IAEA-IWG-NPPCI-97/1
COG-97-47-I
AECL-11772

Proceedings of the

INTERNATIONAL ATOMIC ENERGY AGENCY SPECIALISTS' MEETING ON

EXPERIENCE AND IMPROVEMENTS IN ADVANCED ALARM ANNUNCIATION SYSTEMS IN NUCLEAR POWER PLANTS

Chalk River, Canada
1996 September 17-19

Organized by the
International Atomic Energy Agency
in co-operation with
Atomic Energy of Canada Limited
and the CANDU Owners Group

IAEA-IWG-NPPCI-97/1
COG-97-47-I
AECL-11772

Proceedings of the

INTERNATIONAL ATOMIC ENERGY AGENCY

SPECIALISTS' MEETING ON

EXPERIENCE AND IMPROVEMENTS IN ADVANCED ALARM ANNUNCIATION SYSTEMS IN NUCLEAR POWER PLANTS

CHALK RIVER, CANADA

1996 September 16-20

Organized by
The International Atomic Energy Agency
in cooperation with
Atomic Energy of Canada Limited
and the CANDU Owners Group

IAEA Specialists' Meeting on
Experience and Improvements in Advanced Alarm Annunciation Systems in Nuclear Power Plants
CHALK RIVER, ONTARIO, CANADA
1996 September 16-20

Monday, September 16

18:30 - 21:30 Early Registration, Best Western Pembroke Inn lobby

Tuesday, September 17

09:30 - 09:55 ***Opening Session***
Welcoming Remarks - Dr. P.J. Fehrenbach, General Manager, CANDU Technology Development, AECL

Welcoming Remarks and Overview of IAEA Specialists' Meeting - L.R. Lupton, AECL

09:55 - 10:25 ***Session 1:*** *User Needs and Experience*
Chairperson: Eric Davey, Canada

1.1 Development of An Intelligent Annunciator System for Nuclear Power Plants
Chang-Gi Kim*, Myoung-Eun Che, Korea*

10:25 - 10:50 Coffee Break and Registration

10:50 - 12:10 ***Session 1: Continuation***

1.2 Changes in 900 MW PWR Alarm Processing Policy
Marc Pont*, France*

1.3 Improvements to the Annunciation and Display Systems at Gentilly 2 NGS -- An Integrated Approach
Raymond Dufresne*, Michel Désaulniers, Canada*

1.4 Darlington Annunciation: User Information Needs, Current Experience and Improvement Priorities
Tim Long*, Eric Davey, Canada*

12:10 - 13:30 Lunch Break

13:30 - 15:00 ***Session 2:*** *Regulatory Perspective*
Chairperson: James Easter, USA

2.1 Contribution of Computerization to Alarm Processing: A French Safety View
Williams Cette*, France*

2.2 Advanced Alarm System Design and Human Performance: Guidance Development and Current Research
John O'Hara*, USA*

2.3 Human Factors in Annunciation Systems - Recommendations for a Canadian Regulatory Framework
Suzanne Rochford, ***David Beattie****, Kim Vicente, Canada*

15:00 - 15:30 Coffee Break

15:30 - 16:15 ***Session 2: Continuation***

2.4 Safety Aspects of the Modernization of I&C and Process Information Systems in Nuclear Power Plants with Special Regard to Alarm Annunciation
Freddy Seidel*, Germany*

Discussion on papers from Sessions 1 and 2

19:00 Dinner

Wednesday, September 18

09:15 - 10:35 ***Session 3:*** *New Implementations*
Chairperson: Andreas Bye, Norway

3.1 Development of Alarm Handling Methods for Boiling Water Reactors
Yukiharu Ohga*, Hiroshi Seki, Setsuo Arita, Japan*

3.2 Alarm Processing - Ways to the Future
Dominique Pirus*, France*

3.3 Development of the Newly Advanced Alarm System for APWR Plant
Manabu Shimada*, Yoshihiro Yamamoto, Mamoru Tani, Shuichi Kobashi, Japan*

10:35 - 10:55 Coffee Break

10:55 - 12:10 ***Session 3: Continuation***

3.4 Validation of the Computerized Annunciation Message List System
Mark Feher, *Eric Davey, Lawrence Lupton, Canada*

3.5 Simulator Testing of the Westinghouse Aware Alarm Management System
John Carrera, Emile Roth, ***James Easter****, USA*

3.6 Alarm System for ABWR Main Control Panels
Yuji Kobayashi*, Koji Saito, Japan*

12:10 - 13:30 Lunch Break

13:30 - 14:00 ***Session 3: Continuation***

3.7 Reactor Alarm System Development and Application Issues
Jorge Drexler*, G.O. Oicese, Argentina (not presented)*

14:00 - 15:25 ***Session 4:*** *Alarm Structuring and Design Tools*
Chairperson: Dominique Pirus, France

4.1 An Object-Oriented Implementation to Improve Annunciation
In-Koo Hwang, Jung-Taek Kim, Dong-Young Lee, Jae-Chang Park,
Chang-Shik Ham*, Republic of Korea*

4.2 Alarm Handling Systems and Techniques Developed to Match Operator Tasks
Andreas Bye*, Baard Moum, Norway*

4.3 The CANDU Alarm Analysis Tool
Eric Davey*, Mark Feher, Lawrence Lupton, Canada*

15:25 - 15:45 Coffee Break

15:45 - 17:00 ***Session 5:*** *Moderated Discussion - Are We Addressing the Real Issue?*
Chairperson: Mark Feher, Canada

21:00 Dinner

Thursday, September 19

09:15 - 10:10 ***Session 6:*** *Integrating Annunciation and Diagnosis*
Chairperson: Chang-Shik Ham

6.1 Development Experience and Strategy for the Combined Algorithm on the Alarm Processing and Diagnosis
Hak-Yeong Chung*, Republic of Korea*

6.2 An Evaluation Approach for Alarm Processing Improvement
Jung-Taek Kim*, N.J. Na, Dong-Young Lee, Jae-Chang Park, S.J. Jong, In-Koo Hwang, Korea*

10:10 - 10:30 Coffee Break

10:30 - 11:20 ***Session 6: Continuation***

6.3 A New Diagnosis Method Using Alarm Annunciation for FBR Power Plants
Yoshihiko Ozaki*, Kazunori Suda, Shinnji Yoshikawa, Kenji Ozawa, Japan*

6.4 A Basic Design of Alarm System for the Future Nuclear Power Plants in Korea
Cheol-Kwon Lee*, Seop Hur, Jae-Hwal Shin, In-Soo Koo, Jong-Kyun Park, Republic of Korea*

11:20 - 12:20 ***Session 7:*** *General Discussion, Conclusions and Recommendations*
Chairperson: L.R. Lupton, Canada

12:30 - 13:40 Lunch Break

13:40 - 15:40 Tour of Chalk River Laboratories

Friday, September 20 (Optional)

11:30 - 15:00 Darlington NGS Tour

15:00 - 15:30 Travel to Ontario Hydro Eastern Nuclear Training Centre

15:30 - 17:00 Demonstration of Darlington Training Simulator and walk-by of Pickering A and B Training Simulators

CONTENTS

Specialists' Meeting
on
EXPERIENCE AND IMPROVEMENTS IN ADVANCED ALARM ANNUNCIATION SYSTEMS IN NUCLEAR POWER PLANTS

1996 September 16 - 20, Chalk River, Canada

Welcoming Address: Lawrence Lupton
Chairperson, Conference Organizing Committee
Atomic Energy of Canada Limited

Ladies and Gentlemen,

It is my pleasure to welcome you on behalf of Dr. Vladimir Neboyan and the International Atomic Energy Agency to this Specialists' Meeting on "Experience and Improvements in Advanced Alarm Annunciation Systems in Nuclear Power Plants". Dr. Neboyan has been unable to attend the meeting and sends his apologies.

The meeting is being held within the framework of the programme of the International Working Group on Nuclear Power Plant Control and Instrumentation, and is convened with the support of Atomic Energy of Canada Limited and the CANDU Owners Group. On behalf of the Agency, I wish to also acknowledge the Government of Canada for hosting this meeting and for providing the opportunity for participants from many nations to attend the meeting to exchange their information and experiences.

The topic for this meeting is alarm annunciation. As we are all aware, annunciation is used to ensure that control room staff are promptly alerted to important changes in plant conditions that may impact on safety and production goals. Traditional annunciation systems incorporate alarms derived directly from plant analog and binary data. The use of individual set-points for process parameters and the annunciation of each violation separately is an approach still prevalent in most plant control rooms. This method may be satisfactory during normal operation and minor disturbances, but can lead to an avalanche of alarms during plant upsets, transients and other

abnormal situations. It is at these times that the operator should be provided with additional support and advisory functions to assist in maintaining the safety of the plant.

The need to improve alarm annunciation systems in nuclear power plants was recognized about two decades ago. The following two quotes, both from published material in 1974, provide a historical perspective.

> "Alarm systems are often one of the least satisfactory aspects of process control system design. There are a number of reasons for this, including lack of a clear design philosophy, confusion between alarms and statuses, use of too many alarms, etc. Yet, with the relative growth in the monitoring function of the operator, and indeed the control system, the alarm system becomes increasingly important." [Edward and Lee, "The Human Operator in Process Control", Taylor and Francis Limited, London, 1974, page 418].

> "Alarm systems in general are unsatisfactory, particularly those in computer systems which rely on typewriter print out. Alarms will mushroom after a system is installed; and a better hierarchy strategy is needed. Everyone shutters at the analysis job required to plan and rationalize such systems." [Williams, "Interface Problems in Process Control", Survey paper IFAC/IFIP Symposium, Zurich, 1974, page 63].

It was the Three Mile Island (TMI) accident in 1979 that triggered a large research effort throughout the world. This initial work tended to focus on the use of conventional technologies to address the issues. Since then, the requirements for control rooms and human-machine interfaces, including annunciation, have changed dramatically as a result of:

- evolution of new standards for control room design,
- technological advances in information processing and presentation, and

- evolution of licensing requirements that take increasing account of human factor issues throughout the entire plant (e.g., human-machine interface and human performance).

In addition, the importance of the human-machine interface in supporting operations staff to meet plant availability and safety goals has grown as a result of:

- increased plant complexity that has made it more difficult for the staff to cope with plant information presented in conventional ways, and
- the recognition of the role of inadequate human-machine interfaces in contributing to plant upsets and major industrial accidents.

The current IAEA program on control and instrumentation and nuclear power plant computerization and human-machine interface studies promotes technical information exchanges among Member States with an interest in exploratory or research programs, and publishes reports available to all Member States. The IAEA activities are co-ordinated by the International Working Group on Nuclear Power Plant Control and Instrumentation, which meets periodically to review national programmes of the countries, and to advise the IAEA on its technical meetings and activities where current progress, problems and operating experience are discussed.

The objective of the meeting is to provide an international forum for the presentation and discussion on R&D, in-plant experiences and improvements to annunciation systems. In planning the meeting, we have fully recognized that annunciation is an integral part of control centre design and plant operation. However, we have proposed to keep the meeting focussed on annunciation-related topics so as to maximize the benefits from the discussions. Among us this week, we have 62 participants from 9 countries presenting 22 papers. Further, these representatives are from utilities, design/engineering, research and development, and regulatory organizations. The meeting is organized into 7 sessions, focussing on a specific aspect or perspective on annunciation. Time has been allocated at the end of each day to allow further

discussion on the topic. This should make for an excellent forum to discuss the whole field of annunciation.

In closing, I would like to express my thanks to the members of the Organizing Committee who supported me in the planning of this meeting.

On behalf of Dr. Neboyan and the IAEA, I wish us a successful and productive meeting.

SESSION I

USER NEEDS AND EXPERIENCE

DEVELOPMENT OF AN INTELLIGENT ANNUNCIATION SYSTEM FOR NUCLEAR POWER PLANTS

Chang-Gi Kim, Manager, and Myoung-Eun Che
Instrumentation & Control, Yonggwang Nuclear Units 1&2
Korea Electric Power Corporation
Republic of Korea

ABSTRACT

Yonggwang Nuclear Units 1&2 have developed an intelligent annunciation system to replace the existing obsolete system and to enhance operator support. The new annunciation system, which is currently operating at both units, uses the distributed control technology to enhance reliability and to provide versatile function to operations and maintenance personnel. The hardware and software configuration is based on redundancy so that a component failure would not initiate system malfunction. The data base of the new system provides, through a touch screen, an automatic alarm response procedure for selected alarms, which increases availability of information for plant operation. Other KEPCO nuclear units and the fossil plants are considering installing the new system.

1. INTRODUCTION

Except the newly constructed nuclear plants, Instrumentation and Control systems of operating nuclear plants in Korea do not benefit from the advanced state-of-the-art technology. Recently, Industry trend shows that digital technology is utilized to replace analog based instrumentation and control systems in order to enhance their productivity through automation, standardization and simple maintenance. Most of the operating I&C systems in Korea were designed and fabricated during the 70s, and the systems are experiencing aging problems which result in significant operating and maintenance cost and sometimes in plant scrams.

Recent researches and regulations start introducing high technology to nuclear industry to guarantee higher reliability and to have diverse flexibility of the I & C systems. After the TMI Accident, the USNRC issued NUREG-0737 requiring new additional function and systems to overcome the Human Engineering Deficiencies and to provide operators with upgraded human performance enhancements. The industry has developed systems to meet the performance and reliability requirements.

Operators acquire plant situation and take appropriate actions according to the information available in Main Control Room. The alarms, status lights, indicators and recorders are provided to assist the operator's decision. The previous annunciation systems of the Yonggwang Nuclear Units 1&2 used the technologies of the 70's that was mainly composed of hard wiring method and provided a simple visual and audio alarming function to operators. So the operators were mainly depending on their experience and knowledge to analyze the transient situation and to

decide their immediate actions. When a number of alarms are simultaneously received, it is hard to discern the priority of the received alarms. Also, systematic analysis was difficult as the system lacked the alarm recording function. Furthermore, maintenance of the system also required higher manpower and cost. In order to overcome the problems and to enhance system reliability, YGN Units 1&2 have developed a New Intelligent Annunciation System based on a distributed control technology.

2. DEVELOPMENT OF INTELLIGENT ANNUNCIATION SYSTEM

2.1 Major Development Schedule

(a) Project Feasibility study: '90.1 ~ '90.7
(b) Work Scope review : `90.8`92.12
(c) Technical review : `93.1`93.12
(d) Basic Specification Preparation: `94.1`94.4
(e) Contract volunteers audit and QA approval : `94.1`94.5
(f) Procurement Preparation and Contract : `94.5`94.7
(g) System manufacturing and factory inspection : `94.8`94.10
(h) Interim Installation and Performance Test : `94.11`95.3
(i) YGN Unit 1 Final Installation and Performance Test: `95.3.27`95.4.30
(j) YGN Unit 2 Final Installation and Performance Test: `95.9.10`95.10.10
(k) The New Intelligent Annunciation System is operating at both Units.

2.2 Project Necessity Review

Besides the previous system's aging and maintenance problem, the following shows the necessity of new annunciation system.

2.2.1 Frequent Problems Due To System Aging

The system was experiencing accelerated failure rates due to both unsuccessful connection contacts of the Patch board and failures of electronic cards of the system.

2.2.2 Maintenance Problems

Such a simple work as verifying the electric contact of the patch board required shut down of the entire annunciation system, which accordingly was not allowed during normal plant operation. When a work is done on the patch board, the entire input and output points (Input: 2,250 points, output: 1250 points) have to be checked out for proper electrical integrity of the input output channel.

2.2.3 Necessity of a Diverse Annunciation Function

The previous system had limited flexibility to accommodate the following versatile annunciation function.

- Introducing a Black board concept to MCR annunciation window
- Trip Window (Primary and Secondary system separation)
- Identification of the First-out Alarm
- Relocation of the Alarm Windows according to priority, function and system (Human Engineering Deficiency Upgrade)
- Identification of the Cause of a multi- input Alarm
- Annunciation system failure indication
- Alarm Recording, Storing for root cause investigation

2.3 Scope of Development

Figure 1 shows block diagram of the previous annunciation system, among the system components, Logic Boards, Reflash Boards and Patch Board that have frequent failure rates are selected to be upgraded. The power supply upgrade was also decided and the other components are used to compose the new system. Table 1 shows the scope of the project.

