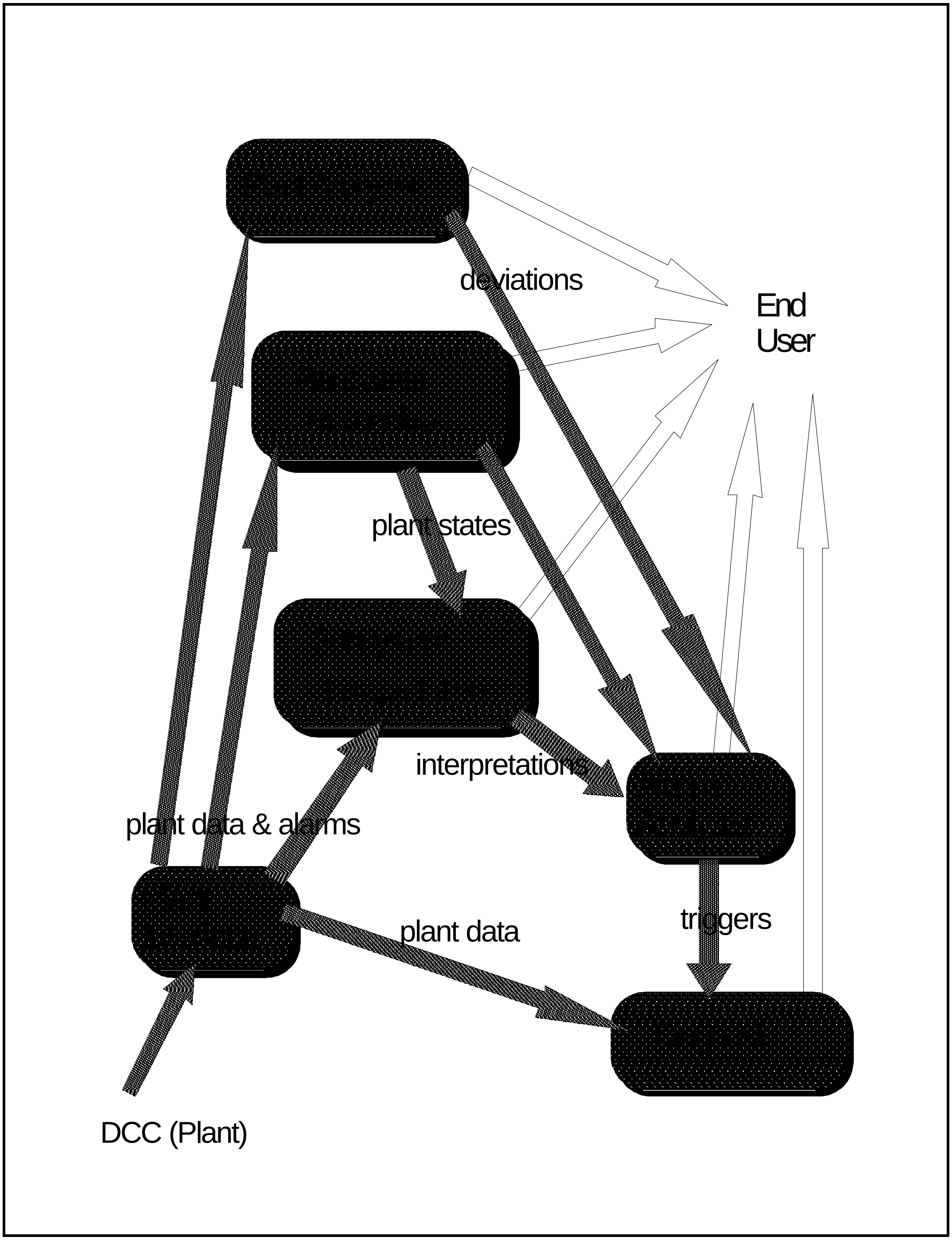

Figure C-1 APACS Functional Relationships

The APACS project is composed of several components, each performing a specialized task, as shown in Figure C-1 (adapted from PRECARN information). Currently a plant simulator running on a VAX 785 provides mock plant data to a Digital Control Computer (DCC) identical to the Bruce B station DCC. In this manner, mock station data are available to all components (via a distributed database). This plant simulator is simply referred to as `the plant'. The modular architecture permits the ready substitution of one plant data source for another, be it stored histories, better simulators, or whatever. Both OH and CAE have extensive experience in this area. Relevant consistency checking of data is done by the DCC, thus ensuring that an alarm and the signal that the alarm was based on are consistent within the DCC. But corruption of the data may occur during transmission from the DCC to the databases, or perhaps the various analyzers may have a bug that corrupts the data at the point of use. Thus local consistency checks seem to be called for. Mike Benjamin stated that the APACS project does not incorporate local checking at this time.

The Plant Analyzer (PA) being developed at Ontario Hydro runs on the VAX 785, providing simulation, tracking and parameter adjustment. Its scope is the feedwater system. Future plans include the inference of variables that are not measured. The PA provides information on plant deviations to the Alarm Analysis component. The overall approach is to use the plant data measurements as the boundary conditions for the models contained within the PA. In this manner, the PA is, to a large degree, always in lock step with the plant. Deviations in the model output (derived data) and plant data that are not used as boundary conditions can only be attributed to model error, measurement error or plants events (degradation of system components or an unpredicted shift in plant state). This parallels the current thinking at McMaster.

The Plant State Recognition (PSR) component is being developed at CAE under the real-time Expert System shell from GENSYM Corporation, G2, running on a UNIX machine. Its scope is the overall plant but the model is focused on providing information relevant to the feedwater system. The component provides the plant state (or context) to the Alarm Analysis component and the Subsystem Interpretation component.

The Subsystem Interpretation component is also being developed at CAE under G2 running on a UNIX machine. It's scope is the feedwater system and provides specific knowledge to the Alarm Analysis (AA) component.

The Alarm Analysis component is another CAE / G2 component. It assimilates information from the plant and the previous components to advise on the alarm state, triggering the Diagnosis component.

The Diagnosis component is being developed at the University of Toronto and is, to date, uncoupled from the other components. This is the only research component in the project. The primary task is to provide a framework for real-time diagnosis. Traditional rule or model based approaches do not reason appropriately on time series data. University of Toronto is investigating a somewhat novel approach that uses heuristics to provide the search tactics for (what appears to be) a strategy modelled along traditional forward and backward chaining paradigms. The heuristic approach is discussed in the PRECARN workshop handout.

It was noted [POP92] that the recent PRECARN-IRIS workshop on APACS showed that the system being developed lacked robustness.

OH expressed concern over the proprietary nature of the APACS project and with ensuring that the work not be taken out of context. Mike Benjamin noted that this is exploratory work and there is no direct link to the stations. The simulator provides the mock plant data and the longer term plan is for installation at the Western Nuclear Training Centre (WNTC). APACS is a test-bed for ideas only. The plan is to make the component implementations non-nuclear and generic. Stelco and Shell are considering prototype development. This is one of the reasons why the feedwater system was chosen as the system to be investigated; it is relatively simple (perhaps too simple, in retrospect) and non-nuclear. The past experience of the participants with plant simulators is a key component in the success of the project to date. Knowledge of simulators and associated technologies allows the ready development of plant event generation and real-time data handling in a multitasking, asynchronous, distributed environment. Phase I of the project is complete and a workshop was held in March, 1992. Phase II is in the early stages.

On the subject of Human Factors (HF), Mike Benjamin stated the focus was not on HF for Phase I; rather the emphasis is on modelling, simulation, data passing and other generic features that have to be developed irrespective of Human Factors aspects. OH has considerable knowledge of the operator, the operator's environment and the needs of the operator; these are being taken into account. First principles (flow models, engineering equation sets, etc.) are required if the functional behaviour of components and systems are to be captured. The alternative is an unworkably large set of rules giving the causal links. Thus first principles are being applied to a great degree in the APACS project, leading to a functional decomposition similar to the view of the design engineer, not the operator. The design view and operation view are quite different from each other but both are equally correct. It is recognized that the two views must be reconciled at some point but this has not yet been addressed in the APACS project.

The APACS project has a functional decomposition (see Figure C-1) similar to Figure B-3. The difference is that in the APACS project the inferencing process is linear or sequential in nature in that all roads lead to their diagnostic unit. The arrangement of Figure B-3 is less structured. APACS is bottom up and detailed. The project has many good features but the one word that comes to mind to describe it is `ponderous'. Little if any HF consideration is being built into the schema; it is based on the engineer's functional approach to systems. APACS is not slated for station implementation; rather, it will be installed at a simulator. As such, it could impact on operator training in the foreseeable future. The APACS approach runs the risk of not being accepted by the operators. The AECB should establish and maintain contact to be kept apprised of significant events. This is probably best initiated through PRECARN, the funding agency.

3. AECL CANDU :

Project: Operator Companion
Sponsor: CANDU Owners Group (COG)
Participants: AECL.
Site: Mississauga, Ontario.
Time Frame: Ongoing.
Project Scale: Several man-years.
Objectives: Provide next generation control room designs.
Methodology: Interact with current users and developers.

Attribute Summary: Not Applicable

Contacts:


```
JOHN PAUKSENS                (416) 823-9040
PROCESS CONTROL
AECL CANDU
SHERIDAN PARK RESEARCH COMMUNITY
MISSISSAUGA, ONTARIO
L5K 1B2

JAD POPOVIC                  (416) 823-9040 X4709
CONTROL ENGINEERING          FAX:823-6120
AECL CANDU
SHERIDAN PARK RESEARCH COMMUNITY
MISSISSAUGA, ONTARIO
L5K 1B2
```


Comments:

AECL CANDU was taking a lead role in the Operator Companion concept in the mid 1980's. Figure C-2 illustrates the architecture (adapted from [LUP89b]). In 1988 a session at the CNA/CNS conference dealt with control room design. The operations people present were in the process of retrofitting Bruce and Pickering. They had a lot to say about the matter and suggested that some R&D be conducted. This led to the work that CRL (Lawrence Lupton) is doing via COG incentives (see the CRL section for details). AECL CANDU remains involved in operator aids through Working Party 16 of COG. Their role is primarily advisory at the moment as they are not actively pursuing the implementation of any operator aid system. Their past activities are outlined in [POP88]. Overall, their approach to the issues are in line with the CRL group.

Bob Moore, AECL CANDU, is involved in Link Analysis. This is a non-computer based analysis of the operator activities in the control room from the layout point of view. He listed the many types of operators: first operator, second operator, shift supervisor, and others. Each have distinct roles and must be integrated into the design and layout of the control room. Bob acts as a reviewer / filter for the concepts that Lawrence comes up with; the focus is on feasibility and implementability primarily for CANDU 3 related projects (the current platform for new ideas). Bob reinforced the emerging notion that the operator does not need tools that tell him there is an SDS1 incident or whatever. He already has that type of information. He needs help with information management. This is the notion of the human-centred approach rather than the machine-centred approach previously discussed.

Scott Malcolm, AECL CANDU, mentioned that much of the current methodology under investigation in the nuclear industry has its roots in the `standards' literature of the military and aerospace industry. The functional analysis aspect is just one part of a larger process. The military model starts with the concept and provides the methodology for an iterated refinement and gives form to the function. The US military information is readily available for free.

He also noted that the Functional Design Methodology (FDM), currently in vogue, is a misnomer; the scope of FDM as defined by CRL is really much broader, covering everything from concept to installed verification and validation.

See references [POP88, POP92] and Section D for more information.

AECL CANDU has no active project of note at the moment. However, the control room design team is playing an important role in vetting R&D ideas coming out of CRL and other COG players. Their focus on CANDU 3 places them squarely where the action will be when the next station is designed. Much of CRL's current thinking on the Operator Companion came from work done at AECL CANDU in the 1980's.

4. Chalk River Laboratories (CRL):

Project: CRL
Sponsor: COG, AECL
Participants: HMSD group at CRL
Site: CRL.
Time Frame: Ongoing.
Project Scale: 11 full time people.
Objectives: To improve human performance through interfaces, annunciation systems and procedures that better match human capabilities to the tasks to be performed.
Methodology: Functional Design Methodology (FDM).

Attribute Summary:

Real-time data acquisition: The SES prototype had a small real-time data acquisition, proving the concept.
Real-time analysis: No real-time analysis was attempted.
Asynchronous activities: Yes, but the prototype had only one advisor agent and one data acquisition agent. This can hardly be a good test of scaling issues.
Distributed architecture: Yes, a LAN was used.
Intelligent inferencing: Yes, a rule based ES shell was used (NEXPERT Object). This is somewhat slow and limited shell for real-time inferencing. The rule base was small.
Disparate knowledge bases and inferencing: No, the scale was too small.
Multidisciplinary agents: No, again the scale was too small.
Different mental models: The operator was considered and the model was based on functional decomposition, but there is little evidence that the mental model of the operator was considered. Again, the scale was too small to see the effects of the tougher issue of providing an integration of intelligent agents operating on different databases and using different paradigms.
Overall control strategy: The human-centred approach is taken since the advisor operates as backup for the operator and can be controlled by the operator.

Contacts:

LAWRENCE LUPTON (613)584-3311
HUMAN-MACHINE SYSTEMS DEVELOPMENT FAX:584-4024
CHALK RIVER LABORATORIES LUPTONL@CRL.AECL.CA
CHALK RIVER
ONTARIO
K0J 1J0

Comments:

Lawrence Lupton is Section Head, Human-Machine Systems development (HMSD), Instrumentation and Control Branch at Chalk River Laboratories. His group of 10 professionals consists of a mix of engineers, computer scientists and psychologists. In the late 80's, AECL pursued the role that AI (notably ES) could play in providing operator aids. One of the outcomes was a prototype operator companion for the Slowpoke Energy System (SES). This prototype is illustrated in Figure C-3. Historical roots lie with the Operator Companion of AECL CANDU, previously illustrated in Figure C-2. There have been a number of changes since then, primarily due to the realization that AI, per se, is not the panacea for operator aids and also due to funding considerations. By mid 89,

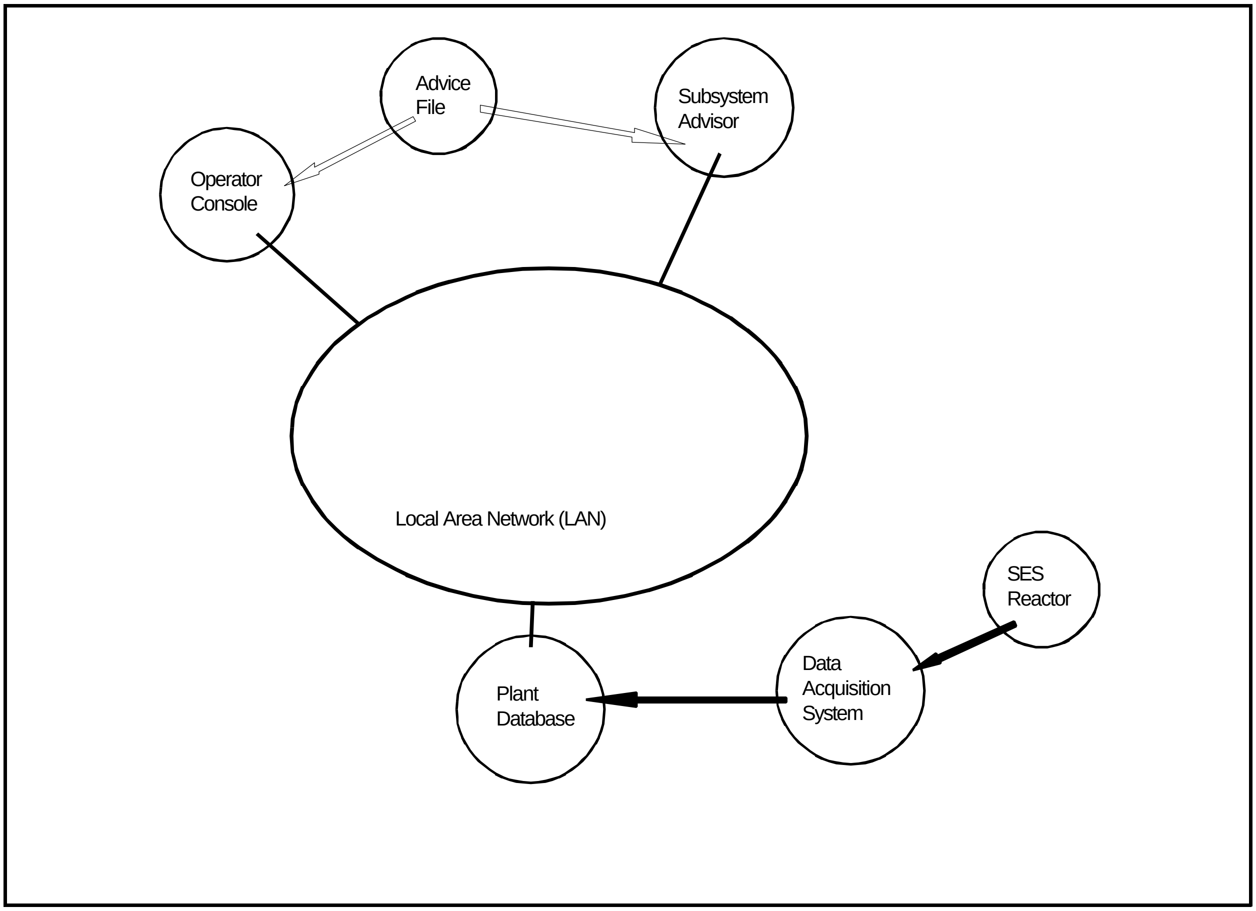

Figure C-2 Overview of the SES Prototype

the focus had changed from AI R&D to CANDU3 alarm enunciation, emergency operating procedures and functional design methodology support. The onset of COG funding in April 90 saw the formation of the current group with its emphasis on human factors aspects. Ed Fenton of Ontario Hydro, is the chair of Working Party 16 (Instrumentation and Control) to which Lawrence reports.

Lawrence emphasized that his programs are focused on R&D. The programs are discussed in [LUP89a, LUP89b, LUP90, LUP92a, LUP92b and LIP92c] (summarized in Section D, these are a `must read'). The prime objectives are to improve human performance through interfaces, annunciation systems and procedures that better match human capabilities to the tasks to be performed.

CRL has contacts with:

University of Toronto, Dr. Paul Milgram, Dr. Mark Chignell and Dr. Kim Vicente, Industrial Engineering
Ecole Polytechnique - Jean-Marc Robert, Industrial Engineering
EPRI
Japan
Norway
DCIEM
PRECARN (APACS and IGI projects)
Hydro Quebec - Radu Manoliu, Head Office
transmission line ES, no nuclear programs

Sources of funding were identified as:
COG (majority)
AECL Research - Advanced CANDU (minority)

The major clients of Lawrence's group are Ontario Hydro, AECL CANDU, Hydro Quebec and New Brunswick Electric Power Commission.

The Pickering NGS CSPAS project was mentioned (examined under a separate heading).

Dr. Paul Milgram, of the Department of Industrial Engineering at the University of Toronto is working with Lawrence Lupton of CRL on a virtual reality project. The project is in the early stages.

The SES prototype Operator Companion was a relatively successful prototype but it is not currently being pursued. CRL has no architecture under development since they are currently focused on the HF aspects that are implementation independent. Clearly, this is a leading group in the HF area and in COG related Instrumentation and Control work in general. This group has pulled together the main thrusts of the literature and brought it to a focus with the FDM. So far, much of the work is in the `ideas' stage but some good working prototypes were developed in the past. CRL ideas are based on a top down approach and are comprehensive but, in our opinion, could stand to be more closely linked to the stations and designers. The Operator Companion includes disparate knowledge bases and inferencing. CRL's current work brings in the features that the SES Operator Companion lacked, namely the human factors.

5. Pt. Lepreau Operator Aids:

Project: Pt. Lepreau Operator Aids
Sponsor: NB Power
Participants: NB Power, University of New Brunswick, McMaster University, and Maritime Nuclear.
Site: Pt. Lepreau.
Time Frame: Ongoing.
Project Scale: Plant-wide, small system aids.
Objectives: Computer automation of routine tasks that currently require manual attention.
Methodology: Methodically and incrementally implement improvements, always keeping the operators' needs in mind.

Attribute Summary:

Real-time data acquisition: Yes. The Gateway system is an excellent approach.
Real-time analysis: No attempt has been made here at all.
Asynchronous activities: Yes, this is inherent in the model.
Distributed architecture: Yes, this too is inherent.
Intelligent inferencing: Yes, the various separate agents developed so far involve some higher level inferencing but no integration is attempted.
Disparate knowledge bases and inferencing: Yes, but no integration is attempted.
Multidisciplinary agents: No.
Different mental models: No.
Overall control strategy: Human-centred.

Contacts:


```
BRYAN PATTERSON              (506)659-2220/2102
NEW BRUNSWICK ELECTRIC POWER COMMISSION
PT. LEPREAU NUCLEAR STATION
P.O. BOX 10
LEPREAU, N.B
E0G 2H0
```

Comments:

John Anderson of AECL CANDU was stationed at Pt. Lepreau from July 88 to Jan 89. He mentioned that the Secondary Side Chemistry System is a system that the operators don't want to control and hence is a good choice for operator aid development. In addition to reviewing the emergency operating procedures, he also worked on Loss of Instrument Air. Apparently, the operators get lost when performing this procedure and many bodies are needed to carry out the procedures. A student put the code on the station computer and John did the documentation. Errors were found in the procedures. John left before the job was completed and tested. NB POWER has been working with the University of New Brunswick for the past several years on Artificial Intelligence (AI) related projects. In late 1990, McMaster contacted Bryan Patterson upon the recommendation of John Anderson, AECL CANDU.

In conversation with Bryan Patterson, it was reported that real-time data is currently available to the technical units at the station via a LAN (GATEWAY). Software has been developed, for instance, to download chemistry data for the condensate-feedwater train and display it on a PC at the engineer's desk. The engineer monitors this data, looking for indications of condenser tube leaks.

Bryan Patterson noted that the technical support staff are faced with many relatively small tasks that require a fair amount of involvement, yet could be automated and are excellent candidates for ES implementation. Major event diagnosis is not perceived to be as urgently needed as the above since mechanisms are in place to diagnose the events and/or treat the symptoms. It's the smaller, more numerous events that would give the best return on investment. NB POWER figures that the 80-20 rule applies here: 80% of the job could be handled by a 20% investment in effort to cover the `normal' tasks. For example, many heat exchangers (HX) need to be monitored over long periods to watch for degradation in performance. The majority of these HXs involve single phase fluids only, which are easy to model and characterize. Thus, it would not be a difficult task to put an automatic monitoring system in place. This would free up precious time and head space for the engineer, time that would be better spent on two phase HXs and other tasks that require the higher level thinking of a human expert. In March 1992, significant progress was reported [KIN92].

Other possible projects cited were:

(1) Identify the cause of a reactor trip. Quick determination is important in order to recover from a spurious trip within the Decision and Action (D&A) time of 30 minutes, thereby averting the high cost (~$500k) of a 40 hour outage.

(2) Determine the adequacy of the reactor heat sink. Heat sink integrity is priority 1 for the operator.

(3) Evaluate the required trip protection for various flux shapes.

(4) Regional Overpower Protection (ROP) calibration.

(5) The use of time derivatives in setting margins.

(6) Off-normal operation, ie. shutdown monitoring.

(7) Event recognition.

(8) Reconstruction of electrical schematics from wiring diagrams.

(9) D_2O inventory estimation.

(10) HX performance (as mentioned above) based on some terminal point data and some expertise. This is to cover fouling and other key performance parameters. Currently, NB POWER is collecting data at a 6 second frequency. The reactor cooling water (RCW) system is a prime candidate for investigation.

(11) Programmable Digital Comparator: PDC1 SDS1 and SDS2 computer logic card failure diagnosis. Maintenance of these cards is a problem costing about $50k/yr. (WFSP subsequently supervised a Master's thesis on this topic.)

(12) Generic diagnosis tool. This would hopefully evolve as individual targeted projects progress.

(13) Condenser tube leak detection. The procedure to monitor and detect tube leakage is in place, as discussed above. However, the procedure could easily be automated using an expert system. McMaster University is currently involved in this project (discussed separately).

(14) CSP advisor. Currently, no attempt is made at event diagnosis in support of response to CSP (critical safety parameter) trends and alarms. Also, CSP trends are not augmented with inferred parameter estimation. For instance, Heat Transport System (HTS) subcooling at the pump suction could easily be calculated from measured pressure and temperature and the Net Positive Suction Head (NPSH) of the

primary pump can then be calculated, giving the margin to pump cavitation.

Bryan Patterson noted that operators hate to call in the technical unit, especially at night or the weekend. Thus, it would be desirable to provide as much aid as possible to the operator. But the support must be developed in cooperation with the operators and the technical units if it is to be useful.

Since that time, many projects have been contemplated and much has been accomplished. Bryan Patterson has adopted the KISS approach, much to his credit. In his view, there are many small considerations that can be made for the operator that go a long way to improving operator performance. Attention is paid to making routine tasks less tedious and more convenient for the operator to perform. The basic philosophy is to methodically and incrementally implement improvements, always keeping the operators' needs in mind. It was also noted that the operator is not prepared to abdicate control to the machine; reasoning systems must do as good as or better than the user. Operators will have no problem with systems that have deterministic reasoning and logic that can be understood and documented, and that the operator can be trained on.

Currently, the following off-line information items (flat files) are available:

fuel channel history
electrical load lists
instrument air load lists
computer I/O lists for the DCC
shift logs
field logs
control room logs
Review Record of Operator Documentation (RROD).

This information is available on a plant-wide information storage and retrieval system. Each is not integrated with each other, although there is no doubt that such a system would be desirable. The inventory system is being renewed; the Work Order System is the next to be re-engineered. These systems are the basis for integration, having at their root an Equipment Record System.

Other like-minded (KISS, piece-wise refinement) implementations are:

Fuel channel selection: A few years ago, a fuel channel selection program was written in FORTRAN to assist in the selection of the best candidates for refuelling, based on inputs of past history and simulations, 13 reactor physics based selection rules (for instance, neighbouring channels should not be refuelled at the same time), and channel thermalhydraulic parameters. These inputs were not integrated with the selection program; manual entry was required. The author of the code passed away and the new fuelling engineer(s) have adapted a spreadsheet that has been augmented with spreadsheet macros to perform this task and allow more flexibility than the FORTRAN program.

Chaining of displays: The control room displays have been enhanced to allow the operator to select (from a menu) a grouping of displays that are chained together. This is just a `convenience item' for the operator; otherwise the chaining would have to be done manually by successive keyboard and screen call-up. The Heat Sink Monitoring Displays are in a convenient chain.

On-screen summaries of alarms by system: A menu driven alarm summary list has been provided that allows direct access to the current alarms on a given system.

Numerical variables screen: The original control room displays permitted up to 8 variables to be displayed on one CRT. A simple change was implemented to allow up to 16 variables. Now liquid zone control (14 zones in all) based data can be conveniently grouped on a singe CRT.

Specifications for variables - ranges, instrument number, trend setup info: Alterations were made to permit the ready display of information associated with trend displays. The operator can now toggle between the trends and the associated information. This saves clearing the screen and calling up the specification screen and vice versa.

Put function (panel 20): Changes were made to allow the operator to invoke changes to the CRT displays on the control room panels from his console instead of just manually at each control room panel.

Hardcopy - remote at operator console: Changes were made to allow the operator to request a hardcopy of a display from his console instead of just manually at each panel.

Analogue Input and Control Input: The specification for each input is available on a dedicated screen (since about 1983) providing: use in control programs, Jumpered State, Alarm State, Alarm message, range, and units.

The following more elaborate projects have been implemented:

Heat sink monitoring when shutdown: A special Annunciation Program monitors 100 points and annunciates when limits are reached or their status changes. It also provides advanced warning of possible impending changes to the heat sink systems.

The following more elaborate projects are under development:

Emergency Operating Procedures (EOP): Some of the EOP alarms are now more appropriately displayed on the CRT's. The Entry Conditions to EOP's are being programmed to allow recognition of these events and Alarming of the conditions.

D_2O Vapour Recovery: A BASIC code had been developed to monitor and control this system. The interesting feature is that it has some adaptive capability in that it remembers the system history for loading and regeneration time and schedules dryers into and out of service accordingly.