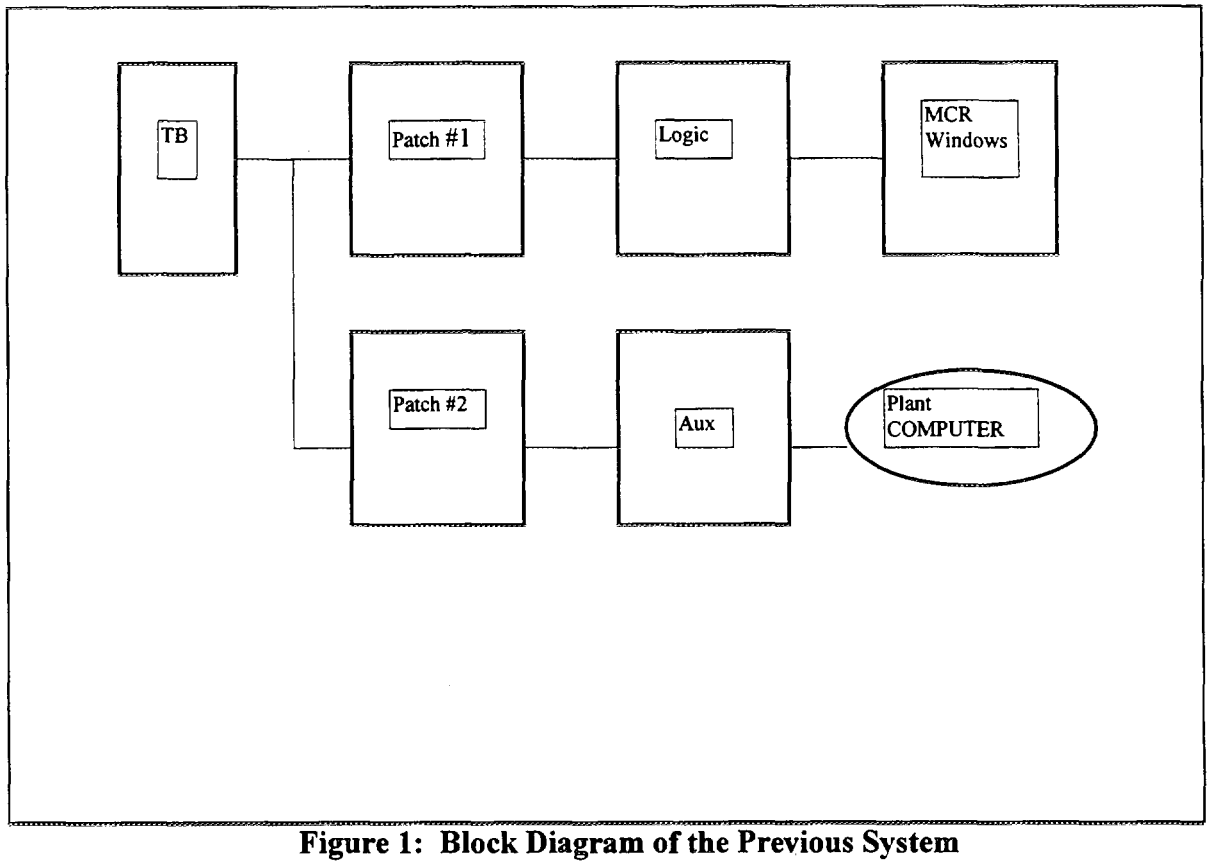


Figure 1: Block Diagram of the Previous System

Items	Quantity	Scope
TERMINAL BLOCK ASSEMBLY	89 sets (2250 Point)	use
AUX. RELAY RACK	5 sets(125 ea.)	use
LOGIC BOARD RACK	50 sets(1250 ea.)	develop
REFLASH BOARD RACK	7 sets(175 ea.)	develop
PATCH BOARD RACK	2 set	develop
POWER SUPPLY	11 set	develop

Table 1: Scope of the Project

2.4 Direction and Strategy

2.4.1 Direction of Development

2.4.1.1 Maintain Reliability of the Annunciation System

Considering the importance of the system, it should be designed to overcome a single failure or multiple failures so the system utilizes DCS, that is also based on redundancy, from the input to the output.

2.4.1.2 Enhance Operations Support Capability

While the previous system simply provided alarms to operators, the new system provides processed information that contains operators actions in response to a received alarm, which is based on a specially designed data base.

2.4.1.3 Simple Operation and Maintenance

As some modifications require annunciation system reconfiguration, during normal system operation, the new system should accommodate the on-line reconfiguration by a simple software modification. The system also should be maintained on-line without affecting system operation. It should have a self-diagnosis function that can support maintenance.

2.5 Development Strategy

2.5.1 Redundant Structure of Communication Network

The annunciation system provides the first information to operators when there is a transient in plant. Thus, the system should be ready for a possible failure mode anticipated in the system. One of the possible problems with a DCS could be a failure of the communication network that connects various distributed components. A network failure could paralyze the entire system that leads to a system shutdown. So the following principles should be preserved.

1. Each main and sub network should have physically independent cable networks
2. The communication modules of the Main and Sub network should be independent each other.
3. The communication modules of the Main and Sub network should have an independent power supplies.

2.5.2 Distributed Structure of the IN/OUT Processing

As previously mentioned, the annunciation system requires high reliability. The system reliability is not guaranteed when a single module controls the entire input and output of the system, for a failure of the module will affect system operation. So, the higher is the number of in/out points assigned to a module the more is the effect of the module failure and system maintenance. Therefore, the new system utilizes a distributed control concept that a unit handles 125 In/Out points and a module processes 16 In/Out points.

3. THE NEW INTELLIGENT ANNUNCIATION SYSTEM

Figure 2 shows the configuration of Intelligent Annunciation system and Table 2 lists the components of the new system.

The new system has the ability of processing 4,096 channels of dual inputs and 2,048 channels of dual outputs. It processes 10,000 simultaneous inputs(events) and stores 240,000 events. The new system has delay time of 0.1 second from input to output, whereas other customized DCS have delay time of over 5 seconds. It uses triple back-up or redundancy in response to failure of both the primary and secondary systems. Korean Standard Time is used to synchronize the system time and IEEE 802.3 standard is implemented to facilitate further system upgrade in the future.

New various functions such as, Identification of the first-out alarm, versatile display, alarm recording, data processing and history management, self diagnosis and fault detection enable the operators to have rapid, accurate and reliable information as well as easy maintenance. The Alarm Response Procedures that contain information regarding the source of the alarm, related automatic actions, required immediate operator actions, post actions and setpoints are available by the new annunciation system through a touch screen monitor located in main control room.

Item Components	Quantity of Subracks	Train	SUBRACKS			
			In/Out capacity	Number of I/O cards	Number of comm. card	Points/ Card
SSU	18	MAIN	128	8	2	16
		SUB	128	8	2	16
ACU	27	MAIN	64	4	2	16
		SUB	64	4	2	16
ADU	*4*	MAIN	128	8	2	16
		SUB	128	8	2	16
MPU	2	MAIN	Input : 4096 Point Output : 2048 Point Number of card : 7 EA/Unit			
		SUB				
PSU	6	Power supply to SSU and ADU				
ECU	1	ENGINEERING Console				
PRINT	2	For ECU only : 1EA for Logging only : 1EA				
Total	SUBRACK : 57SET POWER SUPPLY : 102 SET CARDs : 778 EA - Input CARD : 288 EA - Output CARD : 280 EA - Comm. CARD : 210 EA					

Table 2: Components of the New System

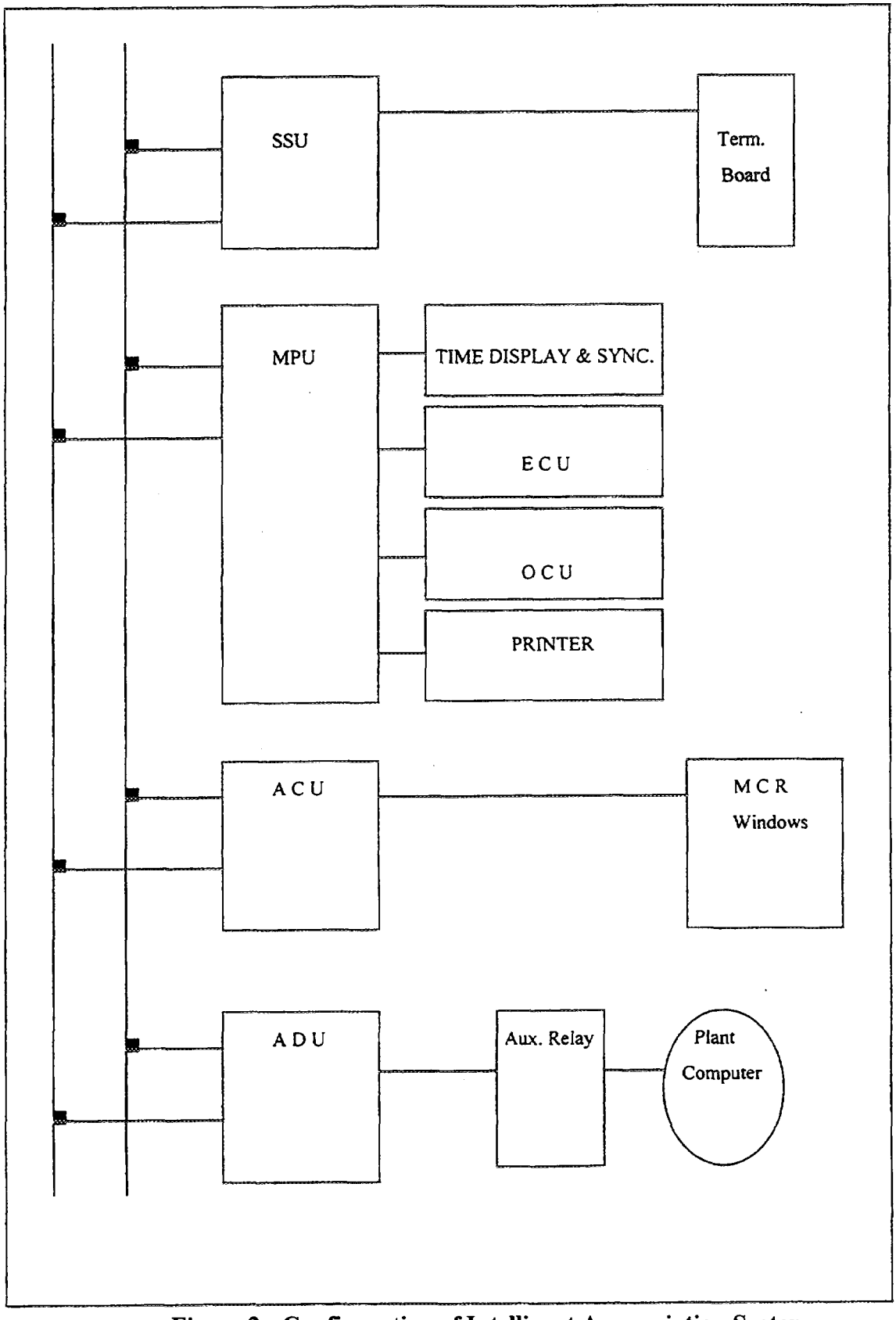


Figure 2: Configuration of Intelligent Annunciation System

3.1 Major Features of the Intelligent Annunciation System

3.1.1 Identification of the First-Out Alarm

The first-out alarm has different flashing rate so that operator easily notices the first out alarm.

3.1.2 Installation of Alarm Response CRT

Alarm response DATA BASE is constructed that contains over 2,000 pages of the previous paper procedure, and the information is accessible by a simple operator's touch on the monitor screen. *Figure 3* shows the example of Alarm Response CRT. Figure 4 shows the one of the automatic Alarm Response Procedures.

# 2 ANNUNCIATION SYSTEM							
ALARM TREND					**MAIN ACTIVE**		**1995/10/18 09:09:09**
11:25:06:234 LOOP 3 STEAM PRESS RATE HIGH ALARM 914-02(SO) **11:25:06:600 LOOP 3 STEAM PRESS RATE HIGH RESET 914-02(SO)** **11:25:07:222 SAG 1 WT. LEVEL LOW-LOW ALARM 912-41(SO)** **11:25:07:955 SAG 1 WT. LEVEL LOW-LOW RESET 912-41(SO)** **This is the end of TREND**							
UP	**DOWN**	**PG UP**	**PG DOWN**	**CLEAR**	**Actions**	**GROUP**	**Append**

Figure 3: ALARM TREND Screen

# 2 ANNUNCIATION SYSTEM		
UA-912-41 : SG 1 WTR LVL LO-LO	**MAIN ACTIVE**	**1995/10/18 10:10:10**

Anununciator 131
S/G Level Control board(JP007 A,B,C) Rev : 1 21/75
Location : JP007A-41
SG 1
Source : AE-LB-473A,474A,
WTR LVL 475A,476A
Set Point : Below 17 %
LO-LO of S/G narrow range
Computer DATA POINT : LD0406
LD0403,LD0404,LD0405

1.0 Cause of alarm

1.1 S/G level control In/Out Signal Abnormal
1.2 Failure of MFCV or Low Power Feed water control valve
1.3 Level Shrink by cold water injection or MSIV close
1.4 MFWP turbine Speed control Abnormal
1.5 Feed line or Steam line Break
1.6 Level Instrumentation failure

2.0 Automatic Actions

2.1 If more than 2/4 channels are lo-lo level
2.1.1 Reactor Trips
2.1.2 S/G Blowdown and Sampling system Isolation
2.1.3 Two Motor Operated Aux. Feed water pumps Start
2.1.4 If more than 2 S/Gs meet more than 2/4 channel 'lo-lo' level,
Turbine Operated Aux. Feed water pump start

3.0 Immediate Actions

3.1 Place S/G level controller from 'Auto' to 'Manual'
Increase the level above the set point level.
3.2 Select other level control input signals when instrument channel fails.

4.0 Post Actions

4.1 Stabilize S/G level By Stabilizing the TBN power .
4.2 Perform Abnormal procedure No. 915 (S/G level Instrumentation Failure).

5.0 Refer to

5.1 DWG : 3-M-AE-F003 Rev. 6
3-J-SB-204 Rev. 4
2326D97, Sheet 7(Rev 1), Sheet 13(Rev 1) (M1-300-18)

UP	DOWN	PG UP	PG DOWN	PRINT	Prev.	Next	Exit

Figure 4: Alarm Response Screen

3.1.3 Versatile DATA Management

The system uses battery backup SRAM module in response for a power supply failure, which also enhances reliability of data storage. All the stored data can be sorted by time, window and system

3.1.4 Various Output Processing

The logging printer prints out the Alarm, Delay and system reports.

3.1.5 Self Diagnosis

All the system components are checked out for proper operation and the results are displayed with status LED and System report and according to the failure modes MPU priority is decided and the transfer is automatically achieved.

3.1.6 Triple Back-Up Mode of Operation

1. Auto Mode

   When a failure is detected on either Main or Sub train the operation is transferred to either train which has no failure.

2. Manual Mode

   (a) Main mode: Despite a failure in the main train the system is not transferred.
   (b) Sub mode: Despite a failure in the Sub train the system is not transferred.

3. Emergency Mode

   When both the main and sub train fails, the system directly connects input networks and output network so that the system continues operating without the control of MPU. This is accomplished by the watch dog timers installed at each module, which control the transfer when they detect a MPU or CPU failure.

3.1.7 On-Line Maintenance

Each In/Out module can be extracted from system not affecting system operation. An alarm point reconfiguration also will not affect system operation and the result of reconfiguration can be directly verified

3.1.8 Testability

Proper operation of the system can be checked out during normal operation and during a refueling outage. The total system check-out takes about 40 minute and the test result is automatically reported.

3.1.9 System Time Synchronization

The Korean national standard time synchronizes the system time clock to provide a plant standard time base.