Items identified for the future are:

On-line procedures: Some form of electronic procedure system is considered useful for the future. Current budgets do not permit the pursuit of this item.

Hand switch position - ROP trip setpoint selection: Currently, when an event has been detected, the operator must set the position of the ROP hand switch to one of three positions, depending on the nature of the event. The operator must manually scan up to 360 event signatures per position to determine if the current event matches one of the permitted events for that ROP setting. If a match is not found for position 1 (the highest setting), then the list for position 2 must be checked, and so on. If no match is found in the end, shutdown is required. This task is an ideal candidate for automation. No work on this is planned.

Auto screen restore after computer restart: It would be convenient if the displays could be reset automatically after a computer restart instead of the operator having to manually setup each display.

Major / minor alarms: Currently, there is a classification of alarms as MAJOR, MINOR and Display on screen, printer or both. For 4 major events (SDS1 reactor trip, SDS2 reactor trip, stepback and turbine trip), only the major alarms are displayed for the first 3 minutes of the event. However, the number of major alarms is higher than necessary and needlessly clutters the displays. The division should be changed to reduce the number of alarms displayed for the major events.

Conditioning of alarms: Currently, alarms are generated even though the associated equipment is out of service and dismantled. Alarm conditioning is required. Provisions have been made but the individual conditioning logic for each point has not been selected.

Trend augmentation: Often there is additional information available that relate to a given trend. For instance, a high temperature alarm may trip at say 50 °C. That information would be useful to display on a temperature trend. It would be nice to have some intelligence built-in to do this. Status displays that provide x-y trends for power dependent parameters and their margins to trip for that parameter is desirable. They would show boundaries or trip levels.

Power dependent annunciation: The operator has to operate the plant over a wide range of states (shutdown cold to 100% FP hot). The plant parameters vary over wide ranges. The current trend displays do not provide information on the permitted ranges for the displayed variables. Context sensitive limits are needed to band the system variables. Alarms in many cases are set for full power operation.

Tech support aids: For system health monitoring, the tech unit can look at parameter trends (seconds to years). The task is to build up the monitoring databases in a systematic manner. Limits can be set on those parameters that are inside the alarm limits used for operation and trends that are off-design nominal can be recognized and acted upon.

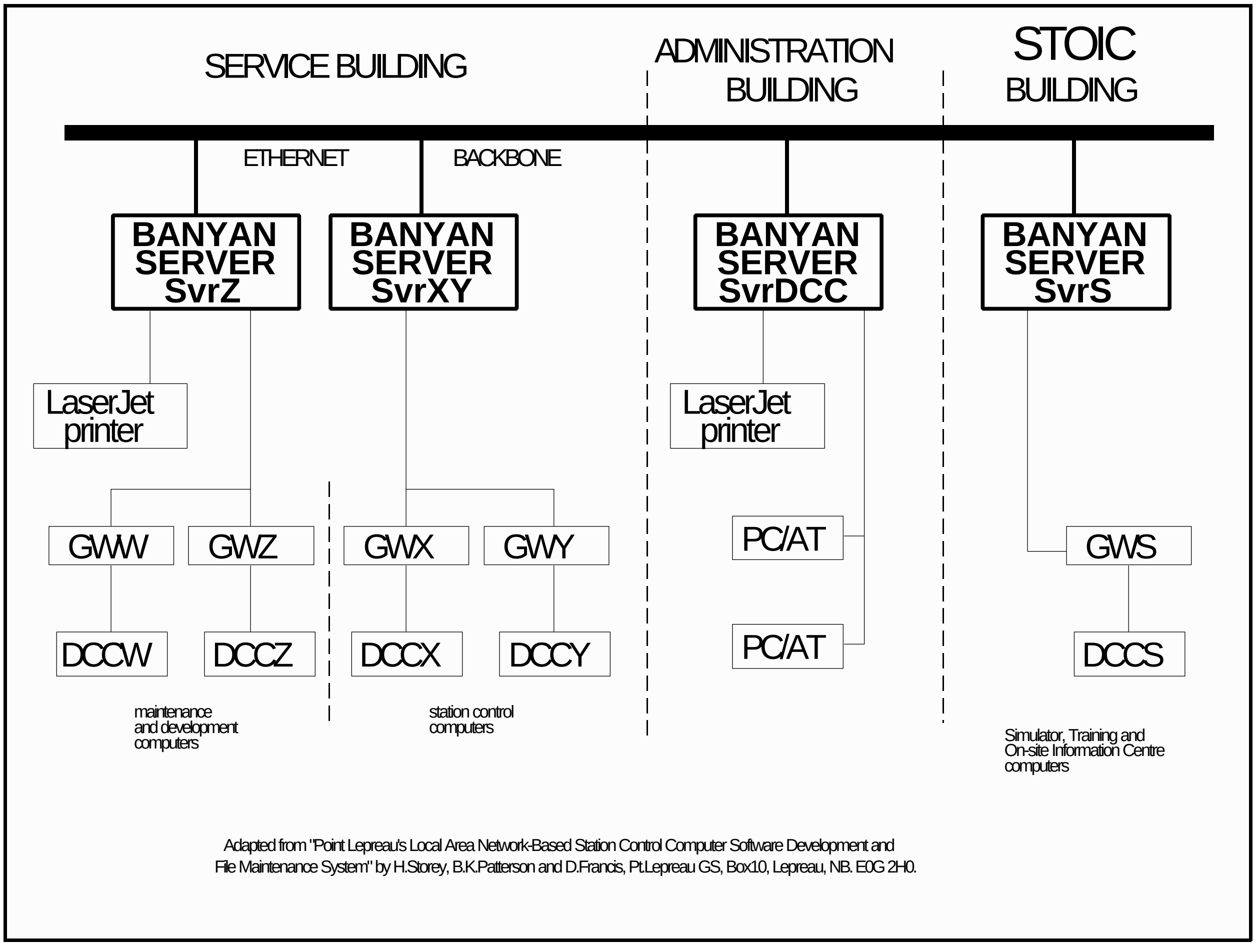

Figure C-3 On-line information access system for Pt. Lepreau

A Gateway system, as illustrated in Figure C-4 (consisting of ethernet, TCP/IP, a BANYAN LAN and real-time software), has been installed providing plant wide communications network capability. The DCC can send data to a file-server and remote PC's can download real-time plant data at will. Time frames can vary from seconds to years. A Generic Monitoring System (GMS), written in PASCAL running under DOS has been installed on systems not monitored by the DCC. The GMS has been installed at site, first for the secondary side chemistry system and is currently being replicated for many other systems. Such a system should be `standard issue' for all stations. GMS also writes to the network. The software was written by Maritime Nuclear who now provide a real-time UNIX based system (QNX) as well as the DOS based system. The Pt. Lepreau setup uses ethernet but there is no Blackboard (BB) or any attempt to provide a coordinated intelligence. The group under the dynamic leadership of Bryan Patterson has built upon current communication technology to create a robust and effective LAN for the benefit of all plant personnel. The key words are incremental, methodical, and practical. This group is doing useful things today to help the technical support teams conduct routine and tedious tasks more efficiently and effectively. Operator aids are limited to enhancing functionality in displays and related devices in the control room.

6. Central Sampling Advisor (OpCoP):

Project: OpCoP
Sponsor: NSERC, NB POWER
Participants: McMaster University personnel (2 faculty members, 2 staff and up to 4 graduate students)
Site: McMaster University
Time Frame: 1991-1994.
Project Scale: $100K per year for 3 years.
Objectives: To develop, for the CANDU 6 central sampling system, an advisor on turbine condenser tube leaks and reactor derating due to secondary side chemistry problems.
Methodology: Employ the blackboard paradigm partitioned along the lines of manager - supervisor - technician, allowing symbolic - numeric coupling in real-time.

Attribute Summary:

Real-time data acquisition: None to date but the architecture is there.
Real-time analysis: Again, none to date but the architecture is there.
Asynchronous activities: Yes, this is inherent.
Distributed architecture: Yes, this is inherent.
Intelligent inferencing: Yes.
Disparate knowledge bases and inferencing: Yes.
Multidisciplinary agents: No.
Different mental models: Yes.
Overall control strategy: Human-centred.

Contacts:

WM. J. GARLAND (416) 525-9140 x4925
DEPT OF ENGIN PHY FAX: 527-8409
MCMASTER UNIVERSITY GARLANDW@MCMASTER.CA
1280 MAIN STREET WEST
HAMILTON, ONTARIO
L8S 4L7

W.F.S. POEHLMAN (416) 525-9140 x2891
DEPT OF COMPUTER SCIENCE AND SYSTEMS
MCMASTER UNIVERSITY SKIP@MCMASTER.CA
1280 MAIN STREET WEST
HAMILTON, ONTARIO
L8S 4M1

Comments:

Research on this project, dubbed the Operator Companion Project (OpCoP), began informally in 1990 and formally in November, 1991 with the award of a 3 year NSERC Strategic Grant.

The objectives of this research are to:

(1) Develop a specific instance in the small of functional and temporal abstraction as applied to intelligent real-time system management.
(2) Develop, for the CANDU 6 central sampling system, an advisor on turbine condenser tube leaks and reactor derating due to secondary side chemistry problems.
(3) Demonstrate the utility of the anthropomorphic approach of applying the blackboard paradigm partitioned along the lines of manager - supervisor - technician, allowing symbolic - numeric coupling with

the inherent efficiency of asynchronous operation in real-time.

Progress to date:

- procedural code to provide a timing benchmark and to validate the logic is in alpha-stage testing.

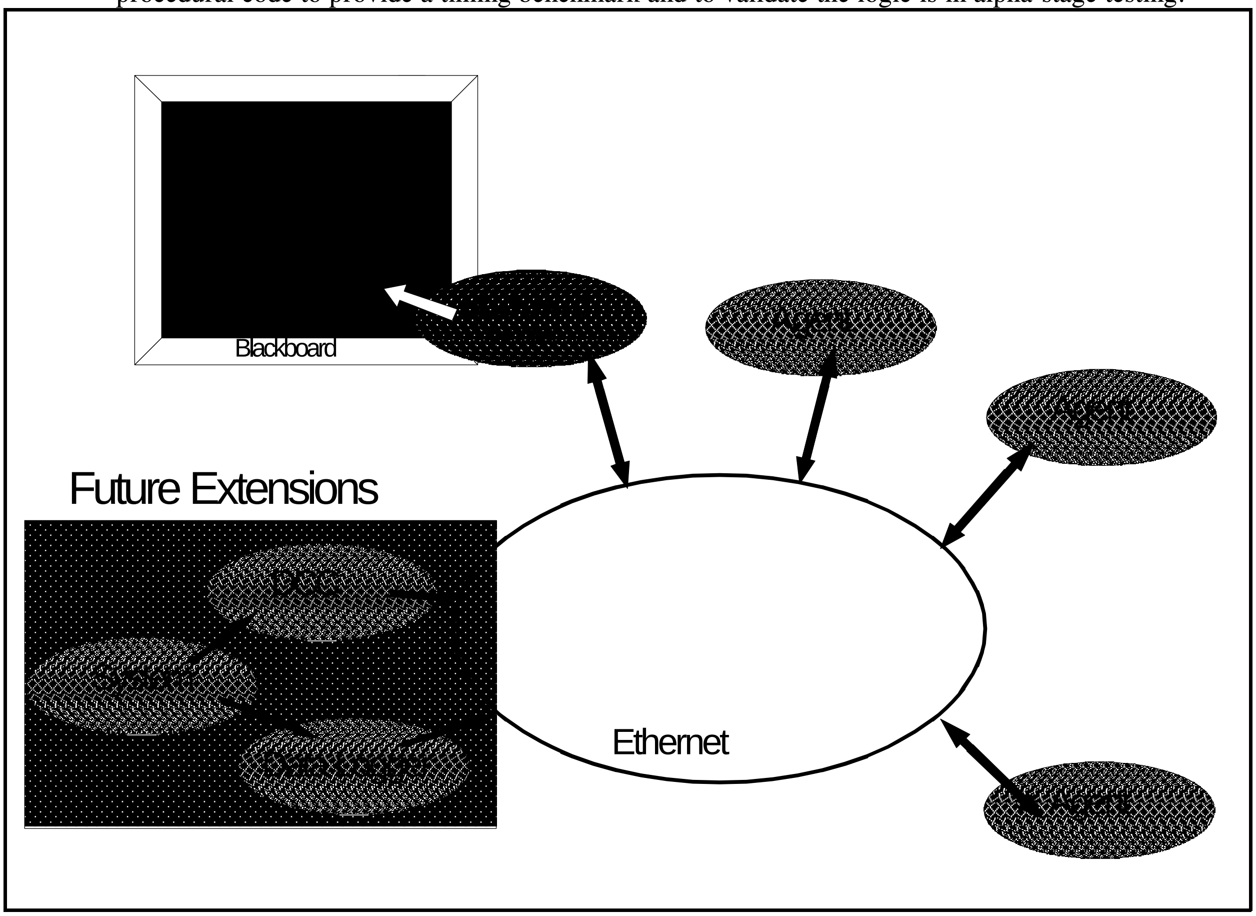

Figure C-4 OpCoP system overview

- PC-based multitasking blackboard prototype has been developed, tested and benchmarked for a toy problem. Figure C-5 illustrates the system overview.
- PC-based blackboard version of the central sampling advisor has begun.
- a LAN based on ethernet and TCP/IP between a SUN Sparc Station and 3 486 PC's has been installed.
- a socket based message passing library over the LAN has been established for UNIX-UNIX communication; PC-PC and UNIX-PC socket libraries are under development.

Interaction with Pt. Lepreau continues.

The group at McMaster is poised to move along with Pt. Lepreau. Some interesting non-nuclear ES's have been successfully prototyped and a cohesive group of researchers has been assembled. OpCoP is based on the model of Figure C-3 but it is not tied into any plant data nor have any real expertise been implemented.

7. University of New Brunswick AI Group:

Project: various
Sponsor: NSERC, NB POWER, Atlantic Nuclear Services, Maritime Nuclear
Participants: University of New Brunswick AI group personnel (9 faculty members and 1 technical assistant)
Site: University of New Brunswick
Time Frame: on-going
Project Scale: several industrial research contracts and grants
Objectives: Objectives: To stimulate research in both applied and theoretical areas of artificial intelligence for industrial availability.
Methodology: Employ techniques common to computer vision, expert systems and machine learning.