3.2 System Hardware Description

3.2.1 Main Processing Unit (MPU)

1. This Unit stores the event data and provides versatile outputs by processing signals from the SSU
2. Processes maximum of 4,096 input points and 2,048 output points
3. Mapping the In/Out Points
4. Utilizes a battery back-up SRAM
5. Operates Event Logging Print
6. Direct Communication with the ECU when system fails
7. Self Diagnosis
8. Time Synchronization
9. Auto, Manual, Emergency Modes of Operation

3.2.2 Sub-Scanner Unit(SSU)

1. Redundant Input signal processing And maximum of 1 milli-second to scan the entire inputs (2,250 points) and to transfer data to MPU
2. Each sub-rack processes 125 points
3. According to the input type (N.O/N.C), the output data is determined
4. Direct communication with The ACU when MPU fails
5. Entire Time base synchronization
6. Event processing and Disable display on a on-line maintenance
7. Self diagnosis

3.2.3 Annunciation Control Unit (ACU)

1. Actuates the MCR alarm windows according to the MPU data
2. Different Flash rate actuation
3. Fast Flash: Alarm Received
4. Slow Flash: Alarm cleared
5. Slow-Slow Flash: the first-out alarm
6. Direct communication with the SSU when MPU fails

7. Each Sub-rack processes 64 output points
8. Annunciation
9. Identification of the first out alarm
10. Reflashing the recurring alarm
11. Time base synchronization
12. Self diagnosis
13. Event processing and Disable display on an on-line maintenance

3.2.4 Aux. Driver Unit (ADU)

1. Operate the Aux. relay board by communicating with the MPU
2. Each Sub-rack processes the 128 outputs
3. Direct communication with the SSU when MPU fails
4. Self diagnosis
5. Time base synchronization
6. Event processing and Disable display on an on-line maintenance

3.2.5 Engineering Console Unit (ECU)

1. Event Data History management and output
2. Edits Data configuration
3. On-line Communication with the MPU
4. Pull-down menu operation

#2 ANNUNCIATION SYSTEM						
GROUP				MAIN ACTIVE	1995/10/10 10:10:10	
UA-901	UA-902	UA-903	UA-904	UA-905	UA-906	UA-907
UA-908	UA-909	UA-910	UA-911	UA-912	UA-913	UA-914
UA-915	UA-916	UA-917	UA-918	UA-919	UA-920	UA-921
UA-922	UA-923	UA-924	UA-925	UA-926	UA-927	
PRINT		WINDOW		TREND		APPEND

Figure 5: GROUP Screen

# 2 ANNUNCIATION SYSTEM				
UA-912-41 SG 1 WTR LVL LO-LO			MAIN ACTIVE	1995/10/18 10:10:10
1	2	3	4	5
11	12	13	14	15
21	22	23	24	25
31	32	33	34	35
41	42	43	44	45
PRINT	ACTION	GROUP		APPEND

Figure 6: Alarm Window Screen

4. CONCLUSION

The new intelligent annunciation system is currently operating at Yonggwang Nuclear Units 1&2 with good system condition. Plant operations and maintenance are satisfied with the new system. KEPCO Kori Nuclear Units 3 & 4 are preparing installation of the system and this system will provide best information to operations and maintenance.

XA9744355

CHANGES IN 900 MW PWR ALARM PROCESSING POLICY

Marc Pont
Electricite de France - Generation and Transmission
Nuclear Power Plant Operations
Paris, France

ABSTRACT

Following a brief description of the current 900 MW PWR alarm processing system, this document presents the feasibility study carried out within the scope of the Instrumentation and Control Refurbishment project (R2C).

1. ORGANIZATION OF 900 MW PWR UNIT INSTRUMENTATION AND CONTROL

1.1 General

A nuclear power plant has specific instrumentation, control and monitoring needs. The instrumentation and control (I&C) of a 900 MW PWR unit is designed to ensure that three principal functions are always carried out with maximum reliability and availability. These three functions are:

- The I&C of normal operation (startup, power increase, power changes and outages) using a logic circuit control system.
- The control of a certain number of parameters using analog or digital control systems.
- The protection of staff and equipment by rapid shutdown and the activation and control of safety systems via a protection system.

Each of these functions receives the necessary information from the main equipment (reactor, steam generator, turbine, diesel-generator sets, etc.) via the appropriate instrumentation (sensors and measurement devices), and activates the control devices (valves, motors, contactors). Each system is also connected to the control room via manual devices and through visual information (LEDs, recorders, displays, screens and alarms).

Monitoring and control tasks are the responsibility of the operating teams. Their job is to analyze situations and take the appropriate action on the basis of information transmitted to them in the control room, in particular via the alarm processing system.

1.2 The 900 MW PWR Control Room

Under normal conditions, unit operation is ensured by two operators from the control room, with the support of technicians in the different part of the plant.

The control room centralizes all the I&C, verification, signaling and monitoring devices required for normal operation, as well as those associated with nuclear safety.
The main area of the 900 MW PWR control room comprises a front control console and vertical boards on the 32 units in the 900 MW PWR CYP series and the Bugey plant (see Figure 1).
The main features of the control room are:

- Its functional layout:
  - functional grouping of instrumentation (recorders, indicators, control devices, etc.),
  - differentiated control equipment: horizontal and vertical boards,
- Classification of control information and devices by:
  - the position of equipment in relation to their usage,
  - distinguishing the basic system using a thick border and distinguishing between the main and secondary areas of the same group of controls (basic system) using a thin border,
- Enhanced visibility and differentiation of equipment thanks to:
  - partial, active mimic panels representing static devices or equipment using colored figures,
  - a distinction between functional areas using contrasting background colors,
  - the use of colored boxes and borders to designate inlet valves or motor valves and their alignment,
  - a separation of electrical channels and different color coding representing these channels,
  - standardized positions for status indicators and associated controls,
  - standardized labeling system: alphanumeric capital letters in three different character sizes, and
  - systematic indication of the electrical board which powers the device in the control room.

The control room at the two Fessenheim units has a specific design, with a U-shaped console and no front control console, similar to the plants in the 1300 MW PWR series.

1.3 Control Data

Control data is information needed by the control room operators to:

- start up or shut down a unit,
- rectify operating incidents to allow the unit to remain connected to the grid, and
- safeguard equipment for which there are no automatic protection systems.

This information is provided using conventional means:

- the status of actuators is shown using status indicators or turn-to-push discrepancy switches,
- the status of utilities and systems and external core measurements are transmitted via indicators or recorders, and
- abnormal or faulty status is shown on alarm windows, with each fault classified according to the degree of urgency of the operator action.

In addition, a computer and data processing system (known as the KIT), provides the operator with more sophisticated data than conventional information systems. This system ensures centralized data processing is based on the acquisition of around 5,000 logic data items and 1,500 analog data items transmitted by the unit.
The system has the following main functions:

- it is the principal monitoring tool for most rotating machinery,
- it complements the control room alarm windows to locate the source of the failure, and
- it is a high-speed unit operation analysis tool.

The control room interface comprises three screens, a keyboard and a trackball. This system is supported by the Safety Panel (KPS), which provides operators with a set of hierarchic and summarized information concerning safety systems.

The interface consists of a control room workstation, comprising: status indicators, core cooling monitoring system, three semi-graphic screens and two keyboards.

Lastly, a graphic data display system (KGB) has been added to the control room to accommodate new applications and round out the alarm and imaging features of the KIT system. It comprises two screens, a trackball and a mouse.

2. ALARM PROCESSING - RULES AND PRINCIPLES

2.1 Definition of an Alarm on a PWR Unit

An **alarm** is a message sent to control room operators to warn them of a malfunction or an installation condition and **to request corrective action.**

The link between the **malfunction, alarm and corrective action** is essential.
The following must therefore be defined for alarms:

- the area to be monitored, for which the **operator** is required to undertake corrective action within the scope of his **job function,**
- the notion of **minimum corrective action**, short of which the event is considered to be instructive, and over and above which it involves an alarm, and
- processing and display aids, which can be a display window or a screen on one of the additional information systems (KIT or KGB).

2.2 Alarm Classification According to Their Display in the MCR

We can round out the above components by specifying the alarm indicator used. It is recommended to classify alarms according to the degree of visibility of the alarm in the control room and the speed with which the operator is required to take the appropriate action:

- **Category 1 alarms – red**, requiring urgent action by the operator, should **preferably be integrated in the alarm windows**. They could remain temporarily on the KGB screen when new alarms are generated to ensure faster responsiveness.
- **Category 2 alarms – yellow**, associated with a deferrable operator action, can be integrated in the **illuminated display windows** or in the KGB screens. The different indicators are selected according to the degree of importance of the monitored equipment (safety-significant or not).
- **Category 3 alarms – white**, associated with automatic actions other than shift to no-load or a safeguard action, are displayed on KGB screens. They may be on display windows, but the latter should be reserved for other alarm categories,
- **Category 4 alarms – green**, associated with automatic safeguard actions or shift to no-load, must be integrated in **alarm windows**.

Moreover, information relating to events which do not require minimum operator action are centralized on the additional information processing system: KIT. This information does not fall within the scope of alarms and must not initiate audio alarms or acknowledgment by operators.

Alarms retransmitted on alarm windows covering several identical equipment items must have the same layout on the boards in the control room. This also applies to sets of identical alarms retransmitted simultaneously in channels A and B.

2.3 Summary of Alarm Processing

<table>
<tr><th>Automated Action</th><th>Malfunctions Impacting on Safety</th><th>Malfunctions Impacting on Availability</th><th colspan="3">Other Malfunctions</th><th>Alarm Color</th><th>Recommended Alarm Indicator</th></tr>
<tr><td>Safety-availability action - Cat. 4</td><td>Action < 10 min
(10 min, level 2 accident)
(10 to 20 min, level 3)(10 to 30, level 4)</td><td>Action < 10 min</td><td colspan="3"></td><td>Green</td><td>- Alarm window
(900 MW)</td></tr>
<tr><td rowspan="2">Automated action other than Cat. 3</td><td colspan="2" rowspan="2"></td><td>Control room resources</td><td>Control room or electrical equip. room</td><td>Decentralized resources</td><td rowspan="2">White</td><td rowspan="2">- Screens
. KGB
. KIT</td></tr>
<tr><td>< 2 mn</td><td>< 10 mn</td><td>< 20 mn</td></tr>
</table>

Operator Action		Corrective Action			Alarm Color	Recommend Alarm Indicator
		Control room resources	Turbine hall resources	Decentralized resources		
Urgent action - Cat. 1		2 < T < 5	10 < T < 20	20 < T < 30	Red	-Alarm window
Deferred action - Cat. 2		> 5 mn	> 20 mn	> 30 mn	Yellow	-Safety-significant equipment: . alarm window - Non safety-significant equipment: . alarm window .KGB screen

2.4 Alarm Management

2.4.1 Principles

The **appearance** and **disappearance** of a malfunction must be signaled separately by **indicator lights.**

Each appearance or disappearance (or reappearance) of an alarm must be accompanied by a – **single** – **audio signal** to warn the operator.

2.4.2 Audio and Light Sequences

Audio and light sequences must comply with the following table:

CAUSE	CONSEQUENCE
Appearance of malfunction	Ringing and flashing or distinctive "appearance" labeling
Disappearance of malfunction before acknowledgment	Ringing and flashing or distinctive "disappearance" labeling (different to the former)
Acknowledgment after appearance	Audio signal stopped - alarm becomes steady light or normal display
Disappearance of malfunction after acknowledgment	Ringing and flashing or distinctive "disappearance" labeling
Acknowledgment after disappearance	Audio signal stopped (if no time delay applied) and alarm deactivated or removed

2.4.3 Processing Procedure

In terms of hardware, the aforementioned processing is distributed as follows:

Processing	Transmission	Management	Display
Equipment	Relays	"Auxitrol" cabinet	Alarm windows or screens

2.5 Alarm Management During Outage

Alarm processing is designed to operate with **all indicator lights off**, in order to only show an alarm if it requires operator action. This system was **designed and installed** on 900 MW PWR units **in operation** and already connected to the grid.

The alarm processing system was not designed for outage conditions. A certain number of alarms are involved, many of which are not applicable for the following reasons:

- the alarm does not correspond to a malfunction under outage conditions; it may be characteristic of the outage, equipment maintenance or the position of a device during outage;
- several alarms indicate the same malfunction at difference levels of importance;
- an alarm can indicate a minor malfunction during a given unit conditions which does not need to be signaled to the operator.

All of these alarms disturb the operator and contribute to making alarm handling during outage less reliable.

3. I&C REFURBISHMENT FEASIBILITY STUDY (R2C PROJECT)

In April 1993, EDF launched a project to carry out the preliminary feasibility studies of refurbishments to the instrumentation and control system of the CP0 and CPY 900 MW PWR reactor series: "the R2C project".

3.1. Project Description

This project included an "I&C Aging Study Committee" and a "Short Preliminary Project". The preliminary project was launched at the same time as the committee in order to plan ahead for the study of possible refurbishment actions for the first site to undergo the second ten-yearly inspection: Gravelines in 1998.

Three strategic orientations underpinned the preliminary project:

- the replacement of "obsolescent" equipment before the third decade of operation;
- the preservation of the original safety principles;
- the integration of only those modifications which would result in safety improvements or availability gains.

3.2 Control Room Refurbishment Hypotheses

The main hypotheses of the study were as follows:

- maintain a maximum number of alarms in alarm windows, in particular Category 1 alarms (red);
- maintain the audio and light sequences;
- respect the alarm policy;

- possibility of installing distributed control room screens for Categories 2 and 3, and possibly Category 4 (green), which are not incident or accident operation mode signals. These screens will be the information vectors for the upgrading of the supervision system.

The main functional improvements requested are:

- seek functioning based on indicator lights being in the off position during outage,
- separate malfunctions grouped under the same alarm window.

3.3 Solutions Examined in the Short Preliminary Study

The short preliminary study concentrated on existing difficulties, i.e., the following two aspects:

- Saturation of the alarm windows and processing cabinets. Saturation made it impossible to add new alarms rendered necessary by the planned technical modifications.
- Improvements to alarm monitoring during outage to allow the operator to easily distinguish between alarms which require operator action and those which are triggered under normal conditions by the status of the unit or the outage of certain equipment.

3.3.1 Saturation of Alarms in the Control Room

Following the modifications planned for the second ten-yearly inspection, two types of components are subject to saturation: the processing cabinets and alarm windows. The following is proposed for the processing cabinets:

- add a cabinet for channel A and a cabinet for channel B.

To avoid alarm window saturation, the following is proposed (see figure 2):

- **add an extension block** to the control console, which would free up alarm windows;
- **reduce the size of the alarm windows** in the control boards, which would free up considerable space.

In terms of hardware, LEDs could be used, which would also avoid having to frequently replace indicator lamps. Just adding an extension block to the control console would make it possible to make sufficient improvements. However, this solution presents the major drawback of not respecting the geographic distribution of alarms associated with the control devices. This is why is it is recommended to modify both the control consoles and the control boards.

3.3.2 Alarm Management Problems During Outage

Three solutions were examined:

- replace the alarm processing cabinets by controllers and **add 9 screens** in the control room; this solution is similar to the organization of the 1300 MW PWR control room;

- add a system with a dedicated screen for monitoring important alarms during outage, with alarm processing based on **"centralized management"**;
- add a **"filter screen"** type mechanism to alarms which are not significant during outage. This solution would spotlight important alarms to be monitored during outage (see Figure 3) and is thus dubbed "mechanical filtering".