Attribute Summary: Not Applicable

Contact:

BRADFORD G. NICKERSON
DEPT OF COMPUTER SCIENCE
UNIV OF NEW BRUNSWICK
P.O. BOX 4400
FREDERICTON, N.B.
E3B 5A3

Comments:

The following projects [MAI90] are being or have been completed by the above personnel:

- an expert system for diagnosing resistance temperature detectors at Pt.Lepreau NGS;
- research in appropriate knowledge representation methods for the knowledge contained in power plant operating manuals;
- a study of expert systems as decision tools for nuclear regulatory tasks under research contract to Atlantic Nuclear Services and the AECB;
- an investigation of the application of expert systems to crisis management for utility power distribution in collaboration with NB Power;
- research into the automated generation of control program test data for the Point Lepreau nuclear power plant under contract to Pt.Lepreau;
- an investigation into expert system methodology for electrical design cost estimation under research contract to Neill & Gunter Ltd.

There is an active group with a number of relevant ongoing projects in AI topics related to nuclear power but no Human Factors focus and no `systems' per se have been attempted.

8. Maritime Nuclear - OADCS:

Project: OADCS
Sponsor: Maritime Nuclear
Participants: Maritime Nuclear
Site: Fredericton, NB
Time Frame: Ongoing.
Project Scale: Approximately 10 full-time people.
Objectives: To develop a highly modular and generic instrumentation and control system for power plants.
Methodology: Distributed high speed computer systems via concurrent engineering techniques.

Attribute Summary:

Real-time data acquisition: Yes. This is their strength.
Real-time analysis: None to date.
Asynchronous activities: Yes.
Distributed architecture: Yes.
Intelligent inferencing: None to date.
Disparate knowledge bases and inferencing: None.
Multidisciplinary agents: None.
Different mental models: None.
Overall control strategy: Not applicable.

Contacts:

JACK SMITH (506) 458-3181
GENERAL MANAGER & CHIEF ENGINEER
MARITIME NUCLEAR
FREDERICTON, NB

Comments:

Maritime Nuclear, a division of AECL CANDU, at Fredericton, N.B. employs 15 people and recently won international contracts to retrofit and update a nuclear plant control room using their OADCS (Open Architecture Distributed Control System). This system is a highly modular (meaning amenable to incremental growth) and generic (meaning readily customizable) for power plant instrumentation and control. Using the QNX Operating System running on multiple Intel 80486 microprocessors interconnected with token passing (acknowledging protocol) ARCNET local area network, OADCS provides alarm annunciation, critical parameter display, event analysis, data logging and archiving as well as process control systems. The user interface is graphical with the OPEN LOOK window manager. Other features include fault tolerance (via redundant systems), intrinsic self-testing, signal validation, and automatic fault detection and recovery. No reference is made to either expert systems or human factors although, in the longer term, such a hardware base in concurrent engineering could form the undercarriage for a delivery platform that encompasses the necessary cognitive engineering properties of an excellent operator companion.

Maritime Nuclear has developed an excellent architecture for real-time distributed control. Couple this with Pt. Lepreau and other Eastern Canada enterprises and you have a recipe for success.

9. Atlantic Nuclear Services Ltd.:

Project: various
Sponsor: various
Participants: Atlantic Nuclear Services Ltd. (ANSL)
Site: ANSL. Fredericton, NB.
Time Frame: Ongoing.
Project Scale:
Objectives: see below
Methodology: see below

Attribute Summary: Not Applicable

Contacts:


```
KEITH SCOTT                    (506)458-9552
PRESIDENT                      FAX: 450-4195
ATLANTIC NUCLEAR SERVICES LTD
P.O. BOX 1268 STA. A
FREDERICTION, N.B.
E3B 5C8
```

Comments:

ARIES is a prototype system designed to test the feasibility of a regulatory expert system directed as an automated decision support system to on-site AECB Project Officers at nuclear power stations. Implementation is centred around a commercial expert system development shell called KnowledgePro which integrates hypertext capability with graphics support on a PC delivery platform. Although nowhere nearly as "intelligent" enough for AECB staff as yet, the proof-of-concept has been made. This project was initiated by the Safety Evaluation Division of the AECB and was funded under the R&D Program of AECB. The need for context sensitive information and rapid reproduction of procedures in times of process upset has been proven. If such characteristics are desired for any operator companion, then this work would be a reasonable entry point for further investigations.

Other aids that have been developed by ANSL include:

1. Containment Simulator - for classroom training of operators.
2. ROP Handswitch Selection - based on input of reactor configuration.
3. ROP Detector Calibration - routine operation aid.

Projects that are underway include:

1. Parallel Processing in the simulation of CANDU reactors.
2. AVAT - A Case Tool for the automatic verification and validation of real-time software and embedded systems.
3. IRMAD - An integrated remote monitoring and diagnostic system.

To date, ANSL is not a main stream player in AI or HF. However, their nuclear experience and their dynamicism may stand them in good stead, especially if they team up with other eastern players. AECB should already be aware of their ARIES project.

10. Spectrum Engineering Corporation Ltd. - ADMS

Project: ADMS
Sponsor: Canadian Space Agency and NRC (STEAR)
Participants: Spectrum Engineering Corporation Ltd. and Queen's University
Site: Peterborough, Ontario
Time Frame: Ongoing.
Project Scale: Several full-time people.
Objectives: To develop a fault predictive, fault detecting, fault diagnosing, and component reliability reporting system for space station applications.
Methodology: Employ tools based on expert systems, database management and operator interface in order to analyze, store and retrieve sensor data from remote systems.

Attribute Summary: Not Applicable

Contacts:

BARRY GRAHAM (705)743-7520
SPECTRUM ENGINEERING FAX: 743-9878
544 MCDONNEL STREET
PETERBOROUGH, ONTARIO
K9J 6Z8

Comments:

Spectrum Engineering Corporation Ltd. is a consulting company located in Peterborough, Ontario. One major project is the Automated Data Management System (ADMS) which is being developed in response to Canada's participation with the International Space Station. It is one of several contained under the Strategic Technology for Automation and Robotics (STEAR) Program ministered by the National Research Council.

ADMS is being designed using expert systems, database management and operator interface tools in order to capture, analyze, store and retrieve sensor data from electromechanical or process engineering systems. Prime functions are fault detection and diagnosis with peripheral applications to trend analysis and failure prediction. A demonstration system, involving a terrestrial application, has been implemented on a SUN SPARC station I using ORACLE database management, X-windows as the user interface base and an inferencing system using NIAL (Nested Interactive Array Language) from Queen's University. This earth-based developed application is ship-board (a Canadian destroyer) and involves the FSS (fairing servicing system) robotic manipulation system necessary to replace damaged fairings on a variable depth sonar cable. The fault diagnosis ES uses collisions and a form of scoring with weights not unlike the heat exchanger prototype that WJG developed for CRL-HTFS 2 years ago. The scoring procedures are rule-based accumulation of 1's and 0's (weighted) depending on whether the fault of that component matches the symptom in question. Tree pruning is done based on heuristics and the systems and components are hierarchically linked.

Future plans include self-modification capability for learning provision, diagnosis tabulated by various ranking criteria, predictive analysis through historical review, and system modularity that facilitates incremental growth [GRA91].

This is an interesting project involving fault diagnosis for robots. There is no direct link to nuclear operator aids but contact should be maintained.

11. Pickering NGS:

Project: CSPAS
Sponsor: COG
Participants: Pickering NGS, AECL
Site: Pickering NGS
Time Frame: Ongoing.
Project Scale: Several people part-time.
Objectives: Develop a Critical Safety Parameter Advisor System for station operators.
Methodology: CRT display of critical parameters, repackage information, annunciation.

Attribute Summary:

Real-time data acquisition: Yes, CSP data is channelled to a PC.
Real-time analysis: No, this is just alarm annunciation.
Asynchronous activities: No.
Distributed architecture: No.
Intelligent inferencing: No.
Disparate knowledge bases and inferencing: No.
Multidisciplinary agents: No.
Different mental models: No.
Overall control strategy: Human-centred.

Contacts:

BRIAN BERNDT
ONTARIO HYDRO
P.O. BOX 160
PICKERING, ONTARIO
L1V 2R5

Comments:

From discussions with Pickering NGS personnel in 1990, we were informed that Ontario Hydro nuclear plants tend to use an `event driven' philosophy (the operator attempts to identify the event and reacts accordingly) vs. the `symptom based' approach (the operator reacts to the symptoms directly in a procedural manner) that is used in the US. However, the critical safety parameter (CSP) approach is symptom based; no attempt at event determination is made and the focus is to do what is necessary to keep the critical safety parameters within safe bounds. Discussion with personnel at the Eastern Nuclear Training Centre (ENTC) at Pickering at around the same time revealed that trainees had difficulty identifying events; their strength lay in their ability to implement procedures as required.

Brian Berndt of Pickering NGS indicated that there has been some activity in developing a fast retrieval system for the latest version of documents via computer. Once brought up on-screen the whole pertinent document can be hardcopied for review. It is not intended to be used in emergency procedures, however. Others are looking into an automatic prompter which is more like an operator companion. Brian does not see the current work on Electronic Emergency Operating Procedures (EEOPS) leading to operator use.

Brian has also been involved in the CSP Advisor System (CSPAS) which is a system for which AECL has been contracted to perform the research and development. This work is proceeding in two phases: Phase I involves monitoring the plant CSPs and repackaging the information (which is already normally monitored in the operations bridge) so that a personal computer (PC) can provide the CSP view. When the CSP varies beyond acceptable limits, alarms occur which force the operator into paper procedures which attempt to move the CSPs back into acceptable areas. The human factors aspects have been accommodated by already exposing the operators to the CSP monitoring system.

Phase II, at the moment involves the scoping of the project into a more active role where a CSP advisor will sort out procedures which should be applied to any CSPs which are out of norm and suggest a course of action for the operator to take. This then is a planning scenario generator. Hence, Phase I is also determining if a prototype of this nature is feasible and the research and development evaluation is in the hands of the AECL group. In the longer term, if the feasibility determination is positive, then, in order for extensive testing to take place, the use of the ENTC training simulators is being proposed. This allows the operators to assess the CSP Advisor and evaluate its usefulness.

Indications are that no projects are ongoing or planned except for those conducted through COG. Plants are moving towards improved data handling in general and operating procedure assistance in particular. CRL and Pickering NGS are working on a COG funded critical safety parameter advisor system (CSPAS). It appears to be a very localized system but human factors are being considered.

12. Hydro Quebec

From [AND90], mention is made of AIDE (Air Instrumentation Diagnostic Expert), an ES that Hydro Quebec intended to build. AECL was involved. This information dates back to 1988. Norman Gour, Gentilly 2 NGS, provided an update on Hydro Quebec's efforts in the area of operator aids. The AIDE (Air Instrumentation Diagnostic Expert) was a embryonic effort into station aids (both for the operator and the technical units). It was dropped in favour of an investigation into safety system diagnostic aids. However, they found that safety experts were not readily available for this project. Hence the project was not pursued further. Attention was redirected to providing an Class III diagnostic aid, but that project also was stopped for lack of available expertise. Hydro Quebec has plans to develop aids for root cause analysis and predictive maintenance but no time line has been set.

13. Other Reactor Sites

Bruce NGS: The APACS project (discussed elsewhere) is based on the Bruce feedwater system but the Bruce site is not directly involved nor will it be targeted for installation of APACS deliverables in the foreseeable future.

Darlington NGS: On the recommendation of Ed Fenton, Ontario Hydro, Rick Hohendorf was contacted for information on operator aids under consideration for Darlington NGS. From his comments, there is an Equipment Status Monitoring system in place at Darlington NGS. It consists of a Sun Work Station linked to a number of data servers. These data servers contain some 1500 graphical flow diagrams covering the plant process flow sheets. The primary function of this system is to aid the Unit first operator in constructing the `Orders to Operate' that are given to the field operators. The Unit first operator can retrieve graphical colour coded information on any piece of plant equipment. The colour coding indicated the status of the equipment (in service, etc.). Desired information can be cut and pasted into the Order to Operate.

Critical safety parameters (CSP) work for Darlington is in the definition phase only. Pickering NGS decided to proceed with their implementation ahead of the other stations and COG coordinated work.

There is some work ongoing in the area of `Configuration Management'. The contact is Stan Harvey.

Real-time issues come up in the maintenance area as well as in the control room. One case in point is reactor retubing. This activity is time-critical and occurs in a radioactive environment. Rick is involved in the development of displays (textual information, real-time animation of tools, and cameras). A prototype has been built and delivery is targeted for next year.

RMC: Hughes Bonin is the contact person in charge of the campus SLOWPOKE. According to Hughes, no operator aids are under consideration at RMC.

University of Toronto: Dr. Ron Hancock of the SLOWPOKE reactor facility was contacted. No operator aid projects have been attempted or are planned since the simplicity of SLOWPOKE operator does not warrant it.

CRL reactors: Bernie DeAgreu, CRL, was contacted regarding operator aid projects that involve the CRL reactors directly. Only one project, the Part-Task project, was cited. This involved the provision of an event simulator for the NRU fuelling machine to be used for operator training and evaluation purposes. Eric Davey, CRL, of Lawrence Lupton's HMSD group, is the person in charge of project development. The project is targeted for training purposes only. Human Factors issues and mental models were discussed, reiterating some of the main points discussed elsewhere in this report. Bernie felt that the engineer / technician mental model proposed by Rasmussen [RAS86] portrays a notion of an engineer that is restricted to the design side of engineering; the operations engineer view is not included.

14. Institute for Robots and Intelligent Systems (IRIS):

Project: IRIS
Sponsor: Federal Centre of Excellence
Participants: over 100 researchers.
Site: nation wide.
Time Frame: variable.
Project Scale: 22 projects with a total funding level of $23M.
Objectives: To develop intelligent robotic devices that can operate in unstructured environments and very hostile conditions.
Methodology: Computational perception, knowledge base systems and intelligent robotic systems.