The following table summarizes the advantages and disadvantages of each situation:

SOLUTION	ADVANTAGES	DISADVANTAGES
Screens distributed throughout the control room	- Known solution (exists on 1300 MW series) - Respects the alarm policy - Saturation problem automatically resolved - An open system with possibility of data processing	- High cost, complex functional studies - Modification of several specs - Intensive training required (control engineers, operations personnel) - Test system must be reviewed - Control boards must undergo earthquake resistance tests - Probably a very tight schedule
Screen for alarms during outage **Centralized management**	- Limited functional study	- Centralization does not comply with the control room approach (alarms near to the controls) - Specific development - Availability of a "critical" system during outage
Current control room with the addition of **mechanical filtering**	- Simple and pragmatic solution - Inexpensive in terms of development and maintenance - Minimum functional studies - Operation procedures remain the same - Little impact on operations documents	- Prevents any subsequent modifications to the control room throughout its operational life - Leads to inconsistencies in the alarm policy - Deemed very "rustic"

Following are the estimated costs for each solution:

SOLUTION	COST
Distributed screens	FFr25 million for the first unit, FFr8 million for the following
Centralized management	FFr2 to 8 million for all units (this option has not been studied in detail)
Mechanical filtering	Estimated FFr3.5 million for all units

Finally, it is unlikely that alarm processing on the 900 MW PWR series using electromagnetic relays will ever be refurbishment due to problems of equipment aging or overall obsolescence. The only improvements which could be envisaged at relatively low cost in the future will involve

the upgrading of the supervision system and will therefore probably be the centralized solution.
The solution selected to improve alarm monitoring during outage is "mechanical filtering".

This modifications has the following additional objectives:

- standardize the very diverse practices at sites by applying the alarm policy during outage,
- retain the list of alarms relevant during outage within the scope of the impact analysis of each modification sheet carried out by the design department.

4. CONCLUSION

Alarm processing is a complex area which has been examined by numerous studies.

EDF has produced several official documents detailing alarm operation procedures. These are categorized according to the degree of urgency of the corrective actions required of the operator.

Alarm processing during outage of 900 MW PWR units is very weak. Before carrying out the second ten-yearly inspections, EDF has launched a preliminary feasibility study into the upgrading of its instrumentation and control system.

No particular aging was observed on the alarms; only alarm window saturation was noted.

The short preliminary study of improvements to alarm processing during outage took these results into account.
Among the solutions examined, ranging from the addition of nine computer screens to the preservation of the existing system, it has been decided to add a block of alarm windows to each main control console and to reduce the size of the alarm windows on the secondary control boards. This modification will integrate an important alarm recognition device during outage (filter screens).

This solution has been selected not only because of its lower cost compared with introducing computerized systems, but also primarily because it allows current operating procedures applied by operating teams to be maintained.

CONTROL ROOM
900 MW PWR
CP1 - CP2

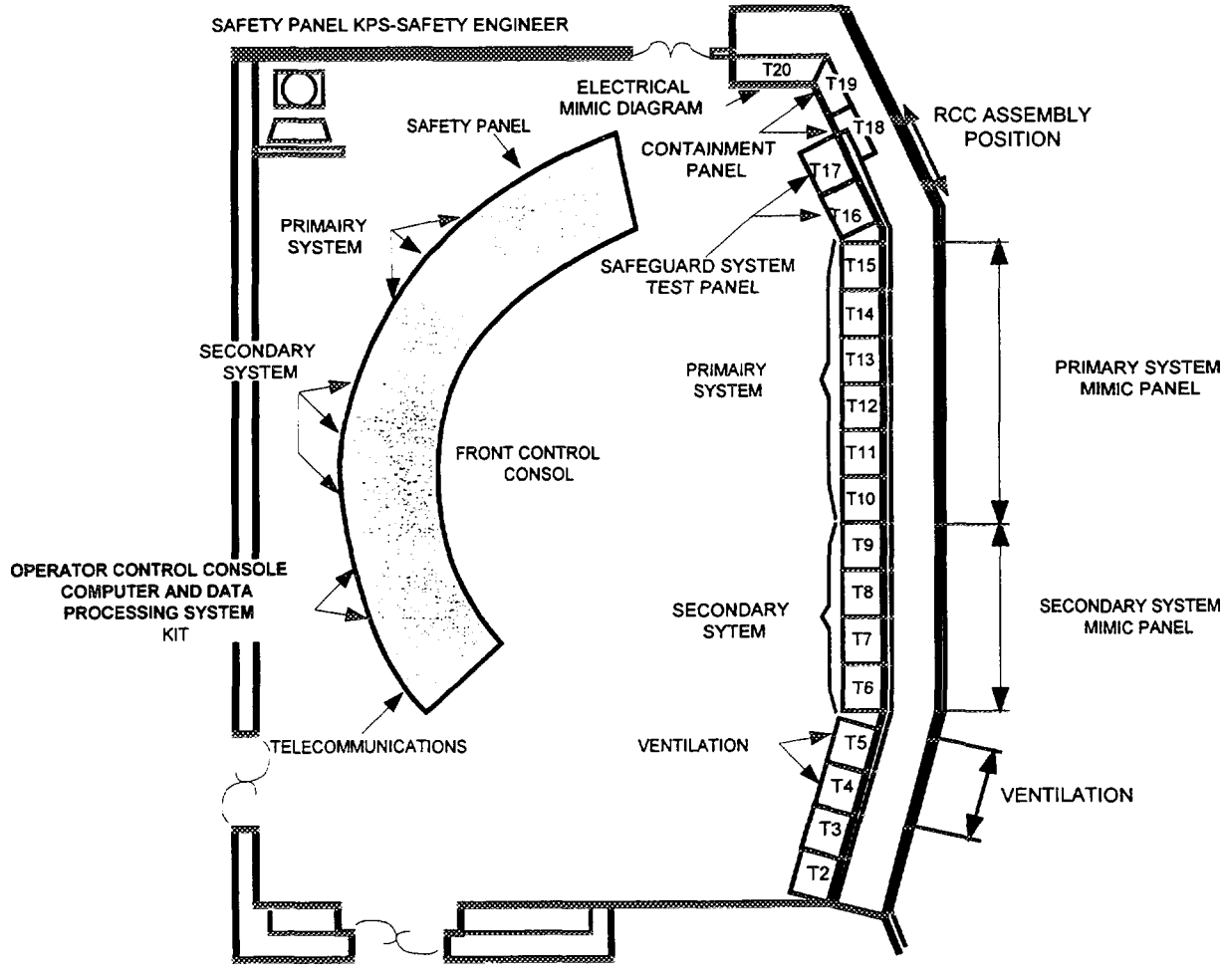


Figure 1: General layout of the CPY Control Room

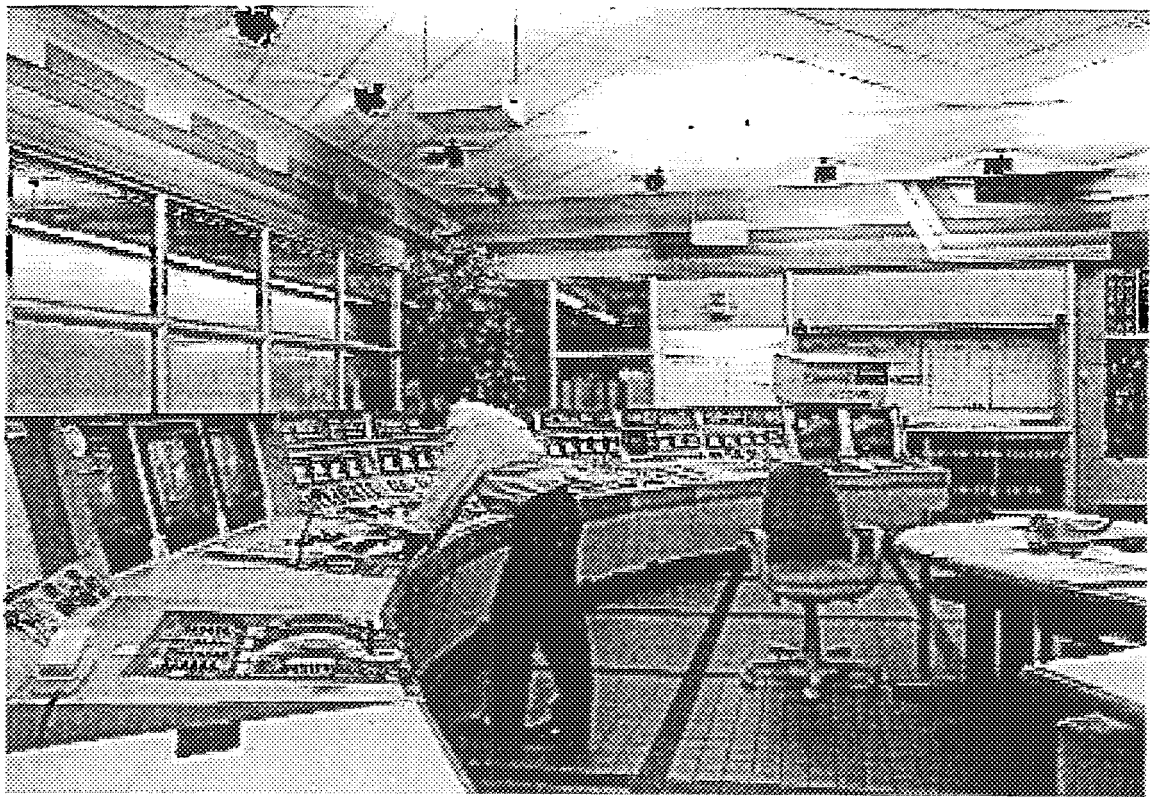


Figure 2: 900MW PWR CP2 Series Control Room

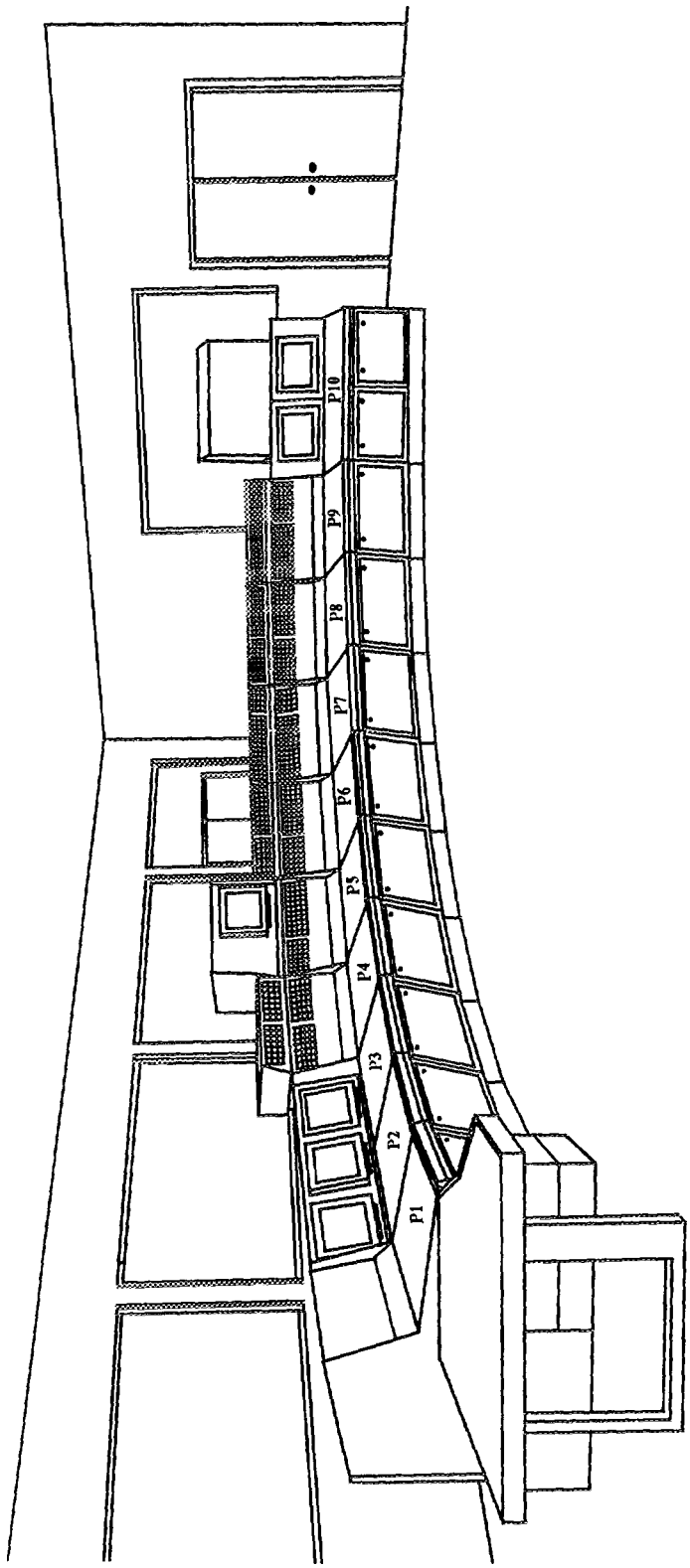


Figure 3: The Addition of Alarm Window Blocks to the Main Control Console

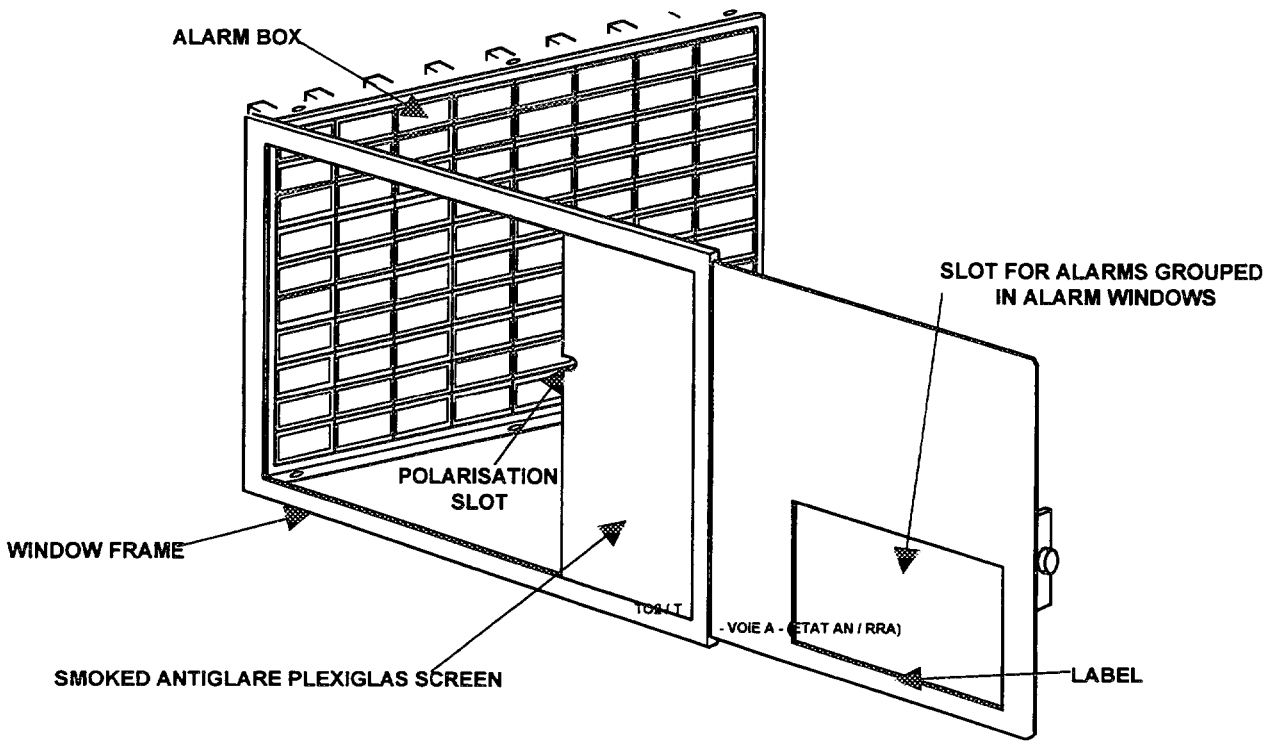


Figure 4: The Filter Board Principle

IMPROVEMENTS TO THE ANNUNCIATION AND DISPLAY SYSTEMS AT GENTILLY 2 NGS - AN INTEGRATED APPROACH

Raymond Dufresne and Michel Désaulniers
Centrale Nucléaire Gentilly 2, Hydro-Québec
Québec, Canada

ABSTRACT

Since 1990, Gentilly 2 Nuclear Generating Station has revised its overall strategy during upsets and abnormal events and has also completely revised its Emergency Operating Procedures (EOP), its abnormal General Operating Procedures (GOP) and is near completing the revision of its Operating Manuals (OM). This strategy, these new EOPs, abnormal GOPs and the abnormal OMs were validated on our full scale simulator when applicable by a multidisciplinary team composed of authorized staff, technical and safety specialists and also candidates in training for authorization. We have identified significant weaknesses in the annunciation and display systems impairing the management of these events. To benefit from CANDU Owner's Group (COG) expertise, we met in some occasions the CRNL's research team on CAMLS project (CANDU Annunciation Message List System). In order to have more immediate benefits, we chose to improve the actual annunciation and display systems using, in some cases, ideas and/or principles used in the prototype CAMLS. After a brief history, we will present the global approach used at Gentilly 2 for upsets and event management and, we will therefore describe in more detail each of the improvements on annunciation and display systems which contributed to reinforce this global approach. Hereafter are some of these improvements: prioritization via color coding of window alarms, re-prioritization (major/minor) of all CRT alarms, coalescence of multi-channel analog and contact CRT alarms, increase in the amount of trends and bar charts for upset management, special alarm summary functions (contextual) for startup after a trip. We did also identify certain needs which are not yet fulfilled with the actual improved system. Finally we will describe some other proposed improvements to the annunciation and display systems that we foresee in the near future.

1. INTRODUCTION

Gentilly 2 is a single unit, 675 MW CANDU nuclear generating station. It is the only reactor owned and operated by Hydro-Québec. Gentilly 2 has had major difficulties since startup to qualify a sufficient number of licensed personnel (figure 1.0-1). It resulted in a lack of operating experience return into the organization, and also a lack of continuous training. In 1990, the Regulator (Atomic Energy Control Board, AECB) accepted to replace temporarily for Gentilly 2, the written examination system by a simulator based special examination system. Gentilly 2 management set up a project team headed by acting Shift Supervisors to prepare for those examinations. It was number one priority, after production.

Gentilly 2 being a single unit station, the resources involved in development are limited. On the other hand, the smaller station staff gives the opportunity to have a more integrated approach to incident management. This situation has allowed to integrate the authorized staff training organization into the revision of the emergency operating strategy. Parallel development of training programs and emergency operating strategy and policies has improved the management of abnormal events at Gentilly 2, mainly because the process has brought together the operating experience of authorized staff, the technical knowledge of specialists and the positive critical approach of candidates in training for authorization.

During 1990, 1992 and 1994 training programs, regarding our new simulator examinations, the following: transient, incident strategy, procedures, and crew responsibilities had to be reviewed extensively [1]. This brought into perspective the need for improvements to the annunciation and to the human-machine interface since no significant work had been done in those areas since commissioning in 1982 [2].

2. CONTROL ROOM TRANSIENT STRATEGY AND PERFORMANCE EXPECTATIONS

Gentilly 2 control room crew response strategy has had a major impact on defining requirements for improvements to the human-machine interface. In some instances, weaknesses could be counteracted by non licensed operators. Gentilly 2 compensated the lack of authorized personnel by implementing a formalized training program for the second operators (non licensed operators in the control room). This helped to limit the scope of the modifications required to the human-machine interface. Modifications were asked when either the shift supervisor, the authorized control room first operator (first operator) or one of the three second non-licensed control room operators (second operator) could not carry out the expectations during credible transients. High fidelity of the full scale Gentilly 2 simulator was an important asset when carrying out the human performance evaluation and high priority was given to achieve and maintain this simulator high fidelity. Authorized personnel performance expectations during transients were station adapted from OCD-ST6 [3]. These expectations cover the following fields:

(a) Monitoring
(b) Initial actions taken at the onset of a transient
(c) Diagnosis and decision making
(d) Procedure conformity
(e) Communication and team work

2.1. Improvement of EOPs, OMs and Incident Management at Gentilly 2

A complete revision of the Emergency Operating Procedures and Incident Management had to be done to meet the generic authorized personnel expectations. Experience acquired since the beginning of the operation of the station has shown that the following issues needed to be addressed in the revision to guarantee a safe operation of the station in all situations:

- Clearly define the organization of the operating team that has to be set up to manage the incident and to guarantee efficient use of all the available resources.
- Clearly define station specific expectations and good practices for the operating staff during abnormal situations.
- Implement continuous monitoring of important safety related parameters.
- Develop a general approach that could be used for the stabilization of the station under any credible abnormal event situation.
- Develop a whole set of EOPs (specific and generic) which must cover all the events used to define the overall safety envelope of the station as defined in the Safety Report, Safety Design Matrices (Probabilistic Safety Assessment) and other analysis submitted to obtain the Operating License.
- Provide a non ambiguous diagnosis (clear entry conditions) for each event based EOP procedure.
- Prepare restoration procedures based on a state approach in order to provide a second alternative to the operational crew following a failure in the application of a specific EOP or in case the main control room becomes inoperative or uninhabitable.
- Provide a way to validate each procedure in a realistic operating environment.
- Ensure that the human-machine interface is adequate in performing the above tasks.

So, since 1990, much work has been done at Gentilly 2 to implement a rational solution to these different issues. An equivalent work is still in progress for the revision of the Operating Manual (OM) Abnormal Procedures, Alarm Sheet Procedures and is completed for the abnormal General Operating Procedures (GOP). The principle is that each alarm in the control room (and in the field) has an alarm sheet which gives the procedure to be followed if the alarm is unique and abnormal operating procedures (combination of alarms) must have clear entry conditions from the annunciation system and must be referred from the individual alarm sheets. Thus, annunciation is a very fundamental key issue in the success of the procedure revision (EOP and OM) and performance of the operating staff.

2.2. Operating Team Organization

The minimum operating staff needed in control room to manage an incident at Gentilly 2 is composed of:

- a Shift Supervisor (SS)
- an Authorized First Operator (AFO)
- an alarm monitoring Second Operator (OP-2)
- two panel monitoring Second Operators (OP-2)

In order to manage adequately an abnormal event, the operator tasks have been defined precisely and tested on simulator during team retraining and during initial training for authorized staff with many different types of events. A summary of the control room organization and the operators' tasks is presented in figure 2.2-1.

A characteristic of this operating team organization is the greater role that Second Operators (non authorized OP-2) now play in the management of incidents, particularly in the monitoring of important parameters and equipments using generic hand-outs. As a result, a formal qualification process for Second Operators (OP-2) has been implemented regarding this issue.

It is also essential to promote good communication between the operators to enhance their ability to perform as a team. Good human interface facilitates communications during transients keeping it to the minimum essential.

2.3. General Approach

The main objective of the general approach is to maximize the retention and the containment of radioactive material under any circumstances and to minimize the economical consequences when possible. The operating staff should perform the adequate actions to implement the main safety functions:

- shut down the reactor
- contain radioactive materials
- maintain appropriate heat sink
- monitor safety function parameters

The improvement of the specific EOP diagnosis has allowed to discriminate in favor of the most important parameters which must be monitored continuously. It resulted in the implementation of a monitoring procedure. In this procedure, three sets of parameters are defined:

- critical safety parameters (CSP)
- main safety parameters (MSP)
- other parameters for specific EOP diagnosis

The CSPs are a small set of parameters whose status, over a determined limit, indicate a threat or a deterioration of the integrity of the safety barriers. For all CSPs, a restoration guide has been prepared aiming at the re-establishment of the parameters within acceptable limits or the mitigation of the consequences.

For Gentilly 2, the CSPs are:

- reactor power
- subcooling margin at the four inlet headers
- pressure in the reactor building
- activity in the reactor building
- activity in the steam generator
- activity in the service water

The MSPs are a greater set of parameters and they give, if maintained inside determined limits, a sure indication that the reactor power is under control, that the fuel is adequately cooled and that the radioactivity is correctly contained. All the CSPs are included in the MSPs. The monitoring of MSPs aims to confirm the response of the plant and allows to re-actualize the diagnosis during the use of a specific EOP.

Some parameters other than CPSs and MSPs, which are key elements in the diagnosis of specific EOPs, must also be monitored continuously. For example, instrument air pressure is a major indicator of a loss of instrument air. The monitoring of this third category of parameter helps to anticipate deterioration of the general plant conditions. Four bar charts have been specially created to rapidly monitor these very important parameters (CPSs, MSPs and other parameters of specific EOP diagnosis).

Also, a more global approach has been implemented to face any abnormal situation. This approach is made up of following major stages.

- The recognition of an abnormal situation (automatic power drop greater than 10% FP).
- The verification of the efficiency and the completion of the actions of automated systems (safety and support safety systems) which are standard after a power transient.
- Actions in the Main Control Room (MCR) prior to evacuation if MCR becomes inoperative or uninhabitable.
- Verification and completion of the actions of Emergency Coolant Injection (ECI), if initiated automatically.
- Continuous monitoring of CSPs, MSPs and other parameters of specific EOP diagnosis.
- Restoration of the subcooling margin, if required.
- Diagnosis.
- Application of a specific alarm sheet procedure or specific abnormal OM procedure or specific GOP or specific EOP.
- Authorization for resetting a shutdown system after a trip and for increasing power

The general approach is presented in a diagram at figure 2.3-1.

The verification of the efficiency and the completion of the actions of the automated systems rely upon documented good practices and a set of generic EOPs (generic hand-outs and the generic procedure "Automatic initiation of ECI"). The figure 2.3-2 presents the station specific expectations and good practices following the initiation of Shutdown System # 1 (SDS1).

In the case of ECI automatic initiation, the verification and the completion of actions of this automated system may also cover the restoration of the subcooling margin, if the deterioration of this CSP is not due to a loss of heat sink.

The continuous monitoring of CSPs, MSPs and other parameters of specific EOP diagnosis rely on a surveillance procedure carried out by a second operator (this does not relieve the SS and AFO to periodically monitor their CSPs/MSPs). The continuous monitoring allows to

reactualize the initial diagnosis, to anticipate further deterioration, to detect additional failures and to initiate restoration procedures more rapidly. Also, this procedure gives the hierarchy and the field of all generic and specific EOPs in order to guide the operator toward the most urgent situation (or dominant event) following a multiple event situation.

Finally, in order to enhance the importance of CSPs and improve the continuous monitoring, a color coding of the window alarms in the MCR has been defined. Now, the red color is used only to indicate the initiation of a Setback, Stepback, SDS1, SDS2, ECI, Containment/Dousing, and to indicate activity in the Steam Generators or/and in the Service Water. Essentially, the red window alarms indicate that CSPs are challenged.

The restoration of the subcooling margin at inlet headers is covered by a generic procedure which gives the ultimate guarantee that the fuel is adequately cooled, whereas the restoration or at least the mitigation of activity in Service Water or in the Steam Generator are covered by specific EOPs. These specific EOPs rely both on the use of ECI manually to preserve (assure) adequate cooling of the fuel.

The purpose of this approach is not to reject the event based procedure approach but to fill a gap with a more generic perspective. The recognition of a specific event and the utilization of an event based procedure always constitute the optimal way to face an abnormal event. However, the good practices toward the initiation of Special Safety Systems (SSS), the continuous monitoring of important safety parameters and the restoration of subcooling margin procedures make up a safety net to event based procedures and frame a second alternative to stabilize the plant following any abnormal event. The general approach has the advantage of stabilizing CSPs before attempting to recognize the event. In fact, if the operator fails to identify the event, the whole set of specific EOPs, specific abnormal OM procedures or specific alarm sheet procedures is quite useless.

Some parameters other than CPSs and MSPs, which are key elements in the diagnosis of specific EOPs, must also be monitored continuously. For example, instrument air pressure is a major indicator of a loss of instrument air. The monitoring of this third category of parameter helps to anticipate deterioration of the general plant conditions.

As a corollary to the monitoring of the CSPs, MSPs and other parameters of specific EOP diagnosis, the concept of monitoring the Main Turbine Parameters (MTP) was developed. The MTPs are a greater set of turbine and Balance of Plant (BOP) parameters and they give, if maintained inside determined limits, a sure indication that conventional risk is correctly addressed. Examples of MTPs are turbine speed, vibrations, lubrication oil pressure, bearing temperatures, alternator hydrogen pressure and temperatures, etc.

The monitoring of MTPs, as for the CSPs/MSPs/EOPs entry conditions, aims to confirm the response of the plant and allows to reactualize the diagnosis during the use of alarm sheet procedure or abnormal OM procedure or specific EOP. Three bar charts have been specially created to rapidly monitor the important turbine and BOP parameters and the generic handout

refers to the applicable alarm sheet procedure or abnormal OM procedure when predetermined limits are exceeded.

The main advantage of this global monitoring approach is that it is redundant to the annunciation system and instead of waiting for alarms to come, the operator goes and checks if major parameter limits are exceeded. Should an alarm be mist, this monitoring constitutes an independent safety net.

Furthermore, we have improved our alarm annunciation system to reinforce this global approach. A review of the MCR window alarms has been done and the orange color has been introduced as an intermediate indicator between the red and the white to enhance the hierarchy of the window alarms. Hence an orange window alarm requires a quick response and it is particularly useful to identify any additional important failure that may occur during the stabilization of the plant following an upset.

Moreover all CRT alarms have been reassessed in the context of major/minor alarms. After an upset (Setback, Stepback, SDS1, SDS2, turbine unloading or turbine trip) only the major alarms appear on the CRT. All the alarms were in principle classified major except for those which correspond to the clean mark of a Setback, a Stepback, a turbine trip, a SDS1, a Containment/Dousing initiation and an ECI initiation. Those were made minor because they are a result of the operation of the system and are therefore not abnormalities. Alarms from non-Safety Related Systems (SRS) were also made minor since they will be reviewed from an alarm summary sheet once the plant is stabilized (see below for more details).

The alarm discrimination is efficient to keep displayed on the CRT the alarms related to the initial cause of the event and to monitor the occurrence of additional failures during the stabilization of the plant, at a pace, acceptable to the alarm panel monitoring operator.

The number of trends and bar charts has been doubled and many of them are dedicated to abnormal events. Hence key parameters are grouped to carry out EOPs and generic monitoring more efficiently. Color coding of window alarms, major prioritization of CRT alarms, the eight generic monitoring easy to use bar charts and use of handouts were major contributors to improve communications between the second operators and the authorized personnel in the control room keeping it to the minimum, though precise, short, simple and complete.

Once the station is stabilized, decision must be made about resetting the shutdown systems and authorizing increase or return to power. These decisions must be taken whether or not the reactor has poisoned out. These decisions must be made without deviating from the Operating License and the Operating Policies and Principles (OPP). Furthermore one does not want to startup without being aware of Safety Related Systems impairments that may force us to shutdown after a short operating period to carryout repairs that cannot be done at power because cycling the plant is counter-indicated for safety and economical reasons. A detailed generic Shift Supervisor procedure was developed to standardize SS decision making. It is in fact a generic EOP handout called from the abnormal General Operating Procedures (GOP) at the steps were these decisions have to be made. Thus what was before an OPP administrative authorization given by the SS to

the AFO is now supported by an SS procedure. When the cause of the shutdown is known and cleared and no significant SRS impairments were identified from the red/orange window alarms and major CRT alarms, there is economical incentive the return to power before xenon poison out. To help the SS to efficiently carryout his generic authorization procedure, two special alarm summary functions (contextual) were developed. The half hour period for red/orange versus white window color coding prioritization criteria and the major versus minor CRT alarm prioritization criteria were done in the context of a return to poison prevent power level. These mode of prioritization help to discriminate alarms that are important to address while returning to power after a transient. It should be noted that the scope of this SS handout covers not only trip from high power but also from low power (including approach to criticality).

2.4 Validation of EOPs, Abnormal Gops, Major Abnormal Om Procedures and Major Alarm Sheet Procedures

Validation is the demonstration that the procedure could be executed by operating staff if they are properly trained. It should be noted that you can train people to operate at a very high level, but the procedure should be executable by normally trained staff.

Validation is the process used to confirm that:

- there are clear entry points to the procedure, thus annunciation is adequate,
- the procedure presentation is adequate to prevent execution errors,
- the human-machine interface actions are correct,
- the procedure could be implemented with the minimum staff of operators,
- the procedure and annunciation are tolerant to additional failure, and
- that all the hand-outs could be executed by second operators (non-authorized).