Attribute Summary: Not Applicable

Contacts:


```
JEAN-CLAUDE GAVREL           (613)727-9576   FAX: 727-5672
PRECARN                      GAVREL%A1.AT0TT2.NRC.CA@VM.NRC.CA
30 COLONNADE ROAD
NEPEAN, ONTARIO
K2E 7J6

NICK CERCONE (Project B4 only, see below)      (604) 291-3229
CENTRE FOR SYSTEMS SCIENCE
SIMON FRASER UNIVERSITY
BURNABY, B.C.
V5A 1S6
```


Comments:

One of the Federal Centres of Excellence is the Institute for Robots and Intelligent Systems (IRIS). As mentioned in the PRECARN section, PRECARN is administrating IRIS. Topic areas are (from the information kit supplied by PRECARN):

Area A: Computational Perception

There are 7 projects in this area dealing with perception slanted towards robotics. None directly impact on operator aids.

Area B: Knowledge-Based Systems

B1: Design of Large Information Systems - basic computer science, not an operator aid

B2: Using Connectionist Learning for Adaptive Interfaces - neural networks for robotics, not an operator aid

B3: Database Techniques for Knowledge-Base Management - focuses on `the frame problem' in robotics, not an operator aid

B4: Design and Human Interfaces - project leader Dr. Nick Cercone, SFU -this work might have some impact on operator aids but not in the short term. This is essentially an envelope for other ongoing research projects (IGI and IntelCAD).

B5: Foundations for Reasoning Systems - basic computer science, not an operator aid

B6: Engineering Applications of Constraint-Logic Programming - basic computer science, not an operator aid

Only project B4 was identified as close enough to operator aids to warrant followup.

Area C: Intelligent Robotic Planning and Execution Systems

There are 9 projects in this area dealing with robotics. None directly impact on operator aids. In various discussions with Hoda ElMaraghy (McMaster University), a researcher in the IRIS Federal Centre of Excellence, her particular project may have indirect impact on Operator Companions. This is in the area of self-planning and execution. That is, if one characteristic of the Companion is to dynamically recognize changing situations and therefore alter analysis approaches, then systems are needed that respond appropriately to rapidly changing real-time information. Such behaviour is required of robots that must be able to plan and replan in a timely manner in order to adapt to changing goals and conditions. This situationally driven system may provide useful insights into similar problems encountered when implementing nuclear power plant operator companions.

IRIS is in a different sphere altogether (autonomous robots). There seems to be no near or medium term overlap with the nuclear industry. The work of IRIS should be monitored so that developments can be factored into the nuclear industry as appropriate.

15. Intelligent Graphic Interface (IGI):

Project: IGI
Sponsor: PRECARN
Participants: MPR Teltech Ltd., Simon Fraser University (SFU), ARC, ...
Site: Primarily Western Canada.
Time Frame: 5 years from February 1991.
Project Scale: $6.7M over 5 years.
Objectives: Provide more effective means for human operators to communicate with real-time supervisory control systems.
Methodology: Combine advanced computer graphics technology with expert systems and human factors engineering.

Attribute Summary:

Real-time data acquisition: No.
Real-time analysis: No.
Asynchronous activities: No.
Distributed architecture: No.
Intelligent inferencing: Yes.
Disparate knowledge bases and inferencing: Yes.
Multidisciplinary agents: No.
Different mental models: Yes.
Overall control strategy: Human-centred.

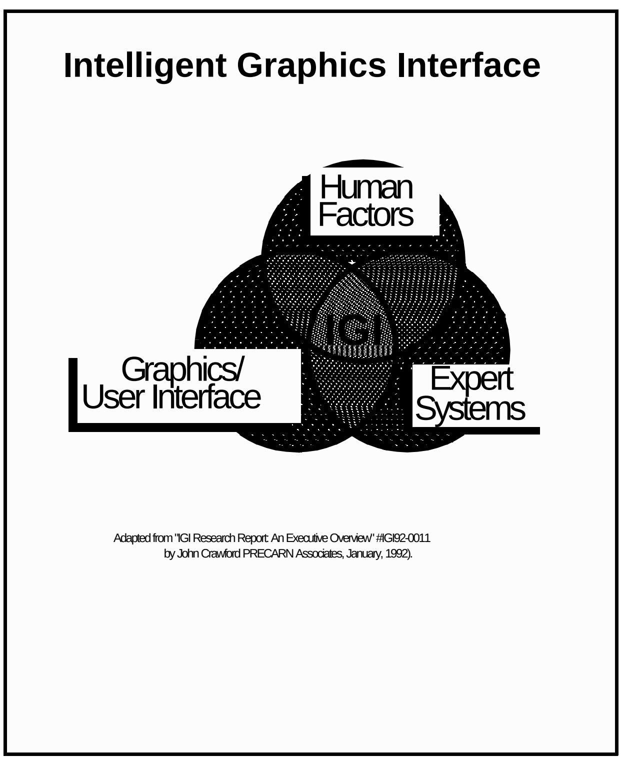

Figure C-5 Intelligent Graphics Interface Overview

Contacts:

```
JOHN CRAWFORD                          (604)
293-5735  FAX: (604) 293-5787
MPR TELTECH                           EMAIL:
CRAWFORD@MPRGATE.MPR.CA
8999 NELSON WAY
BURNABY, B.C.
V5A 4B5
```

Comments:

The five year project, begun in 1991, involves both Canadian industry and academic communities whose goal is to combine advanced computer graphics technology with expert systems and human factors engineering to produce the Intelligent Graphics Interface (IGI) as shown in Figure C-6. Projected use is as an expert assistant for operators of real-time supervisory control systems.

IGI is a PRECARN project funded to the $6.8M level and involves Alberta Research Council, B.C.Tel., DEC Canada, HP Canada, Shell Canada, Simon Fraser University, H.A.Simons, TransAlta Utilities, Virtual Prototypes and Xerox Research Centre of Canada. MPR TelTech is the Lead Contractor and Project

Manager. Prototype installations are being developed for the B.C. network control centre, Alberta electric power network control centre and Xerox pilot plant research facility.

Importance is given to how computer aids interact with the user's mental model of the on-going process. Hence, the project actually distinguishes between three types of knowledge: system self-knowledge, user knowledge and process (domain) knowledge. Another thrust of this work is the real-time aspect which starts at the bottom end with the real-time expert system called Echidna. This expert system shell is being developed in the Simon Fraser University Expert Systems Laboratory. IGI is designed to provide improved decision support tools for supervisory control by utilizing research into graphics user interface techniques, real-time expert systems and human factors issues. Although not of short-term importance, the long-term significance of this work may impact future strategies for reactor operating companions. Reference: [CRA92]

IGI is narrower in focus (GUI) than the `system' type projects investigated herein. This work is closely linked with IRIS and the comments noted for it apply here.

IGI evolved from the older IntelCAD project at Simon Fraser University which combines a tri-level approach to the problem of assisting the user in design and synthesis. (Note that identical approaches can be taken with the operation of process control systems and this has been done with the more recent IGI and IRIS projects at SFU. The important concepts developed here include the realization that for best results, the assisting computer must interact with the operator's model of the problem and its solution, not with the physical process under focus. Such work is laying the groundwork in man-machine tuned knowledge structure and the use of AI in delivering intelligent GUIs to the control and/or design engineer.

D. SUMMARY OF SELECTED READINGS

AND90 J.W.D. Anderson, "The Use of Expert Systems for Operations Support in the CANDU Nuclear Power Supply System", report of a technical committee meeting organized by the IAEA and held in Vienna, 17-21 October, 1988. IAEA-TECDIC-542, 1990.

This document predates [LUP89a] and covers similar ground. It does mention some projects not mentioned elsewhere, namely:

Pump Seal Replacement Advisor - in progress
Eddy Current Inspection Interpreter - in progress
Automatic Fault Tree Construction - planned

Mention is also made of AIDE (Air Instrumentation Diagnostic Expert), an ES that Hydro Quebec intends to build. AECL is involved.

BER89b John A. Bernard, Takashi Washio, "Expert Systems Applications Within the Nuclear Industry", American Nuclear Society, 1989, ISBN: 0-89448-034-0.

This is a compendium of who is doing what in ES applied to nuclear systems. Some 300 programs are surveyed but the coverage is necessarily shallow. However, some useful overviews and interpretations are given. The Operator Companion of AECL is covered and it is noted that, contrary to other projects, the emphasis is not on advice during emergencies, but on improvements in routine operations.

The authors state that there are few actual implementations of nuclear expert systems (as of the time of publication) and even fewer reports on the resulting benefits and/or problems. At the recent ICHMT forum [BER92] John Bernard noted in an excellent paper that the need for the operator is real-time diagnosis. Past ES's were machined-centred whereas it is now recognized that operator aids should be human-centred. The industry is no longer headed down the machine-centred route. John mentioned that EPRI has a human factors group.

BER92 John A. Bernard, "Issues Regarding The Design and Acceptance of Intelligent Support Systems for Reactor Operators", ICHMT 2nd International Forum on Expert Systems and Computer Simulation in Energy, University of Erlangen, 17-20 March 1992.

This paper is a `must read'. Since it is well written, it is sufficient to simply quote extensively:

"The central premise is that conventional expert systems which encode experiential knowledge in production rules are not a suitable vehicle for the creation of practical operator support systems. The principal difficulty is the need for real-time operation."

"Three findings stood out. First, about twenty-five percent of the identified expert systems were being developed to assist humans with managerial responsibilities in the areas of plant design, management and maintenance. A second trend was that enormous resources were being devoted to the development of expert systems that would assist licensed reactor operators in the discharge of their responsibilities, especially emergency response. This is evident from the figure which shows that forty percent of the total number of identified expert systems were for real-time diagnostics, operator advisers, or emergency preparedness. A third, and very disturbing trend, was that little had been done in the way of experimental work to assess operator response to expert systems."

"The most gratifying change that has occurred during the past two years is that several operator-support expert systems have either become operational or are very close to that goal. In the United States, the most prominent is the Reactor Emergency Action Level Monitor or REALM which was developed for the Indian Point Unit 2 plant and is now also under consideration for San Onofire ... In Asia, the Emergency Operating Procedures Tracking Systems (EOPTS has undergone extensive and very successful testing at the Taiwan Power Company's Kuo Sheng plant ... Also, the Japanese national effort on the Advanced Man-Machine System for Nuclear Power Plants (MMS-NPP) continues to progress ... In Europe the very impressive SAS-II system is undergoing testing at Sweden's Forsmark plant where it will be used to assist shift supervisors in following emergency operating procedures ..."

"What can we conclude about the needs of licensed reactor operators? First, as a result of their extensive training and operating experience, most operators have excellent pattern recognition skills and can readily distinguish between expected and abnormal plant behaviour. Second, operators know the appropriate response for a given casualty. When difficulties do arise, they are most often the result of inability to identify the nature of the problem. An operator's principal need is therefore for timely, accurate analyses of actual plant conditions."

"During the 1960's the approach taken was to provide licensed operators with abnormal operating procedures (AOPs) for every conceivable casualty. This event-oriented approach was challenging even to those who operated plants of only a few hundred megawatts and, as plant sizes grew, it became totally impractical. One alternative was to increase the number of instrument readouts. However, this merely swamped the operator with information. In the early 1980's, the industry introduced symptom-based procedures. While this symptom-based approach is an improvement, it results in lengthy procedures that have multiple entry points. Hence, despite improvements such as symptom-based procedures, the need still exists for a real-time diagnostic capability."

"Thus, the creation of expert systems for real-time diagnostics cannot be achieved through the extension of the concepts observed in the development of off-line systems. Rather, the entire process needs to be rethought and new approaches identified."

"The traditional method for the construction of an expert system is for a knowledge engineer to identify a human expert and then, through a series of interviews, to extract the relevant information. This approach is not recommended for the design of support systems that offer a real-time diagnostic capability."

"... found that four distinct but related domains had to be surveyed ... These were operations, training, licensing, and design."

"... advocates the use of process models for the construction of a knowledge base. Reliance on such models as a source of knowledge is an increasingly common characteristics of intelligent support systems."

"One advantage of incorporating models in a system for automated diagnostics is that expected plant responses can be determined for any set of initial conditions."

"Unfortunately, the model-based approach to the construction of a knowledge base engenders many difficulties. First the model must function in real time. "

"... it is necessary that the model be periodically calibrated."

"... third challenge is to transform a model so that the information generated is of use for automated diagnostics."

"The computer-based model should be directly coupled to the actual physical process."

"In conventional expert systems, such as those developed for water chemistry analysis, the user supplies the various test results and is queried as necessary for additional information. This mode of interaction is not acceptable for intelligent support systems because, int he first place, it couldn't be done in real time and, more importantly, it would distract the reactor operators from their licensed duties. The alternative is for all of the information needed by the intelligent support system to be provided directly from the plant instrumentation. However, many existing plants were not instrumented for this purpose and would required retrofitting. For example, existing diagnostic expert systems such as those for turbine-generators, have required the installation of significant numbers of additional sensors ..."

"There are a number of special requirements imposed on the inference engine of a real-time, intelligent support system. These include:

> The search must be accomplished rapidly so as to maintain real-time performance. Alternatively, the expert system should be programmed to provide the best possible answer within a fixed time interval ...
>
> The system should be capable of iteration because the receipt of new or updated information may alter conclusions that have already been reached ..."

"The proper design of the man-machine interface is recognized as the single-most important factor in determining user acceptance of an expert system."

"Thus, there is no longer any question that artificial intelligence methods can contribute to the safe, effective use of nuclear energy. However, the issue remains as to the proper roles of man and machine."

"This machine-centred approach has now been recognized as unwise."

"A superior approach is a human-centered one ..."

"On 26 June 1988, an A320 crashed during a French air show killing three and injuring fifty. At the time of the crash, the pilot was making a low-speed pass at an altitude of only 15 meters. The intent was to fully display the A320 to those attending the air show. The pilot may have assumed that the computer-based protective system would automatically intervene if the plane's speed reached the stall point. But, the software was programmed to assume that a landing was in progress if the plane was being flown manually below 30 meters, Hence, there was no automatic protective action. The plane did stall and then crash .... The implication for the designers of intelligent support systems is that extreme care must be exercised not only to design an intelligent tool that is both reliable and accurate but also to create one that is fully understood by its prospective users."

"However, it remains an open question as to whether intelligent support systems can be successfully developed for real-time diagnosis and operator guidance."

"Finally it is imperative that each incremental advance in the technology be tested in an operational setting. Experimentation is the key to maintaining the technology both realistic and of benefit."