A first verification/validation is done during the training program on the simulator by the authorized shift supervisor in charge of the training and by the candidates for authorization. Several trial runs with different leak rates, additional failures and different candidates are carried out to validate the robustness of EOPs, Abnormal GOPs, of the major abnormal OM procedures and of the major specific alarm sheet procedures.

A second validation is carried out on the simulator, in a teamwork approach, by at least one operating crew where each section of the procedure is tested by the personnel who will have to perform the job, and during a table-top review by authorized personnel not involved in the development of the procedures.

This validation process for the procedures plus the OCD-ST6 simulator examination process [3] has confirmed that the modifications to the annunciation and to the human-machine interface have greatly improved the control room crew performance during transient operation.

3. DETAILED ANNUNCIATION, HUMAN-MACHINE INTERFACE AND DCC'S IMPROVEMENTS AT GENTILLY 2

The following is the detailed description of Gentilly 2 NGS annunciation and human-machine interface improvements implemented to support the generic control room transient strategy and to meet the control room staff performance expectations. Additional DCCs software improvements at Gentilly2 are also reported.

3.1 Annunciation System

3.1.1 Window Alarm Color Coding

During normal operation all alarms are important and have to be addressed with due diligence. During an upset, color coding facilitates implementation of a hierarchy of priorities that is described here. The main purpose of the annunciation window is to be informed that something new is happening. This was our governing principle for window alarms prioritization. Highest priority for annunciation is given to the red window alarms. It is an implementation of the «control, cool and contain» concept.

One red window alarm per channel for SDS1 and for SDS2 and two red window alarms for reactor Stepback and Setback (one each) were implemented for «control». This concept permitted to remove almost all red windows from SDS1 and SDS2 panels. When a shutdown system trips, nothing is more important than to go to the panel to check its effectiveness; the cause of the trip can be a white window since it is a source of information for diagnosis, not an annunciation of a trip.

Seven red windows were implemented for ECI: two for ECI initiation (odd & even), three (one per channel) for Main Steam Safety Valves (MSSVs) initiation and two for low pressure manual initiation (low dousing water level and high enough water level in the reactor building sump). This is for the «cool» concept. When ECI is initiated, it is the highest hierarchy of our emergency operating procedure that applies (after MCR evacuation), so the entry conditions for it are simple and clear.

Four red windows cover the «contain» concept: one for containment boxup, one for dousing initiation, one for D_2O in H_2O detection in the steam generators and one for D_2O in H_2O detection in the recirculated cooling water system (heavy water leak outside containment).

Any red window alarm requires immediate attention and action by the operator, though in some cases, it may only require to initiate field action for confirmation and the leak rate might yet be below the scope of application of an EOP.

Orange versus white window alarm selection criteria were the following:

(a) All windows should be orange, following a transient unless addressing this window within a time frame of less than half an hour would be counterproductive. Thus a window that does not have to be addressed within half an hour will be white.

(b) Causes of SDS1 or SDS2 or ECI or containment are white because they are a source of information and we do not expect the operator to pickup the alarm sheet to do actions from such a window alarm. There is usually a more significant process alarm sheet to pickup to do actions from.

(c) A window alarm that is a multiple contact alarm, some of which do not have to be addressed within the first half an hour of a transient will be white given that the causes that have to be addressed within half an hour have specific CRT alarms that are selected major (see CRT major mode below) or the parameter is monitored from a generic hand-out.

For instance at Gentilly 2, 34 window alarms do come in, in the first five minutes following a clean SDS1 trip followed by a turbine trip (turbine motorization is not permitted at Gentilly 2). The number of window alarms to review is limited following such a trip to four red window alarms (Ch D/E/F & Stepback) and four orange window alarms (two for turbine trip, one for HPHR and one for LPHR train isolation). The window alarm review is thus much simpler and any other red or orange window alarm is an indication of the initial cause of the trip or is the result of a significant additional failure that needs to be addressed or explained in the circumstances.

3.1.2. Major/Minor Prioritization

In the original design of Gentilly 2 DCC annunciation system, there was an automatic function allowing minor alarm suppression on the annunciation CRT's during an incident. The purpose of that function was to reduce significantly the amount of alarms scrolling on the CRT's in order to help the operator to diagnose the event.

Initially, the alarm priority (major/minor) were given by system engineers, according to the importance of the alarm in regard to the system which they were responsible. Thus, during an upset, while displaying only the major alarms on CRTs, many "major" alarms were useless for the operator and many others, considered "minor", were missing on the CRT's. That situation was not helping operating staff to diagnose the cause of events or to cope with additional failures and could have lead them to make wrong decisions. So, the minor alarm suppression function had been disabled since commissioning. All the alarms were always displayed on annunciation CRTs allowing a tremendous amount of alarms scrolling on the CRTs during events. This situation lasted for 12 years.

A team of an experienced shift supervisor and a senior control room second operator with large simulator experience was setup to review major/minor alarm classification and to define priority selection criteria. Once the criteria to CRT alarms were adopted, a complete review of A/I, C/I and program alarms has been done to set them to their new priority. Also, many event scenarios

has been performed on simulator facility triggering several adjustment in alarm priority choice and leading to the final version. The final version has been presented to AECB and installed in the control room.

Major versus minor selection criteria were the following:

(a) Major mode should facilitate diagnosis of the initial cause of a transient and diagnosis of significant additional failures that may occur once the transient is evolving.

(b) Major mode should facilitate the work of the second operator at the annunciation panel. Since this operator is not a licensed operator, we expect him to read aloud the alarms that are occurring on CRTs to keep informed the first operator of new alarms while he is performing actions on the panel (this does not relieve the first operator from independently reviewing periodically his CRT alarms).

(c) All alarms are important and should in principle be major unless there is a good reason to set them minor. This simple principle was our main breakthrough since 45% of the alarms are major. This means that 1824 out of the 4167 CRT alarms are major. The main point is that they don't come all at the same time, but if there is something significant, the operator will be made aware of it.

(d) Alarms that are indicating correct operation of an expected automatism following a power reduction or turbine trip are set minor. In fact they are not indicating an abnormality but are normal in the circumstances. The confirmation of correct operation of these automatisms is done by the second operators performing the generic handouts. These alarms are the most noxious ones since they are flooding the CRT screen at the very beginning a trip and the cause related alarms of the trip can most of the time only be found on the paper printouts at the rear of the control room. For instance at Gentilly 2 in minor mode, 152 alarms do come in the first two minutes following a clean SDS1 trip followed by a turbine trip (turbine motorization is not permitted at Gentilly 2) and 61 alarms return to normal. In major mode five alarms are on the screen five minutes after a clean SDS1/turbine trip. Any other alarm on CRTs are related to the cause of the trip (the minor alarms showing the unfolding of a progressive failure are still on the screen since they were there in minor mode before the trip and can still be seen on the screen) or they are the result of additional failures that occurred because of the transient.

(e) Alarms known from station trip alarm printouts to frequently pass from alarm to normal to alarm were set minor since they distract the crew from stabilizing the plant and they increase the work load and stress of the annunciation panel second operator. If the parameter is important, it is monitored from handouts with a larger acceptable bracket.

(f) Coalescence of alarms was extensively implemented to reduce the number of alarms on the CRT screens (see below).

(g) Hand-switch (HS) position were made minor to limit the number of CRT alarms during upsets. Turning a HS whether it gives an alarm or not is not an error. Self-checking was continually reinforce in the simulator training for authorized personnel to limit wrong HS manipulation. Alarm summary at the end of the transient and before startup are used to check wrong HS positioning that did not affect stabilization of the plant.

(h) Drift and irrationality alarms were made minor except if they constitute entry conditions to important alarm sheet procedures, abnormal OM procedures or EOPs since these alarms require investigation by maintenance personnel that can be postponed for half an hour and it may be normal that some come in during transients.

(i) High delta-P for strainers and ion exchange columns were made minor because it is normal that they come in under transient high process flow.

(j) Causes of SDS1 or SDS2 were made minor since they appear on the respective SDS panels and are taken in note by the second operator monitoring the CSPs/MSPs (see below Alarm Reset Push-button Conditioning with Incident Detection).

(k) Strategically selected limited number of reactor building (R/B) gamma monitors alarms were set major to prevent flooding the CRTs under LOCA conditions. Service building gamma monitors are all set major.

(l) When there are several alarms at the same set point, one of the most representative coalesced one is set major, and all the others are minor. For example, when R/B pressure reaches 3,5 kPa(d), only the coalesced (3 A/I) message is major and all SDS1, SDS2, ECI and Containment C/I alarms are set minor since these alarms appear as white windows on the panel alarms.

(m) Equipment and parameters that are monitored by the operator executing the « General handout following containment, ECI and/or dousing initiation » are set minor to prevent flooding the CRTs under LOCA conditions. The alarms relative to airlocks and spent fuel penetration are major because of their importance in respect to containment integrity.

Each new alarm priority modification has to be defined by operating staff according to the chosen criteria before implementation in the DCCs. As reviewed, the annunciation system responds now to the original goals and allows the safety operation of the station.

To improve efficiency, A/I and C/I messages were rewritten to have their number on the screen. When an alarm comes on the screen, the first operator can right away ask for the alarm sheet to a second operator as he starts investigating on the panels. In less than one minute he has a procedure in hand to help him take the right course of actions. Window alarms have been numbered for the same purpose. Program alarms are under the process of being modified to have the message numbers on the screen; this modification needs a re-edition of the programs, this is why it is not yet completed.

3.1.3. Contact And Analog Alarm Message Coalescence

In major conditions, only proper alarm messages have to be displayed on the alarm CRTs. When ever there is multiple channel messages on CRTs, this can overwrite some other important alarms.

The contact and analog alarm message coalescence (figure 3.1-1) eliminates this problem by decreasing the number of alarm messages displayed on the CRTs by coalescing different channels in only one message, all the time. The resulting message (coalesced message) announces the channels combination in alarm and displays one alarm number. When a status change occurs, this coalesced message is updated. If the message is already displayed on the CRT, the existing message is updated at the same place on the CRT, without new skeleton message emission. In that way, the operator can survey easily the status of a given coalesced message because it stays at the same place on the CRT.

For alarm messages of opened MSSVs (number of 16), all of these alarm messages are represented by only one coalesced message which displays on the CRTs the number of opened valves. Also, for SDS1 and SDS2 alarm messages, the color of the message changes from red to white when more than one channel is in alarm. The white color was chosen because of its high contrast with the black CRT background to identify an unexpected power reduction (SDS1, SDS2, stepback and setback events).

The implementation of contact and analog alarm message coalescence is easy because it demands small modifications of the analog alarm scan program (AAS) and contact alarm scan program (CAS). Because contact and analog alarm message coalescence is based on the resulting files of AAS and CAS, there is no duplicated logic or coding. Also, many integrated facilities allow fast and easy maintenance by technical team.

Advantages of contact and analog alarm message coalescence are:

- decrease in the number of alarm messages displayed;
- decrease of the searching time for information on the CRTs;
- emphasis of operators attention on most important alarm messages;
- better survey of alarm messages by operators;
- easy implementation;
- integrated diagnosis tools for updates.

3.1.4 Alarm Reset Push-button Conditioning with Incident Detection

When an incident occurs, there is a certain amount of alarms displayed on the annunciation panels and CRTs, some of them return to normal, others continue to come in. The second operator at the annunciation panel has a natural tendency to clear the alarms to be able to follow the occurrence of new alarms and report them to the authorized personnel. However there are instances where the alarm which indicates the cause of the trip may return to normal immediately

after action of automatisms thus, clearing them, jeopardizes diagnosis by the authorized staff. An example is a log rate trip.

To eliminate this problem, a modification has been done and implemented to override the erase button action if an incident has been detected. A new lighted push button has been added.

Now, a pre-defined event logic detection triggers a numerical output of the DCC to latch external relay logic. This logic overrides the erase push button and lights the new added push button light to tell the alarm monitoring second operator that the alarm reset button is disabled. He will simply have to push the new added button to enable the alarm reset button after authorization by the first operator. The AFO will give his authorization after he and the SS have reviewed the alarms to make the proper diagnosis of the event and after the second operator monitoring CSPs/MSPs has taken all the SDS window alarms in note in his handout which will be of utmost importance in the decision of resetting the SDS(s) that tripped and for authorizing return to power (see below SS handout). If a new incident is detected, the alarm reset button will be disabled again. For example, if a setback is detected, the alarm reset button will be disabled. The second operator will enable it after authorization and after a while, if another event is detected, it will disable the alarm reset button again and so on.

Briefly, the conditions disabling the alarm reset push button are:

- setback;
- stepback;
- SDS1;
- SDS2;
- atmospheric and condenser steam discharge valves open in interruption control mode;
- loss of class IV electrical power;
- turbo-alternator speed error > 1%;
- turbine trip;
- loss of grid.

3.1.5 Special Alarm Summaries (Contextual)

The latest implemented EOP handout is the SS «Authorization procedure for SDS resetting and for power increase». One important and time consuming step was to complete a full alarm summary review from a DCC printout and to ask a second operator to look for expected alarms that were missing from a check list. This is important to prevent Operation Policies and Principles (OPP) violation. Resetting a SDS and increasing power can violate several OPP articles since a large number of systems have changed state following a transient and SRS's availability has to be confirmed, taking into account systems that changed state. It should be noted that *missing* alarms review is as important as *present* alarm review since it might indicate unavailability of a protective feature which needs correction before resetting a SDS or before increasing power. For example a missing SDS1 or SDS2 inhibition parameter alarm , requires opening (or leave tripped) the faulty channel. At Gentilly 2 after a clean SDS1/turbine trip

(motorization is not permitted), 15 minutes after the trip, a summary alarm review consists of 120 alarms to analyze and of 69 alarms to check for their presence. For safety and economical reasons there is high incentive to automate this process. Two special alarm summary review have been developed and implemented, one after a SDS trip and one after a power reduction. There is also facility to add other contextual alarm summaries as required by Operations. Now after a clean SDS1 trip, a summary alarm review consists of 25 alarms to review and any missing alarm will be printed on the summary sheet; so no alarm is listed on that missing summary sheet when there is no missing alarm that may affect startup. The power reduction summary alarm was made in the context of a power reduction to low power (neutronic <1%FP). Thus after a clean stepback/turbine trip, a summary alarm review consists of 17 alarms to review and any missing alarm will be printed on the summary sheet, so there is no alarm listed there when no additional failure occurred that may affect startup. If the power reduction is at an intermediate power level, there will be some alarms that will appear in the missing alarm listing (such as SDS inhibition parameter alarms that did not come because power is not low enough), but there is more time to analyze and conclude that the situation is normal before xenon poison-out.

Figure 3.1-2 shows how the Special Alarm Summary program (SAS) is integrated to the actual DCC annunciation system. Figure 3.1-3 is a copy of the menu interface following a demand. The function display the number of abnormalities that were detected while the complete list of these messages are printed.

SAS provides also a useful maintenance facility to know which alarm messages is eliminated or announced-if-missing for each section of the special alarm summary. SAS may print all eliminated alarm messages and all announced-if-missing alarm messages associated to a given summary by a simple command.

Advantages of SAS facility are:

- Provide fast event analysis;
- Provide possibility to know which important alarm message is missing (impossible to access to that information directly by existing facilities);
- Eliminate some human distractions on long and hard summary analysis;
- Provide statistics directly on the CRT on the content of the special alarm summary;
- Avoid long shutdown and economic losses due to reactor poisoning, because the analysis time was too long.

3.1.6 Historical Alarm Page Display & Print out Facility

During the commissioning of Gentilly 2, alarm pages were only printed on paper without any alarm page backup. Thus, if the paper was tear up or lost, there was no way to recover the information contained on that paper. In some cases, that information could be very important to diagnose events.

The project of historical alarm page display and printout facility came to fill up this gap. An interface has been designed to allow alarm information access on demand. Now, it is possible to display and/or to print any page of these 25 pages contained in the BMU wrap around buffer of historical alarm pages.

Advantages of historical alarm page display and printout facility are:

- No loss of information;
- Possibility to consult desired information;
- Guaranteed access to information by few facilities (CRT display and/or printed copy);
- Fast access to desired information;
- Improved event analysis tools.