BHA91 S.C. Bhatt, "Assessment of the Canadian Instrumentation and Control Technology in Nuclear Power Plants", document produced for the National Science Foundation and department of Energy, U.S.A., 1991.

This paper deals with Instrumentation and Control matters that lie well outside the scope of this report. However, one section outlines operator aid related projects in Canada:

- OH is developing an ES for the coolant injection system.

- OH is developing a `feedback' ES to process information and be interposed between the operator and the plant.
- AECL has not yet implemented an ES at any Canadian utility. It is planning to implement a real-time system at a coal-fired station with the next year. (Comment: This sounds like Maritime Nuclear.) The usual list of aids that AECL is involved in is given:
  - ES for temperature control
  - defect detective
  - condenser saltwater leak advisor
  - on-line diagnostic checklist shell
  - safety system impairment advisor
  - programmable digital comparator diagnostic expert
  - secondary heat transport (whatever that means)
  - process control (that narrows it down!)
  - fault diagnosis
  - spent fuel bundle count
  - development of training manuals.
- AECL is developing a few ES's for the Canadian Electrical Association.
- OH is working on operator aids for:
  - alarm analysis
  - heavy water inventory
  - status monitoring
  - diagnostic monitoring.

COM88 J.G. Comeau, "Routine Trend Analysis Program for Plant Process Parameters", Proceedings of the 9th Annual Conference of the Canadian Nuclear Society, Winnipeg, 1988.

This extended abstract is a forerunner of work described at the recent CNS Student Conference held at McMaster (1992). This is a good example of the kind of assistance that plant personnel really need: tools to help out with the routine and procedural activities, tools that work in the background over long periods, tools that compliment, not replace, the human, tools that enable.

HAR88 R.S. Hart, "CANDU 300 - The Next Generation", Proceedings of the 28th Annual Conference of the Canadian Nuclear Association, Winnipeg, 1988.

This paper states that the CANDU 300 (now called the CANDU 3) design features "Enhanced man-machine interface and computerized monitoring and testing capability." and "While building on the traditional CANDU approach to safety, CANDU 300 incorporates many improvements, ranging from enhanced systems performance to improved man-machine interfaces."

HEY88 I.S. Hey and D.F. Meraw, "Ontario Hydro Nuclear Generation Division Information Systems at Darlington NGS", Proceedings of the 9th Annual Conference of the Canadian Nuclear Society, Winnipeg, 1988.

This extended abstract illustrates the importance of knowledge bases.

LIN88 R.P. Linsay and B.A. Rolfe, "The Development of Ontario Hydro's On-Line Computerized Wiring Information System", Proceedings of the 9th Annual Conference of the Canadian Nuclear Society, Winnipeg, 1988.

This extended abstract os a good example of the importance of knowledge bases visa vi the human centred approach. The focus is on providing meaningful tools to personnel, capitalizing on cheap computers and

rising labour costs.

LUP89a L.R. Lupton, R.A.J. Basso, L.L. Anderson, and J.W.D. Anderson, "Expert Systems Use in Present and Future Nuclear Power Supply Systems", AECL - 10073, November 1989.

The report summarizes the state of operator aid related R&D at AECL as of 1989. Discussed are:
(1) OPERATOR COMPANION: Conceived as a family of ES's connected via a LAN. The advantages of such a distributed and modular architecture is discussed. Discussions with design and operations gave the following main activity areas:

Alarm Annunciation
Fault detection and diagnosis
Plant Configuration
Vital operating parameters
Operating procedures

Each of these areas are discussed and a prototype using NEXPERT OBJECT is outlined. Current status: Nothing more has been done beyond the prototype in the lab.
(2) REFUELLING (FUELEM): Demo system. No details given except that it is being customized for Pt. Lepreau. According to Ben Rouben of AECL, this project is no longer being pursued since site personnel did not show sufficient interest.
(3) FUEL DEFECT DETECTIVE: No details. According to Al Manzer of AECL, this project is no being pursued. (Comment: John Anderson was the developer.)
(4) DIGITAL COMPARATORS: To reduce unnecessary board swapping at site. (Comment: WFSP was asked to look at this by Pt. Lepreau. This project was worked on by John Anderson at Pt. Lepreau GS.)
(5) CONDENSOR LEAK ADVISOR: No details. (Comment: From our conversations with John Anderson and Bryan Patterson, we know that Brian used EXSYS to code up some of the operating procedures at Pt. Lepreau and that John fashioned a Pascal forward chaining inference engine to mirror Bryan's EXSYS prototype. These are toy implementations for discovery purposes. On Bryan's suggestion, a major program was mounted at McMaster to prototype a real-time blackboard based system. This is discussed in Section C, OpCoP.)
(6) SHUTDOWN SYSTEM ADVISOR (SADAU): Root cause analysis system for G2. No details. Plans to integrate this with the Operator Companion. Project changed to SADAC based on further review at G-2, looking at Class III/ IV electrical system diagnosis. Project deferred due to unavailability of staff at G-2 to participate (i.e., higher priority work came first).
(7) EMERGENCY OPERATING PROCEDURES: Hypermedia based. Plans to integrate this with the Operator Companion. Work was deferred as a result of funding change to COG. Concepts will be incorporated, as appropriate, in CSPAS.
(8) S&T DESIGN ADVISOR: No details. (Comment: the advisor referred to was an EXSYS exercise done by Rick Basso using and HTFS document, DR 18 Part 1. Another toy system. WJG is pursuing this through HTFS.) References look too old to be relevant.

LUP89b L.R. Lupton, L.L. Anderson and R.A.J. Basso, "The AECL Operator Companion - An Overview", AECL - 10074, November 1989.

This report is an expansion on the Operator Companion described in AECL - 10073 [LUP89a]. Ethernet was used for the LAN to link a VAXstation to Macintosh machines. The prototype worked up was for the SES reactor. Future development included message passing. (Comment: The concept was proved but not put into operation.)

LUP90 L.R. Lupton, J.J. Lipsett, R.A. Olmstread and E.C. Davey, "Foundation for Allocating Control Functions to Humans and Machines in Future CANDU NPPs", Proceedings of an International Symposium on Balancing Automation and Human Action in Nuclear Power Plants, sponsored by the IAEA and OECD,

Munich, July 9-13, 1990, IAEA-SM-315/28 pp 349-367, also as AECL - 10198.

This paper warrants careful reading. It builds on NUREG-0700, EPRI NP-3659 and especially IEC 964 to provide a functional design methodology (FDM) for determining the work split between the operator and the machine. The AECB have issued a draft policy statement (ACNS-9) which requires that systematic methods in the HF area be applied to new nuclear facilities. The work described in this paper does just that. This work takes the intend of IEC964 and applies it to the CANDU since such a methodology did not exist for CANDU before now. The overall scope and principle of the control room design process is done for the most part. Detail work is currently underway (as evidenced by the work outline in the overheads supplied by Lawrence (Record of Discussion 92-04-20).

Worthy of note is the explicit recognition of the dual goals of power production and safety. One of the nicer aspects of the FDM is that it makes all the relevant issues explicit and this is necessary to ensure that both masters are being served appropriately.

The paper recognizes that there are job functions that only a human can do (creative), that only a machine can do (hard control) and functions that fall between these two extremes. The FDM has, as its primary objective, the identification of which jobs fall into which category. (Comment: It is interesting to note that, once again, we have 3 levels. They call them `knowledge based', `rule based' and `skill based', and we call them `Manager', `Supervisor' and `Technician'.) Figure 1 is a nice conceptual representation of the control process. The paper also recognizes that the plant design may differ from the actual plant. The term `set' is used to signify that a plant can be represented by state descriptions and transition values between states. The plant must not be allowed to operate outside the bounds of the known and understood.

Information = synthesized data. Nice. Compare this to Lupton's international survey paper: knowledge is data with known syntax and semantics.
(Comment: Preferable definitions might be:

noise + syntax -> data
data + semantics -> information
information + systemics -> knowledge
knowledge + context -> meta-knowledge.)

Problem solving is divided into 3 stages: perception, planning and execution (3 levels again!) This drives the notion that the operator needs contextually correct information if he is to perform the correct tasks at the correct time. Right on.

The rest of the paper deals with FDM on a more detailed level, dealing with the criteria for function allocation, etc.

(Comment: Overall, a very impressive and systematic work program. One is inclined to say: Yes, yes, go for it. But at what cost? There is the direct cost of all that very detailed engineering. That could be staggering if the FDM is pursued by the AECB with a vengeance. And, given the finite resources of the utilities, what would be neglected in other areas. As always, a balance must be struck. These ideas must be explored at an aggressive pace but not at undue expense of other programs that equally affect (or effect) plant safety or performance.

Internal reports were prepared but could not be released. AECL CANDU, as part of CANDU 3, has made a formal presentation to the AECB regarding what they will do in the way of a design methodology. It is somewhat different than what is shown in this report. Hence, the work shown in this paper is NOT an industry standard (the designers shared my concerns regarding cost, schedule, etc.). Ontario Hydro, as part of the Bruce A rehabilitation, will be preparing Human Factors plans to cover design work and will follow an abridged version. Treat this paper as a first pass at the process, with lots more work required.

LUP92a Lawrence R. Lupton, "An Overview of Control Centre and Applied Human Factors Research for CANDU Nuclear Plants", extended abstract to be published.

Lawrence provided this 3 page extended abstract to go with the copy of the overheads on COG funded research. Main point of interest is that the bottom-up approach to alarm processing had limited success. Now they seem to be taking the top-down approach (functional abstraction). See the discussion of AECL - 10198 [LUP90].

LUP92b L.R. Lupton, "COG-Funded Applied Human Factors Research and Development", copies of overheads to be presented.

An overview is given to place this work within the COG setting (Working Party 16). The stated goal is to improve plant performance and support operations by conducting R&D in Instrumentation & Control and related areas. The stated engineering objective is to develop new concepts, methods, tools and prototypes.

WPIR 5100 Control Centre and Applied Human Factors Development

(1) Human-Machine Interface Evaluation: Working on:
- Bruce A Operating Diagram (SOD)
- 3D graphics and animation (U of T)
- Display architecture
- Workload assessment (Pt. Lepreau)
- Criteria and methods for aid assessment
- Functional abstraction methodologies
- HF prototyping facility

Demos are not available yet (perhaps in a few months). U of T can NOT release any material without permission from WP 16.

(2) Alarm and Related Information System Improvement: New approach: systematic top-down and bottom-up (see AECL - 10198). Working on:
- What are the relevant HF issues?
- Functional role of improved alarm system
- Prototypes
- Performance monitoring and predictive monitoring (RPC/UNB)

(3) Plant Operating Procedures Resource Centre: Working on:
- Review of CANDU and international experience
- On-line EOP (Pickering)
- OH EOP supervisor's meetings

Prototype EOP syntax checker will be demonstrated to PNGS in about 2 months. At which point, Lawrence may be able to release details to others.

(4) CANDU Plant Applied Human-Factors R&D: Looks like planned work only

WPIR 5108 Critical Safety Parameter Advisor System

Monitor prototype planned for December 92
Advisor prototype planned for December 94
More details to come later this year, after the usability testing. Ontario Hydro will review anything that is released.

WPIR 5115 Human Factors Familiarization Training

Course prepared and delivered
Future additions planned
Next course to be given later this year. Course notes are proprietary to COG and consultant that developed

material. The material is being updated at the present time.

LUP92c L.R. Lupton, P.A. Lapointe and K.Q. Guo, "Survey of International Developments in Alarm Processing and Presentation Techniques", to be presented.

As the title indicated, this paper focuses on alarms, just one of the work areas listed in [LUP92b]. As has been found in the literature before (and is obvious anyway), one cannot begin to manipulate objects unless one first identifies the objects and the relationships between those objects. Alarm processing is no exception. Thus, two main branches of investigation are identified as:

Knowledge Representation
Decision Making

Structure is the key to knowledge representation. The paper identifies:

- Casual Structures
  - cause-effect, root cause, event trees, etc.
- Plant Functional Analysis Trees
  - system descriptions (functionally decomposed) and relation to goals
- Alarm Relationship Trees
  - alarms and relations (alarm A causes alarm B, etc.)
- Quantitative / Qualitative Representation Models
  - models (mathematical or otherwise) to represent behaviour

(Comment: Can the plant can be so neatly carved up into these categories? Like any attempt at grouping objects, there is no unique organization; what's best depends on the goals and `the proof of the pudding is in the eating'. Any given implementation will be a mix of different techniques and structures.) Lawrence Lupton replied: Deciding which ones apply for a given need is a good question! we do not have a well defined structure as yet.

The decision aspects are covered in some detail in the paper. Here we are talking about firing rules, setting priorities, etc. The breakdown is as follows:

Validation / Inhibition Rules

- Operating Mode
- Dynamic Thresholding
- Operating Status
- Alarm Jumpering
- Signature of Alarm
- Direct Precursor
- Level Precursor
- Chattering Removal
- Redundant Alarm Removal
- Irrational Alarm Filtering

Conceptual Alarm Generation Rules

- Functional Alarm Generation
- Category Grouping
- Event-Driven Alarm Filtering
- Pattern Recognition
- Status Monitoring
- Sequence Monitoring
- Transient Guidance

Diagnostic Reasoning Rules
Qualitative reasoning Models
Early Fault Detection (EFD)
Root Cause Identification

Prioritization Rules
Static
Dynamic

All the above are defined and described in the paper. Seems comprehensive and reasonable. (Comment: Everything is in there except for the kitchen sink. Which raises the question of how to keep everything organized and modular. Can all those modules be kept relatively independent? How can one be sure that rules from one category do not clash with rules from another category. Software QA raises its ugly head again.) Lawrence Lupton replied: This is a major challenge. This is one reason why COG is asking CRL to work in this area. If it were simple, someone else would have done it before!

The paper then moves on to implementation technologies. This is the usual list, spanning various hardware and software tools, various displays, etc.

Next, the paper surveys the international scene from 1968 to 1990. The 14 systems reviewed can be categorized along a methodology dimension:
1st generation - static procedural
2nd generation - dynamic procedural
3rd generation - dynamic declarative.
Another dimension is functionality:
alarm annunciation, filtering and prioritization - alarm massaging
diagnosis, prognosis and filtering
blackboard like integration.