3.2 Human-Machine Interface System

3.2.1 Calling Function Menu Interface

The calling function menu interface is built to eliminate memorization of too many calling function sequences by operators; to group functions by general to more specific subjects; and to give an easier system survey.

The menu interface is called by the operator by a push button on a display keyboard. The first page of the menu is then displayed. The operator can, as desired, go up and down in menu levels, whatever the first menu displayed. In the same way, the operator has the possibility to display next page menu or previous page of the menu if they exist. Thus, the display of adjacent page is done by pressing only one push button. The display of a given page may be command by entering the number of an option included in the desired menu page. The operator may also enter two parameters in the same sequence for quick access to a function. To select an option, the operator has only to enter one of the displayed option numbers to initiate the execution of that function.

The menu structure definition (ex.: figure 3.2-1), and menu option specifications, are all contained in a menu table. This table, which is apart of the program, can be easily modified to define desired menu structure.

The menu linkage give the possibility to add a menu page at a given menu or to add a new menu without modification to the calling function menu interface program. Also, the addition of new menus is made easy. A menu option can represent a lower level menu or a function. Each menu may be acceded by a push button, where ever the menu is in the menu structure.

Also, system maintenance is simplify by the addition of indicators on the CRT like displayed menu number and option menu numbers. The title of trends and bar charts is updated automatically when an operator do some changes to trend and bar chart titles.

In the plan of executive program (EXEC review), the use of the menu interface logic freed large space of core memory (0600 words freed). Thus, the associating table between push buttons and functions, located in core memory, has been located in auxiliary memory (BMU). EXEC program calls now menu interface to initiate a function, except for instant response function push buttons and the calling function push button. This last function, part of the KBNTD program, uses the same associating tables than menu interface. Thus, it gives two ways to initiate the execution of a function, allowing an easy maintenance for these programs.

Advantages of the calling function menu interface are:

- Immediate access to any menu in the structure by a display keyboard push button;
- Elimination of heavy sequence memorization by operators;
- Easy way to go up and down in menu structure;
- Automatic update of trend and bar chart titles;
- Decrease used core memory (0600 words freed);
- Easy linkage of menus;
- Menu structure can be totally shaped as desired;
- Fast menu modification.

3.2.2 Increase of the Amount of Trends and Bar Charts

Operating staff asked for an increase of the amount of trends (64) and bar charts (64) to help them monitor the plant in different situations because there was not enough trends and bar charts available. The software allowing to modify specification, or to display trends and bar charts has been modify to double the amount of trends and bar charts. New specification tables has been added on the MBU for that purpose. This expansion allowed to define new trends and bar charts called from EOPs and GOPs.

Advantages of the increase of the amount of trends and bar charts are:

- better system monitoring;
- easier and faster execution of EOPs and GOPs;
- appropriate scale and data sampling for incident management
- variety of information amalgamations and displays.

3.3 **Data Acquisition System**

3.3.1 Fast Data Collection

This system allows recording of 16 variables for a sample period which may vary from 100 milliseconds to one second. The date is saved in a wrap around buffer of 39 minutes capacity for a one second sample period. This data may be displayed on trends, printed and/or transmitted by a serial data link of our computer network. The recording of data stops automatically when an incident is detected by the data collection on incident system. It allows backup of certain amount

of data when an incident occurred with a resolution of 100 milliseconds. The time period where this data is saved begins 1,5 minutes before the incident and stops 2,5 minutes after the incident.

During the transmission data process, graphics are made and send automatically to the laser printer located in the computer room.

3.3.2 Automatic Data Collection On Incident

This system allows recording of 64 variables per computer for a sample period of one second and more. The data is saved in a wrap around buffer located in bulk memory unit (BMU). This buffer has a 12 minutes capacity for a one second sample period.

This system may be used for data recording during testing time or, it may be used in incident detection mode. In the last case, incident detection starts an automatic stop process which allows to modify the sample period during incident. This give us the possibility to collect data for a 2 seconds sample period from 5 minutes before the incident up to 5 minutes after the incident. Then, the sample period is changed to larger time step, allowing the data collection to extend over one hour following the incident detection.

The data collected may be transmitted by a serial link to a data server of our computer network. During the transmission data process, graphics are made and sent automatically to the laser printer located in the computer room. This allow a faster event analysis.

3.3.3 Continuous Data Collection With A Serial Link

This system permits recording and transmitting on the serial link with a maximum of 320 variables per computer at a sample period of 10 seconds or more. These 320 variables are split into five data collection processes of 64 variables each. Each data collection process may have a different sample period. A human interface permits to specify the title, variables and the sample period of each data collection process. Each of these data collection can be turned on/off all together or separately.

This system permits also asynchronous transmission of alarm pages from the 25 pages buffer located in the bulk memory unit (BMU).

The 640 variables and alarm pages who came from the Digital Control Computers (DCC's) are transmitted to the data server of our computer network.

3.3.4 Operation Data Transmission System (STDE)

We have recently completed the implementation of a new data transmission system which permits to us to transmit all parameters from DCCs (A/I's, C/I's, D/I's, D/O's, DTAB's and some core memory addresses) at a 5 seconds sample period, to the data server of our computer network. STDE is used by our technical staff for systems and equipment's surveillance.

This system permits also the daily backup of the bulk memory unit (BMU) and the main memory. These backups are used in our DCC software configuration control process. Also, the local backup in the communication link computer will allow us to make a fast analysis of the bulk memory unit (BMU) when a computer breakdown may affect its data. Thus, we will decrease the unavailability time of the DCC's.

The figure 3.4-1 shows the overall configuration of this system. The data server LCSD1 located on a local isolated LAN has been design to allow the development of new PC based applications in the control room. (see chapter 4.3.)

3.3.5 Off-line Annunciation Feature

Gentilly 2's HDS system called STDE includes a special feature very much prized by our technical staff: an annunciation module computing the statistics of occurrence of alarms and messages printed out on the control room printers. This annunciation statistics module provides, for every single alarm point or message encountered (several thousands for a 600 MW reactor), its rate of occurrence for the current day, the day before, the last 30 days, the last 365 days and a yearly average since June 1993 (the start date of the data base). A roll down menu automatically updated every time a new page is received, displays the information for a subset of the alarm points. The System Responsible Engineer (SRE) can scroll rapidly through his or her system related alarms and instantly learn about the health of the system. Also these occurrences are processed as any other variables, so one can plot the trend of occurrences of any specific alarm point in time and see if it degrading or not. The module has been built on top of a product called PARSER developed by COG within the project CAMLS (Candu Annunciation Message List). PARSER being the module which parses the message pages into a data base of messages.

3.4 DCC's Executive System Enhancement

3.4.1 Overlay Expansion

The capacity of the overlay has been increased by 01000 words by moving the starting address from 030000 to 027000, providing a potential of 011000 contiguous words for the execution of slow programs. The new starting address is optional and is specified by setting bit 15 of the program length word in the executive disc information table. Thus, this modification, while allowing the addition of new functionalities to already tied up control and other programs, didn't impose any change to any program to fit the new starting overlay address. Any old program can continue being loaded at 030000 as before.

3.4.2 Core Memory Savings By The Use Of Menu Program

Keyboard button assignment tables, where moved from core memory to bulk memory unit (BMU), freeing about 0600 words of core memory. A menu manager demand program named MAF is called by the executive to serve the push buttons, except for the instant response functions which are still handled by the keyboard driver itself. MAF then call whichever demand

program is needed to respond to the function button pushed. There is no apparent delay for the operator, compared to the previous way of driving the keyboards.

3.4.3 Core Memory Savings By Splitting The Printer Page Buffer

A modification to the printer driver allows the printer page buffer to shrink from 05000 to less than 01000, freeing about 04000 words in core memory. Page outflow is apparently not changed and transfers to the other DCC is smooth and flawless.

3.4.4 New Keyboard On First Operator Desk

In answer to Operation's need, an additional function keyboard has been implemented on the Control Room Operator's (CRO) desk. The same keyboard is used to select and to control the display on two new RAMTEK channels (channels 6 and 7). This keyboard allows access to DCCX only, because no interrupt was available on DCCY, these interrupts being dedicated to the fuel handling machine CRT's (channels 16 and 17).

3.4.5 Coefficient Table Expansion

The conversion coefficient's table has been expanded in answer to the lack of space for new equations and to allow the expansion of A/I's and DTAB's. A/I's from 0300 to 0477 have been added as well as addresses 0500 to 0677 for DTAB's. Before the modification, there was a possibility for up to 0400 different equations for mixed A/I's and DTAB's. Now, the new table manages separately A/I's and DTAB's, and allows up to 0400 equations and 0100 equations respectively.

3.4.6 Gateway Driver

One of the motivations to free core memory was to implement a driver for the on-line Parallel Data Link Controller (PDLC) to send a full set of data (analog and digital), every 5 seconds, from de DCC's to a LAN server. This topic is covered in section 3.3.4.

3.4.7 Extended BMU Addressing

The Bulk Memory Unit (BMU) driver has been modified to allow addressing up to its full memory capacity (32Mb). An additional word is passed to the driver to specify a track offset to which the usual address offset is added to calculate the real starting address. Like overlay expansion, programs which are not yet using this feature can still address the BMU normally without any patches. A bit has to be set in the first word of the data block to indicate to the driver the use of the extended addressing.

3.4.8 More Patching Space For Fast Programs

Freeing space in the core memory has allowed to assign more patching space for RRF, Stepback and fuel handling drivers and control loops; programs which suffered lack of space to implement long awaited modifications.

3.4.9 Multiple Crunch Buffer

CRUNCH is a buffer which is filled with the contents of the core memory whenever a computer restart occurs. Most of the time a second restart, due to a watchdog time out, would overwrite the buffer, deleting any trace which might have led to diagnose the root cause of the first restart. A modification allows writing up to four separate CRUNCH buffers before overwriting the first one.

3.4.10 Solution To A Dual DCC Failure Design Problem

In November 1995 we had an outage due to a dual DCC's stall which has been caused by a design faults in the RAMTEK displays system. In May 1996 we have implemented a modification in the executive system to solve this problem in combination with a minor hardware modification. A technical report has been produced to fully document the design problem analysis and the proposed solution.

4. FUTURE DEVELOPMENT

4.1 Annunciation System

4.1.1 Conditioning of Electrical Alarms

The loss of power supply on distributing busses generates large amount of alarm messages which still floods the annunciation panels and CRTs. The object of this project is to analyze consequences of a loss of power supply for different distributing busses. Thus, it will define which of the alarms will be conditioned by the loss of power supply for each distributing bus. After that, AAS and CAS programs should be reviewed to allow more conditioned alarms.

4.1.2 Improvement Of The Historical Alarm Page Facility

This function which permits to display and print up to 25 historical alarm pages could be improved to add some other facilities. One of these could be the display and printout of certain predefined categories of alarms according to their sequence of occurrence. This new option could be useful to improve the decision process for authorizing return to power.

4.2 Human Machine Interface

4.2.1 Addition of a chain Option In Menu Program

The actual menu interface version allows access to all functions. But, to have access to another function, the menu interface has to be called again. During the execution of event procedures or incident procedures, it would be desirable to allow access to a function sequence (trends, bar charts and status displays) by a single touch of a push button function like "forward" or "backward".

By the modification of the menu interface program MAG (MENU function) and function programs themselves (trends, bar charts and status displays), it will be possible to initiate display of a menu in "chained" mode, allowing efficient monitoring of a set of parameters.

4.2.2 Trend display of Historical Data Saved on Incident Detection

The actual trend system allows to the Operating staff to display process parameters in one graphical trend on different time scales (2 sec, 6 sec, 10 sec and more). The 2 seconds time scale is especially used for the monitoring of the critical parameters. But, this time scale saves a maximum of 6 minutes of historical data. Thus, 6 minutes after the beginning of an incident, the operating staff begins to loose information which preceded the incident.

The considered modification consists to preserve a second copy of short-term historical data (2 sec, 6 sec, 10 sec) by HDS program. When an incident is detected, the update of the second copy will automatically stop few minutes later. The operating staff will be able to see incident historic by the same trend system. After the display of a trend, the operator will just compose a simple sequence of push buttons to see the incident historic on the same trend display.

The needed modification to see incident historic will not be major, because it will take advantage of the extended BMU addressing which has been developed at Gentilly 2 Station. Only a track offset will be modified to access incident historic by the same trend system.

4.2.3 New Status Displays

The status displays offer a good overall view of systems which are represented. These figures are particularly useful to make a diagnosis and to confirm actions taken by the operating staff. For example, we intend to develop one or few status displays to allow a better monitoring of the secondary circuit. Also, some status displays, like Reactor Regulating System (RRS) status display, will be modified to make them more ergonomic.

4.3 PC Based Operator Help System

Even if some more improvement can still be done in the Digital Control Computers, we foresee the need for new applications that will require a higher computer capacity and the access to SDS1/SDS2 input signals. Figure 4.3-1 shows a system configuration which is taking advantage

of the availability of the data in a server (LCSD1) located in the control room LAN. A processing server (LCSA1) would run the new applications and get the data from LCSD1 using a Client/Server approach.

Two of these applications (FLR and STCPC) are used on a PC in the control room, but are getting their data by the public network from a computer located in the technical support building. The new system configuration will secure these applications by locating them in a dedicated and configuration controlled computer. Furthermore, there input data will come directly from the data server LCSD1 located in the control room's protected LAN. The following is a short description of these actual and foreseen applications.

4.3.1 High Precision Flux Mapping (FLR)

This application bas been made available to the operators in order to give them a fast and accurate estimate of the maximum bundle power and the maximum channel power. This function is particularly helpful during a fast reactor startup in order to permit the increase of the reactor power rapidly and safely to full power.

FLR uses the bundle power to flux ratios calculated by the off-line code HQSIMEX which are transferred to the PC of the operator by the physicist of the station every 2 to 3 days. These ratios, used to estimate the local power ripples, are combined to the mapped fluxes with the modal amplitudes that are computed from the 102 Vanadium detectors by the on-line flux mapping program (FLX). These modal amplitudes are obtained by a data transmission command in the DCC.

4.3.2 Tool For Fuel Channel Blockage Verification (STCPC)

Flow blockage verification is performed at various reactor power levels during startup after an outage. This verification is done using 380 channels outlet temperature. A thorough verification is done using the STCPC application available to the control room operator (CRO); suspicious channels are readily identified by this software. Channels outlet temperatures used as input to the program are obtained by a data transmission command in the DCC.

4.3.3 Aid for Diagnosis

This function would confirm or suggest to the operator which EOP or abnormal OM procedures should be executed based on input conditions (presence of alarms and trends of parameters). All these conditions are well defined in the new version of the operating procedures. All the data required would be available in LCSD1.

4.3.4 System to Support Upset Recovery Actions

Considering the importance of the decision of resetting the SDS(s) that tripped and for authorizing return to power, we consider the design of more powerful functions in a PC based Operator Help System. These functions would have the following goals:

- Establish the sequence of alarms of the tripping parameters of the Shutdown and Regulating Systems;
- Do more parameter checks, using the DCC's and SSS's analog signals available in the data server LCSD1;
- Automatic verification of parameters that are presently verified by the first operator on the control room panels.

These functions would contribute to improve the decision process for authorizing the return to power giving benefits to safety and economic aspects.

5. CONCLUSION

Since 1990 Gentilly 2 underwent a major revision of the following: Emergency Operating Procedures (EOP, completed), abnormal General Operating Procedures (GOP, completed) and also its Operating Manuals (OM, 77% completed). The EOPs, abnormal GOPs and major abnormal OM procedures (including major alarm sheets) were simulator validated to ensure their usability by the control room team. Emergency crew response, role and responsibilities, expectations and good practices had to be formalized after ten years of operation. This led to a major upgrading of the human-machine interface to support applicability of these procedures (diagnosis and execution) and good practices (simplicity and effectiveness). In order to have more immediate benefits, we chose to improve the actual annunciation and display systems using, in some cases, ideas and/or principles used in the prototype CAMLS. The integration of these activities finally resulted in a high success rate of the candidates at the AECB simulator examinations for the 1990-1994 period (100%). Modifications to the human-machine interface implemented during that period was a major contributor to this high success rate. These modifications were well received among already authorized personnel because they were naturally improving their performance on the simulator during retraining, they were consistent with practices and culture developed since startup and such implementation was done to limit major modifications to their environment. These human-machine interface modifications were done through the existing annunciation and station computers which ensured that they were to the same quality assurance standards as Safety Related Systems.