Among other (less noteworthy) things, they found that:

> "Projects that are oriented for alarm annunciation, filtering and prioritization use plant functional analysis and/or alarm relationship trees as general structures to represent knowledge about alarms. Systems oriented to achieve operator support functions use causal structures or qualitative / quantitative models for knowledge representation."

The paper concludes:
- current and proposed systems tend to be knowledge based
- represent alarms using trees based on functional decomposition and causal relations
- filter and prioritize based on the various rule groupings already mentioned
- modularize
- CRT's are dominant
- significant HF issues and practical problems need to be addressed before these advanced DSS technologies can be introduced.

(Comment: Another great paper. This covers a lot of ground. It is nice to see the issues enumerated. Now, what about the details? Lawrence Lupton replied: The details will be covered as part of our COG R&D towards improving CANDU annunciation. Stay tuned for the details.

MAN88 A.M. Manzer, J.W.D. Anderson and C.W. So, "Defect Detective: An Expert System for the Detection and Evaluation of Fuel Defects in CANDU 600 Nuclear Reactors", Proceedings of the 9th Annual Conference of the Canadian Nuclear Society, Winnipeg, 1988.

Looks like a useful application. A prototype was developed but the project was dropped.

NRC81 Nuclear Regulatory Commission, "Guidelines for Control Room Design Reviews", Rep. NUREG-0700, Washington, DC, 1981.

No material of interest here. Specifics of knob design, etc. plus a call for task analysis.

OLM89 R.A. Olmstead and J. Pauksens, "New Approaches to Alarm Annunciation for CANDU Power Plants", Proceedings of the 10th Annual Conference of the Canadian Nuclear Society, Ottawa, 1989.

Not much new here. Does talk about the fact that alarm conditioning has helped but the number of sensor points has gone up. Mentions that alarm information will be based on categorization according to:

- system function status (on /off)
- user category
- action time

This will help in design of the control room displays, filtering, etc.

POP88 J.R. Popovic, J.W.D. Anderson and H.E. Sills, "The Role of Expert Systems for Supporting Nuclear Plant Operations in Canada", Third International Topical Meeting on Nuclear Power Plant Thermal Hydraulics and Operations, B6-41, November 1988, Seoul, Korea.

POP92 PRECARN-IRIS Workshop Trip Report, AECL memo from J.R. Popovic to J. Pauksens et al, file CANDU 3, 1992 March 27.

RAS86 Jens Rasmussen, "Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering", North-Holland Series in System Science and Engineering, 1986, ISBN: 0-444-00987-6.

This is a seminal work that is already well recognized by the nuclear industry. Some of the more pertinent material is summarized here for convenience:

Chapter 1: Two major trends influenced our current situation: larger and mor complex systems with centralized control and information technology. Automation does not remove humans from the system; basically it moves them from the immediate control of system operation to higher-level supervisory tasks and to longer-term maintenance and planning tasks. One-sensor-one-indicator technology is well developed and has a flat optimum. Extensive use of information technology will give a better but more peaky optimum. Probably cannot evolve; rather must jump to new designs. Thus we need a conceptual framework as a guide. (Comment: whether we can or cannot evolve is a moot point in that we need a framework anyway.)

Chapter 2: Figure 2.1 is central to the whole book. Decision making involves:

- detection
- observation
- identification
- interpretation
- evaluation
- definition of target state
- task selection
- procedure planning
- execution

It is noted that short cuts and bypasses are frequent occurrences. Common events can be handled by a reflexive jump from detection to execution. The more complex the situation, the more likely it is that the full schema would have to be employed.

Chapter 3: Two separate aspects are recognized: problem space and search strategy. (Comment: This is sometimes referred to as objects and operations on objects. The objects include the relations between objects.)

Chapter 4: The full implementation of the strategy of Figure 2.1 requires knowledge about the functional properties of the system. The way in which the functional properties are perceived depends upon the goals and intentions of the person. In general, objects in the environment in fact only exist isolated from the background in the mind of the human, and the properties they are allocated depend on the actual intentions. Figure 4.1 shows the abstraction hierarchy used in mental models:

functional purpose
abstract function
generalized function
physical function
physical form

`Why' questions are addressed from the top down; `how' questions are addressed from the bottom up.

Chapter 5: The designer and the technician have different viewpoints and problem solving strategies; indeed, they do not perceive the same situation in the same manner. In fault diagnosis, the designer uses only a few observations but employs complex data processing and high functional abstraction. The trained technician uses many observations in a sequence of simple decisions. His method is a general search procedure that is not dependent on the actual system or specific task. The technician defines his task primarily as a search to find where the faulty component is located in the system. He does not consider it to be a problem-solving task. As soon as an indication is found that a familiar, general search routine may be applied, this is chosen without considering a possible, more efficient ad hoc procedure. Records indicate that the technicians have a great deal of confidence that general search routines will ultimately lead them to the fault. Apart from the need to obtain `block-diagram understanding' of the system, it was not considered worthwhile studying the internal functioning of the circuitry. However, very rational procedures were formulated when the search cost was high, as in dangerous situations. To change a procedure, the technician has to perceive, in advance, the task as one calling for a special search strategy. Meaning is not sought by the technician. What is rational depends on the performance criteria adopted by the person.

Chapter 9: Three levels of performance are noted: skill-based behaviour, rule-based behaviour and knowledge-based (or model based) behaviour.

Chapter 10: Complexity is not an objective feature of a system; complexity perceived depended on the resolution applied. Problem-solving involves the shifting from mental model to mental model, from strategy to strategy. A major task in knowledge-based problem solving is to transfer those properties of the physical environment that are related to the perceived problem to a proper symbolic representation.

Chapter 12: The foregoing framework is not a predictive model of human behaviour, but rather a taxonomy.

ROU88 B. Rouben, D.A. Jenkins and C.R. Calabrese, "FUELEM: A Microcomputer Program to Automatically Select Channels for Refuelling", Proceedings of the 9th Annual Conference of the Canadian Nuclear Society, Winnipeg, 1988.

See LUP89a for comments.

SCO88 C.K.Scott, B.G.Nickerson and K.Ward, "ARIES: An Expert System for Regulatory Information and

Compliance Requirements", 10th Annual CNS/CNA Conference, Ottawa, Ontario, 8pp., June 4-7,1989.

ARIES is a prototype system designed to test the feasibility of a regulatory expert system directed as an automated decision support system to on-site AECB Project Officers at nuclear power stations. Implementation is centred around a commercial expert system development shell called KnowledgePro which integrates hypertext capability with graphics support on a PC delivery platform. Although nowhere nearly as "intelligent" enough for AECB staff as yet, the proof-of-concept has been made. This project was initiated by C.T.Downie (Safety Evaluation Division, AECB) and was funded under the R&D Program of AECB. The need for context sensitive and rapid reproduction of procedures in times of process upset has been proven. If such characteristics are desired for any operator companion, then this work would be a reasonable entry point for further investigations.

SIL88 H.E. Sills and J.W.D. Anderson, "Operations Decision Support Systems for CANDU Nuclear Plant Operations", Proceedings of the 9th Annual Conference of the Canadian Nuclear Society, Winnipeg, 1988.

"…operators must be provided with better information more quickly on the current status of plant components, actions to be taken, expert advice on complex situations, and the basic reason(s) for upsets."

Rasmussen quoted - the introduction of computer based information processing necessitates a reconsideration of the situation, should treat as an integrated system (designer, operator and plant); one sensor / one indicator philosophy led to many alarms so that computers had to be used to analyze alarm signals to avoid overload from the high number of alarms. Advances in computer hardware allowed better displays and DSS as per current CANDU control rooms.
This paper deals with the shorter term goal of better utilization of currently available plant information. Longer term goals have a wider scope. Paper states that the plant is in normal mode most of the time. Will get better bang for the buck if efforts were spent on programs to assist normal operation and maintenance. **More importantly, frequent use of such systems away from crisis situations would instill operator confidence in their use and increase the likelihood such systems would be used in less probable situations. (This is a quote from a station manager)**. The massaging of alarms have not entirely solved the alarm flooding problem or adequately improved the operators' ability to diagnose events. The computers ability to be exhaustive and tireless in searches offers the best prospects for automated fault detection and diagnosis.

Paper advocates:
- improved alarm annunciation,
- on-line fault detection and diagnosis,
- equipment monitoring,
- on-line procedures,
- vital parameter monitoring.

Other areas:
- modules for special tasks,
- auto testing of safety system components,
- ES tools for design and construction.

Rasmussen again: 5 levels of abstraction:
- functional purpose
- abstract function
- generalized function
- physical function
- physical form

Identifying the causes of system malfunction requires info from the lower levels.
The reasons for correct operation are derived from higher levels.

Depth of knowledge underlying human action related to:

- skill-based
- rule-based (compiled pattern matching)
- knowledge-based (model based)

behaviour. This is related to the choice of strategy:

- topographic - tries to locate sources of deviation from normal
- symptomatic - match observations with stored templates
  - pattern recognition - operator training
  - decision table search - manuals and procedures
  - hypothesis and test

The routine can be handled by pattern recognition and tables. For deeper events, need access to a deeper knowledge as per topographic and hypothesis and test. **This suggests that a number of diagnostic strategies should be made available to plant operators.**

The paper discussed a prototype (SES project at CRL)

E CONCLUSIONS AND RECOMMENDATIONS

The foregoing identifies and reports on operator aiding expert systems within the Canadian nuclear industry (and a bit beyond). An assessment of the identified projects was made with an eye to the practicality and probable implementation. To provide a context for our assessment, we provided our view of the context that we believe is appropriate. In summary, what then are the key findings?

(1) We found that there are many ways to view operator aids. There are the differing mental models of the users which lead to differing perspectives; the implications for system development are profound. But this is not the only axis of delineation. Other axes include event based vs symptom based response to alarms, human-centred vs machine-centred control philosophy, the coupling of symbolic vs numeric processes, whether one controls from the top down or bottom up, whether processes are classed as diagnosis or event driven, and whether backward vs forward chaining as used in inferencing. These all illustrate different aspects that we can use to organize our models around - none is more inherently correct than the other. We simply note the multifaceted nature of the issues when addressing operator aids.

(2) Neither engineer nor operator wants to abdicate control. The human-centred approach is the currently accepted choice. No project reviewed involved replacing human judgement.

(3) Nobody has conquered real-time analysis issues. Various strategies are under investigation and the result is not likely to be `a' way to handle real-time. Rather, the answer will be more akin to the weave of a cloth than any individual thread.

(4) No reactor site installations for operator aids are planned for the short to medium term. All projects are classed as R&D only and some are slated for testing on simulators. Pt. Lepreau and Pickering have some projects under development but they cannot be classed as operator aids since the projects are either non-intelligent display enhancements or are for the technical units.

(5) Most of past with a nuclear focus efforts are `toy projects' except for APACS in that they are small scale. Scaling up to full scope aids will provide fertile ground for developers.

(6) Very little AI appears in any of the projects. The APACS Diagnosis agent and the explanation facility at IGI are two notable exceptions. ES shells are used for graphical front end and hypertext access and presentation but this is done because the shells provide ready access to these capabilities. Their use is gross overkill and will not likely appear in more fully developed systems.

(7) AECL and OH are the main players, to no one's surprise. What is a surprise is that NB Power seems to be the place to implement. The size of the organization and the attitude of the personnel at Pt. Lepreau seem right for a site test. The supporting groups in close proximity (Maritime Nuclear, Atlantic Nuclear and the University of New Brunswick) are major additional pluses.

(8) OH has APACS and COG roles which don't communicate adequately. This arises out of the sheer size of OH and the separate funding sources, COG and PRECARN, both of which impose restrictions on information flow.

(9) AECL has CRL and CANDU arms which are not working in concert. The CRL / COG approach is HF biased but is not close enough to the control room engineers for AECL CANDU to consider the ideas to be practical. The time frames for the two groups are different but since the CANDU 3 is the platform for next generation ideas and since the CANDU 3 falls under the domain of AECL CANDU, it would seem prudent for CRL to take full advantage of the opportunity. This is our impression of the situation but it could be erroneous, given our limited inside knowledge.

(10) CRL ideas are based on a top down approach and are comprehensive while APACS is bottom up and detailed. The mental models are quite different. Will the twain ever meet? How will the twain meet?

(11) The APACS approach is model / design engineer biased and runs the risk of not being accepted by the operators. This would be a shame because the project has much merit.

What, then is the next step? We feel that the AECB should establish and maintain contact to be kept apprised of significant events. We found that the people involved in the various projects were interacting with some of the other projects. However, no one is linked to all the projects. The COG WP 16 membership provides a forum for most of the nuclear related activity but the PRECARN related work, the COG related work and the university based work are all being conducted in an insular fashion, to everyone's loss. And, of course, nobody goes out of the way to keep the AECB informed. Some mechanism needs to be established to open up communications; that is the key.

F. REFERENCES

AND90 J.W.D. Anderson, "The Use of Expert Systems for Operations Support in the CANDU Nuclear Power Supply System", report of a technical committee meeting organized by the IAEA and held in Vienna, 17-21 October, 1988. IAEA-TECDIC-542, 1990.

BER89a D.Berg and W.F.S.Poehlman, "An Accelerator Operator's Companion for the McMaster University Model FN Tandem Accelerator", IEEE Trans.Nucl.Sci., NS-36, pp.1409-1417 (1989).

BER89b John A. Bernard, Takashi Washio, "Expert Systems Applications Within the Nuclear Industry", American Nuclear Society, 1989, ISBN: 0-89448-034-0.

BER92 John A. Bernard, "Issues Regarding The Design and Acceptance of Intelligent Support Systems for Reactor Operators", ICHMT 2nd International Forum on Expert Systems and Computer Simulation in Energy, University of Erlangen, 17-20 March 1992.

BHA91 S.C. Bhatt, "Assessment of the Canadian Instrumentation and Control Technology in Nuclear Power Plants", document produced for the National Science Foundation and department of Energy, U.S.A., 1991.

COM88 J.G. Comeau, "Routine Trend Analysis Program for Plant Process Parameters", Proceedings of the 9th Annual Conference of the Canadian Nuclear Society, Winnipeg, 1988.

CRA92 John Crawford, "IGI research project: an executive overview", MPR TelTech Report #IGI92-0011, Jan.15,1992.

GAR89 W.J.Garland, W.F.S.Poehlman, N.Solntseff, J.Hoskins and L.Williams, "Intelligent Real-time System Management: Towards an Operator Companion for Nuclear Power Plants", Eng.Comp., 6, pp.97-115 (1989).

GAR90 Wm. J. Garland , "Knowledge Base Design for Heat Exchanger Selection", Engineering Applications of Artificial Intelligence, Vol. 3, # 3, September, 1990.

GAR92 Wm. J. Garland, "Dynamic Focusing in the Selection of Heat Exchangers", to be published.

GRA91 J.B.Graham, "Automated Data Management System with On-Line Fault Detection and Diagnosis", Proc. 3rd Symposium/Workshop on Applications of Expert Systems in DND, 2-3May,1991, RMC, Kingston, Ont., pp.37-46.

HAR88 R.S. Hart, "CANDU 300 - The Next Generation", Proceedings of the 28th Annual Conference of the Canadian Nuclear Association, Winnipeg, 1988.

HEY88 I.S. Hey and D.F. Meraw, "Ontario Hydro Nuclear Generation Division Information Systems at Darlington NGS", Proceedings of the 9th Annual Conference of the Canadian Nuclear Society, Winnipeg, 1988.

KIN92 D.M. King, "Systems Health Monitoring Program", Proceedings of the 17th CNA/CNS Student Conference, held at McMaster University, Hamilton, Ontario, March 27-28, 1992.

LIN88 R.P. Linsay and B.A. Rolfe, "The Development of Ontario Hydro's On-Line Computerized Wiring Information System", Proceedings of the 9th Annual Conference of the Canadian Nuclear Society, Winnipeg, 1988.

LIN92 Peter Lind and Skip Poehlman, "Design of an Expert System-based Real-time Control System for a Van de Graaff Particle Accelerator" by presented at AIENG'92: Applications of Artificial Intelligence in Engineering occurring at the University of Waterloo, Ontario, Canada from 14-17 July, 1992 (Wessex Computational Mechanics Institute, U.K.)

LUP89a L.R. Lupton, R.A.J. Basso, L.L. Anderson, and J.W.D. Anderson, "Expert Systems Use in Present and Future Nuclear Power Supply Systems", AECL - 10073, November 1989.

LUP89b L.R. Lupton, L.L. Anderson and R.A.J. Basso, "The AECL Operator Companion - An Overview", AECL - 10074, November 1989.

LUP90 L.R. Lupton, J.J. Lipsett, R.A. Olmstread and E.C. Davey, "Foundation for Allocating Control Functions to Humans and Machines in Future CANDU NPPs", Proceedings of an International Symposium on Balancing Automation and Human Action in Nuclear Power Plants, sponsored by the IAEA and OECD, Munich, July 9-13, 1990, IAEA-SM-315/28 pp 349-367, also as AECL - 10198.

LUP92a Lawrence R. Lupton, "An overview of Control Centre and Applied Human Factors Research for CANDU Nuclear Plants", extended abstract to be published.

LUP92b L.R. Lupton, "COG-Funded Applied Human Factors Research and Development", copies of overheads to be presented.

LUP92c L.R. Lupton, P.A. Lapointe and K.Q. Guo, "Survey of International Developments in Alarm Processing and Presentation Techniques", to be presented.

MAH92 Ashraf Mahmoud, Wm.J.Garland and Skip Poehlman,"Multitasking Strategies in Support of a Knowledge-based Operator Companion", AIENG'92: Engineering Applications of Artificial Intelligence VII, ed. D.E. Grierson, G. Rzevski and R.A. Adey (Elsevier Applied Science, New York: 1992) pp. 1001-1015, Waterloo, Ontario, Canada, 14-17 July, 1992 (Wessex Computational Mechanics Institute, U.K.)

MAI90 G.Maillet, "Knowledge Representation for a Power Plant Interactive Operating Advisor", Faculty of Computer Science report #TR90-050, July,1990 114pp.

MAN88 A.M. Manzer, J.W.D. Anderson and C.W. So, "Defect Detective: An Expert System for the Detection and Evaluation of Fuel Defects in CANDU 600 Nuclear Reactors", Proceedings of the 9th Annual Conference of the Canadian Nuclear Society, Winnipeg, 1988.

NRC81 Nuclear Regulatory Commission, "Guidelines for Control Room Design Reviews", Rep. NUREG-0700, Washington, DC, 1981.

OLM89 R.A. Olmstead and J. Pauksens, "New Approaches to Alarm Annunciation for CANDU Power Plants", Proceedings of the 10th Annual Conference of the Canadian Nuclear Society, Ottawa, 1989.

POE89 W.F.S.Poehlman and J.W.Stark, "Integrating Knowledge-based Systems into Operations at the McMaster Tandem Accelerator Laboratory", IEEE Trans.Nucl.Sci., NS-36, pp.1494-1498 (1989).

POP88 J.R. Popovic, J.W.D. Anderson and H.E. Sills, "The Role of Expert Systems for Supporting Nuclear Plant Operations in Canada", Third International Topical Meeting on Nuclear Power Plant Thermal Hydraulics and Operations, B6-41, November 1988, Seoul, Korea.

POP92 PRECARN-IRIS Workshop Trip Report, AECL memo from J.R. Popovic to J. Pauksens et al, file CANDU 3, 1992 March 27.

RAS86 Jens Rasmussen, "Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering", North-Holland Series in System Science and Engineering, 1986, ISBN: 0-444-00987-6.

ROU88 B. Rouben, D.A. Jenkins and C.R. Calabrese, "FUELEM: A Microcomputer Program to Automatically Select Channels for Refuelling", Proceedings of the 9th Annual Conference of the Canadian Nuclear Society, Winnipeg, 1988.

SCO88 C.K.Scott, B.G.Nickerson and K.Ward, "ARIES: An Expert System for Regulatory Information and Compliance Requirements", at CNS/CNA conference in Fredericton, June,1992 8pp.

SIL88 H.E. Sills and J.W.D. Anderson, "Operations Decision Support Systems for CANDU Nuclear Plant Operations", Proceedings of the 9th Annual Conference of the Canadian Nuclear Society, Winnipeg, 1988.

SMI89 Smith, R., "The Facts on File Dictionary of Artificial Intelligence", Facts on File, 1989, ISBN 0-8160-1595-3.

G. ACKNOWLEDGEMENTS

The authors would like to thank the AECB for suggesting that we conduct this survey and for providing the funds to do so; the survey was needed and the funds were welcome. We also thank the many individuals that we contacted. Their readiness to discuss issues with us is much appreciated. Without them, there would be little to report. And finally, we thank our families who have patiently put summer vacations on hold without complaint … well, not much anyway.

APPENDIX A

VOCABULARY

algorithm A formal procedure that always produces a correct or optimal result. An algorithm applies a step-by-step procedure that guarantees a specific outcome or solves a specific problem. The procedure of an algorithm performs a computation in a finite amount of time. Programmers specify the algorithm that the program will follow when they develop a conventional program. [SMI89]

Artificial Intelligence AI, the field of computer science that seeks to understand and implement computer-based technology that can simulate characteristics of human intelligence. Methods of symbolically representing knowledge, in a way that the computer can use the symbols to make inferences, is a central task of any artificial intelligence project. [SMI89]

attribute A property of an object. [SMI89]

blackboard A data base that is globally accessible to problem-solving applications. It serves to structure communication among multiple independent knowledge sources according to an established protocol. [SMI89]

breadth-first search A search strategy applicable to a hierarchy of rules or objects. All rules or objects on the same level of the hierarchy are evaluated before any of the rules or objects on the next lower level can be evaluated. [SMI89]

certainty factor A numerical weight assigned to a given fact or relationship that indicates the confidence a person has in the fact or relationship. Most rule-based systems use certainty factors. In contrast to probability factors, the methods for manipulating certainty factors are generally less formal than the approaches for combining probabilities. [SMI89]

declarative knowledge The representation of facts and assertions. The knowledge can be stored and retrieved but not immediately executed. The knowledge is encoded in passive data structures that must be interpreted by other procedures (procedural knowledge). [SMI89]

deep knowledge Knowledge that contrasts with surface (shallow) knowledge. Deep knowledge includes knowledge of basic theories, first principles, axioms, and facts about a domain. [SMI89]

depth-first search In contrast to a breadth-first search, a search strategy within a hierarchy of rules or objects in one rule or object on the highest level is examined and then rules or objects below that one are examined (before other top level rules or objects are searched). [SMI89]

domain expert An expert in a specific field of endeavour or knowledge whose expertise informs the expert system. Domain experts work closely with knowledge engineers in order to build knowledge-based systems. [SMI89]

expert system A computer program with a knowledge base of expertise capable of reasoning at the level of an expert in some given domain. The term is often used to refer to any computer system that was developed by means of a loose collection of techniques associated with AI research. [SMI89]

fact A proposition or datum whose validity is accepted. In most knowledge systems, a fact consists of an attribute and a specific associated value. [SMI89]

frame A data structure (or knowledge representation method) for representing declarative and procedural information in terms of predefined internal relations. Frames associate features with nodes representing concepts or objects, and are similar to records in data bases. Frames may be arbitrarily complex and have procedures (self-contained pieces of code) attached to the slots for the purpose of adding or removing values from the slots. [SMI89]

fuzzy logic Also called fuzzy set theory, an approach to approximate reasoning where the rules of inference are approximate rather than exact. [SMI89]

heuristic A rule of thumb or other device that simplifies, reduces, or limits search in large problem spaces; in particular, searches for solutions in domains that are difficult and poorly understood. Unlike algorithms, heuristics do not guarantee correct solutions. [SMI89]

inference The process of reaching a conclusion from an initial set of propositions, the truth of which are known or assumed. [SMI89]

inference engine Also known as the control structure or rule interpreter, the section of an expert system that controls the system's operation; that part of a knowledge system or expert system that makes inferences based on information in the data base. [SMI89]

KE The acronym for knowledge engineer. [SMI89]

knowledge acquisition The process of extracting, structuring, and organizing knowledge from some source, usually from a human expert, for use in a program. [SMI89]

knowledge base A collection of knowledge represented in the form of rules, procedures, schemes, or working memory elements. The knowledge base consists of facts and heuristics about a domain. [SMI89]

prototype The initial version of a developing system. The purpose of a prototype is to test the adequacy of the overall knowledge representation and inference strategies being used.

shell A domain-independent expert systems "framework", i.e., an inference engine with explanation facilities etc., but without any domain-specific knowledge. [SMI89]

symbolic reasoning Problem-solving based on the application of strategies and heuristics in order to manipulate symbols representing problem concepts. [SMI89]

symbolic versus numeric programming The two primary uses of computers. Such tasks as data reduction, data base management, and word processing are examples of numerical programming. Knowledge systems on the other hand depend on symbolic programming for manipulating strings of symbols with logic rather than numerical operators. [SMI89]

taxonomy A hierarchical classification of objects. [SMI89]

APPENDIX B

ACRONYMS

ADMS	Automated Data Management System (Spectrum Engineering)
AECB	Atomic Energy Control Board
AECL	Atomic Energy of Canada Limited
AIDE	Air Instrumentation Diagnostic Expert (Hydro Quebec)
ANSL	Atlantic Nuclear Services Ltd.
APACS	Advanced Process Analysis and Control System Project
ARC	Alberta Research Council
ARCnet	a type of local area network or LAN
ARIES	AECB Regulatory Information Expert System (ANSL)
ARK	Autonomous Robot for a Known Environment
AVAT	an ANSL project
blackboard	paradigm for a message handling computer code
CAE	CAE Electronics Ltd
CNA	Canadian Nuclear Association
CNS	Canadian Nuclear Society
COG	CANDU Owners Group
CORFFA	Control of Robots for Future Applications
CRL	Chalk River Laboratories
CSP	Critical Safety Parameter
CSPAS	Critical Safety Parameter Advisor System
DCC	Digital Control Computer
DCIEM	(CRL contact)
DOS	Disk Operating System -- single user computer operating system
DSS	Decision Support System
Echidna	a logic programming language from Bill Havens, Simon Fraser University
EFD	Early Fault Detection
ENTC	Eastern Nuclear Training Centre (at Pickering site)
EOP	Emergency Operating Procedures
EPRI	Electric Power Research Institute (U.S.A.)
ES	Expert System
ethernet	a type of local area network or LAN
EXSYS	a commercial expert system shell
FDM	Functional Design Methodology
FUELEM	Refuelling expert system
GATEWAY	name given to Pt. Lepreau's local area network
GUI	Graphical User Interface
HMSD	Human-Machine Systems Development group at CRL
HQ	Hydro Quebec
HTFS	Heat Transfer and Fluid Flow Service (CRL and Harwell)
HX	Heat Exchanger
ICHMT	International Centre for Heat and Mass Transfer
IGI	Intelligent Graphic Interface
IntelCAD	Intelligent Computer Aided Design
Internet	International Network for electronic message passing
IRIS	Institute for Robots and Intelligent Systems
IRMAD	Integrated Remote Monitoring and Diagnostic system (ANSL)
KAD	Knowledge-Aided Design
KISS	Keep It Simple, Stupid
KnowledgePro	a commercial expert system shell

KR	Knowledge Representation
LAN	Local Area Network
NetNews	an electronic news network using the internet
NIAL	Nested Interactive Array Language (Queen's University)
OADCS	Open Architecture Distributed Control System (Maritime Nuclear)
OH	Ontario Hydro
OpCoP	Operator Companion Project (McMaster University)
PDC	Programmable Digital Comparator
PRECARN	PRE-Competitive Applied Research Network
QNX	Real-time UNIX Operating System
RMC	Royal Military College
ROP	Regional Overpower Protection
RROD	Review Record of Operator Documentation
SADAU	Shutdown System Advisor
SDS1	Shutdown System One
SES	Slowpoke Energy System
SFU	Simon Fraser University
SOD	Bruce A Operating Diagram
STEAR	Strategic Technology for Automation and Robotics
TCP/IP	Transmission Control Protocol / Internet Protocol
TDS	Telerobotics Development System
U of T	University of Toronto
UNB	University of New Brunswick
UNIX	multi-user operating system for computers
WFSP	Wm. F. Skip Poehlman
WJG	Wm. J. Garland
WNTC	Western Nuclear Training Centre (at Bruce site)

INDEX

- end of document -