Notes about the authors:

Mr. Raymond Dufresne has been the authorized shift supervisor in charge of the simulator training and the AECB simulator based examination for shift supervisor and control room operator candidates from 1991 to 1994. Since 1991, he is the Operation's coordinator for the development of Gentilly 2 operating response strategy to abnormal events, for the improvement of the human-machine interface and for the EOPs and abnormal GOPs revision. He has been a safety engineer for seven years before moving to Operations. He is now Operation's Support Superintendent (acting) and still an authorized shift supervisor.

Mr. Michel Désaulniers is Section Head of the Control Computer Group since 1993. He was Section Head of the Simulator Group from 1991 to 1993. He was working as Integration Specialist on the design and commissioning of the full scale simulator from 1986 to 1991. And, from 1978 to 1986, Mr. Désaulniers worked as software and control engineer for the commissioning and technical support of annunciation, human-machine interface and control programs in the Control Computer Group at Gentilly 2.

REFERENCES:

[1] Boulay, D., Dufresne, R., Pageau, R., «Abnormal Event Management - Gentilly 2 Approach», CNA/CNS Annual Conference, Montreal (1994).
[2] Désaulniers, M. et al., « DCC Software Improvement at Gentilly 2 », COG Computer Conference, Toronto (1995).
[3] Atomic Energy Control Board, « Simulator-based Examinations », OCD-ST6, (1993).

ABBREVIATIONS:

A/I	Analog input
AAS	Analog Alarm Scan program
AECB	Atomic Energy control Board (Regulator)
AFO	Authorized First Operator
BOP	Balance of plant
C/I	Contact input
CAMLS	CANDU Annunciation Message List System
CANDU	Canada Deuterium Uranium
CAS	Contact Alarm Scan program
Ch	Channel
CRNL	Chalk River National Laboratory
CRT	Cathode ray tube annunciation monitor (driven by DCCs)
CSP	Critical Safety Parameter
DCC	Digital Control Computer
ECI	Emergency Coolant Injection
EOP	Emergency Operating Procedure
GOP	General Operating Procedure (PGE)
HPHR	High Pressure Heater Heat Exchanger
HS	Hand-switch
LOCA	Loss of coolant accident
LPHR	Low Pressure Heater Heat Exchanger
MSP	Main Safety Parameter
MTP	Main Turbine Parameter (includes main BOP parameters)
OM	Operating Manual
OP-2	Second Operator (non licensed operators in the control room).
SDS1	Shutdown System number 1
SDS2	Shutdown System number 2
SRS	Safety Related System

SS Shift Supervisor

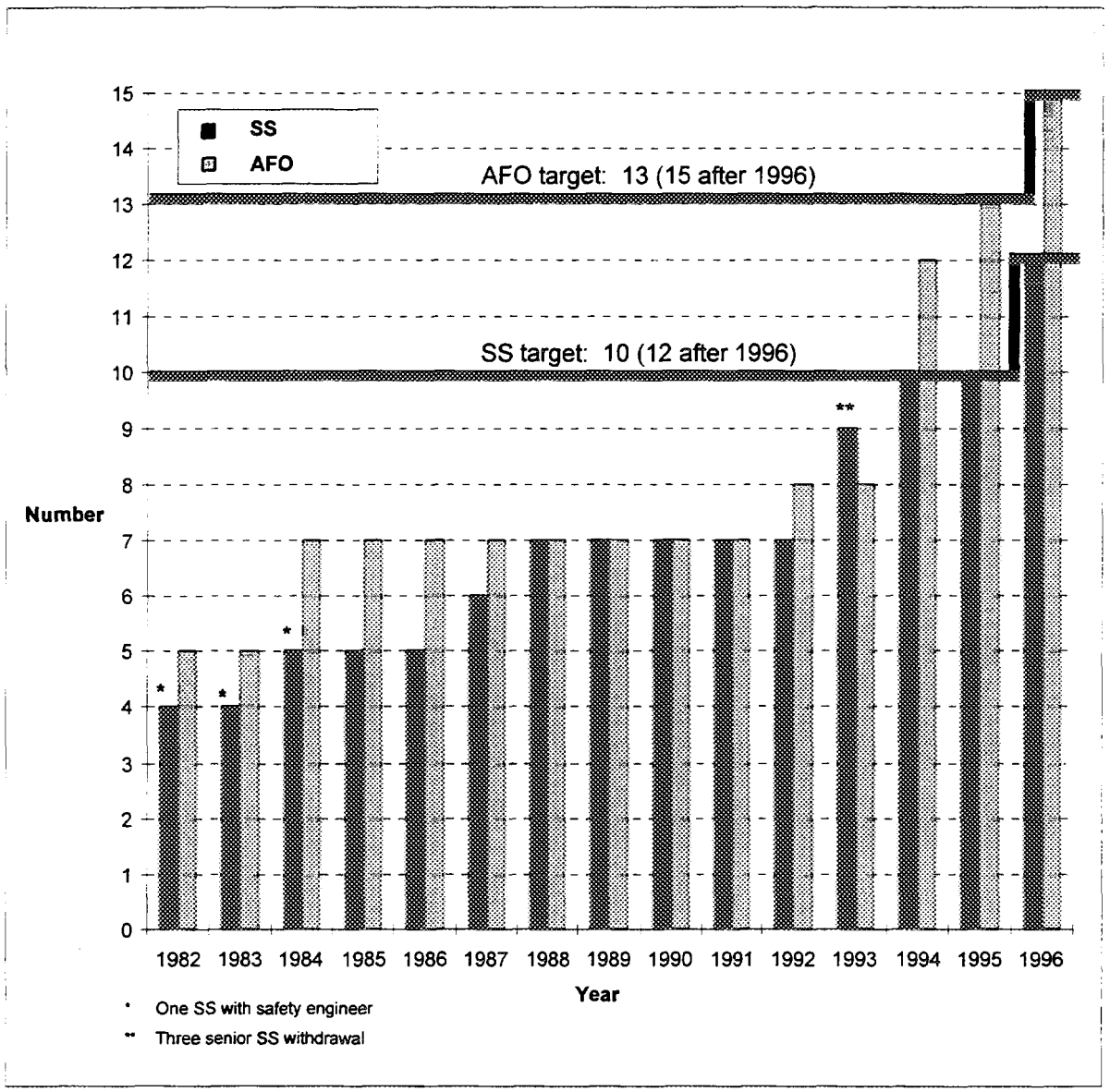
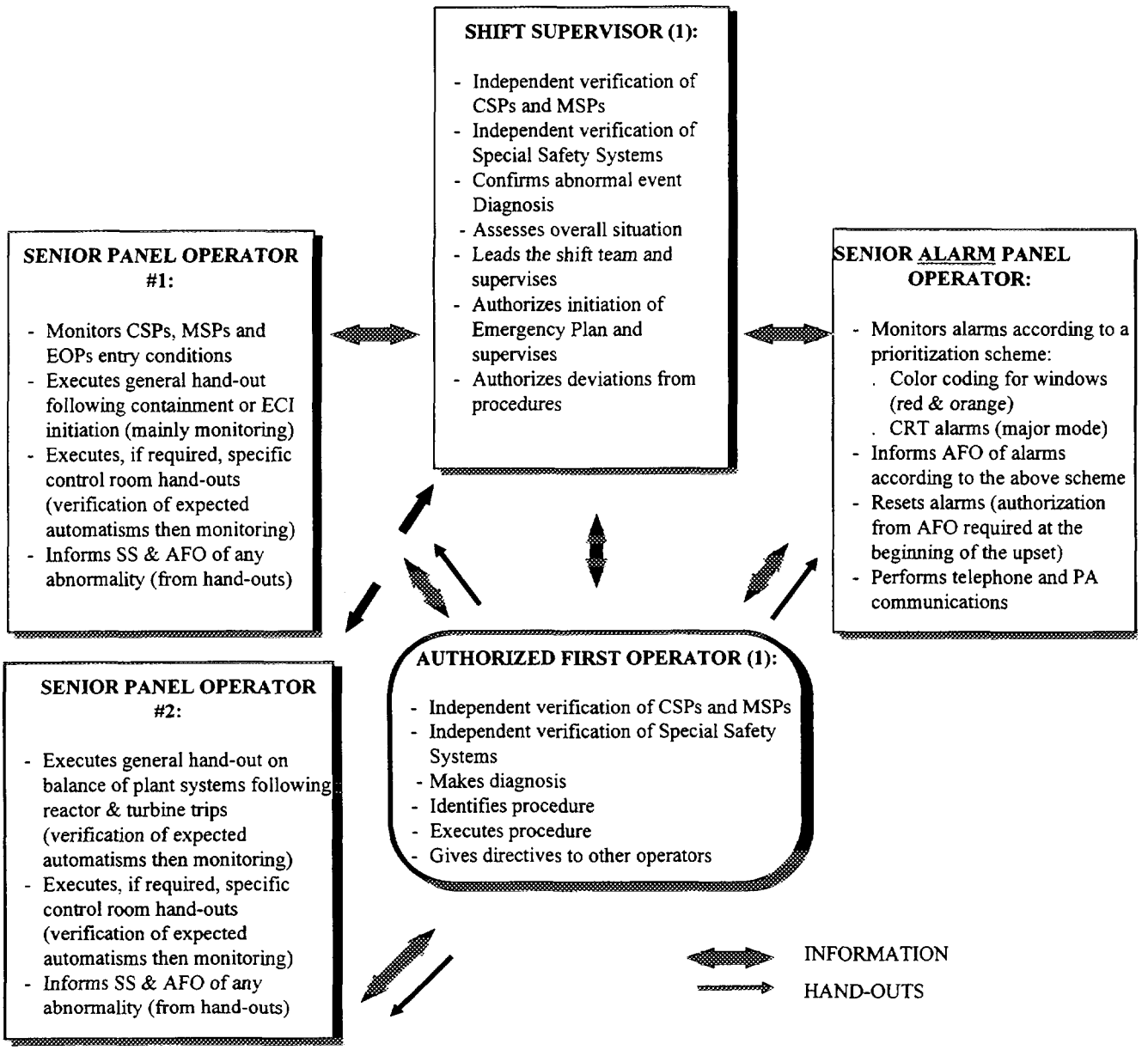


Figure 1.0-1: Number of Authorized Shift Supervisors (SS) and First Operators (AFO)

Figure 2.2-1: Control Room Staff Set-up During Abnormal Events



NOTE.
IF NEEDED THE SS MAY BRING APPROPRIATE CHANGES IN THE OPERATION STAFF SET-UP

Figure 2.3-1 Operating Response Strategy to Abnormal Event

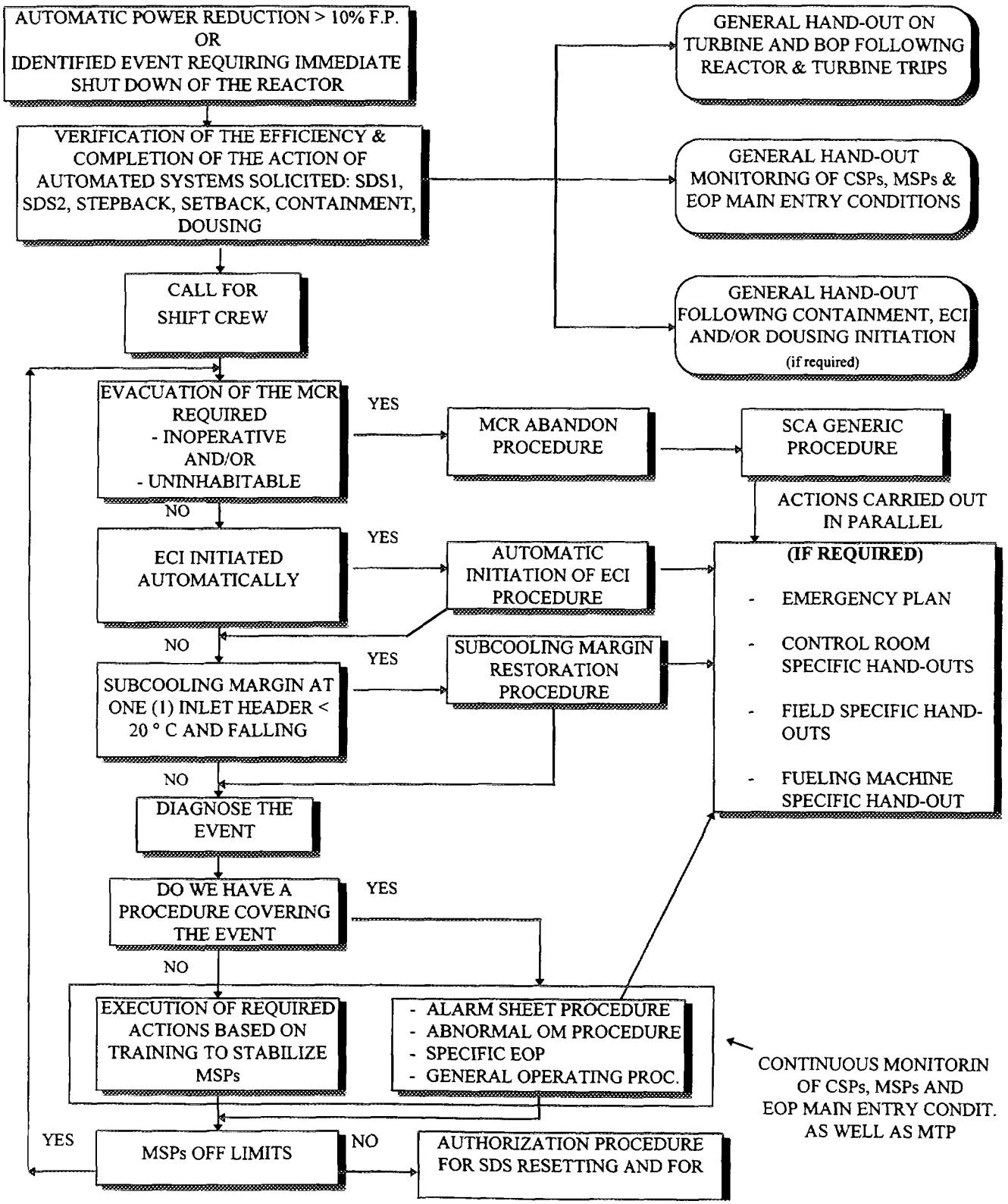


Figure 2.3-2 Station Specific Expectations and Good Practices
Following the Initiation of a SDS1 Trip
(Authorized First Operator)

2/3 RED WINDOW ALARMS ON SDS1 PANEL (Entry condition)

* - CONFIRM REACTOR POWER < 1% F.P.

* - CONFIRM SDS1 EFFICIENCY (AT LEAST 26 SORs IN CORE)
- ASK ALARM MONITORING SECOND OPERATOR TO CALL SHIFT CREW IN CONTROL ROOM
- ASK SECOND OPERATOR #1 TO TRIP THE TURBINE AND TO EXECUTE THE GENERIC HAND-OUT ON TURBINE AND BOP (3 BAR CHARTS)
- ASK SECOND OPERATOR #2 TO EXECUTE THE GENERIC HAND-OUT TO MONITOR CSPs, MSPs, AND OTHER PARAMETERS OF SPECIFIC EOP DIAGNOSIS (4 BAR CHARTS)

* - CHECK CSPs AND MSPs (2 BAR CHARTS)

* - CHECK IF ANY OTHER RED WINDOW ALARMS (EXCEPT SETBACK/STEPBACK)

* - CHECK ORANGE WINDOW ALARMS AND MAJOR CRT ALARMS

* - PERFORM DIAGNOSIS
- ALLOW RESETTING OF ALARMS
- EXECUTE APPROPRIATE PROCEDURE

* Independently done by the Shift Supervisor

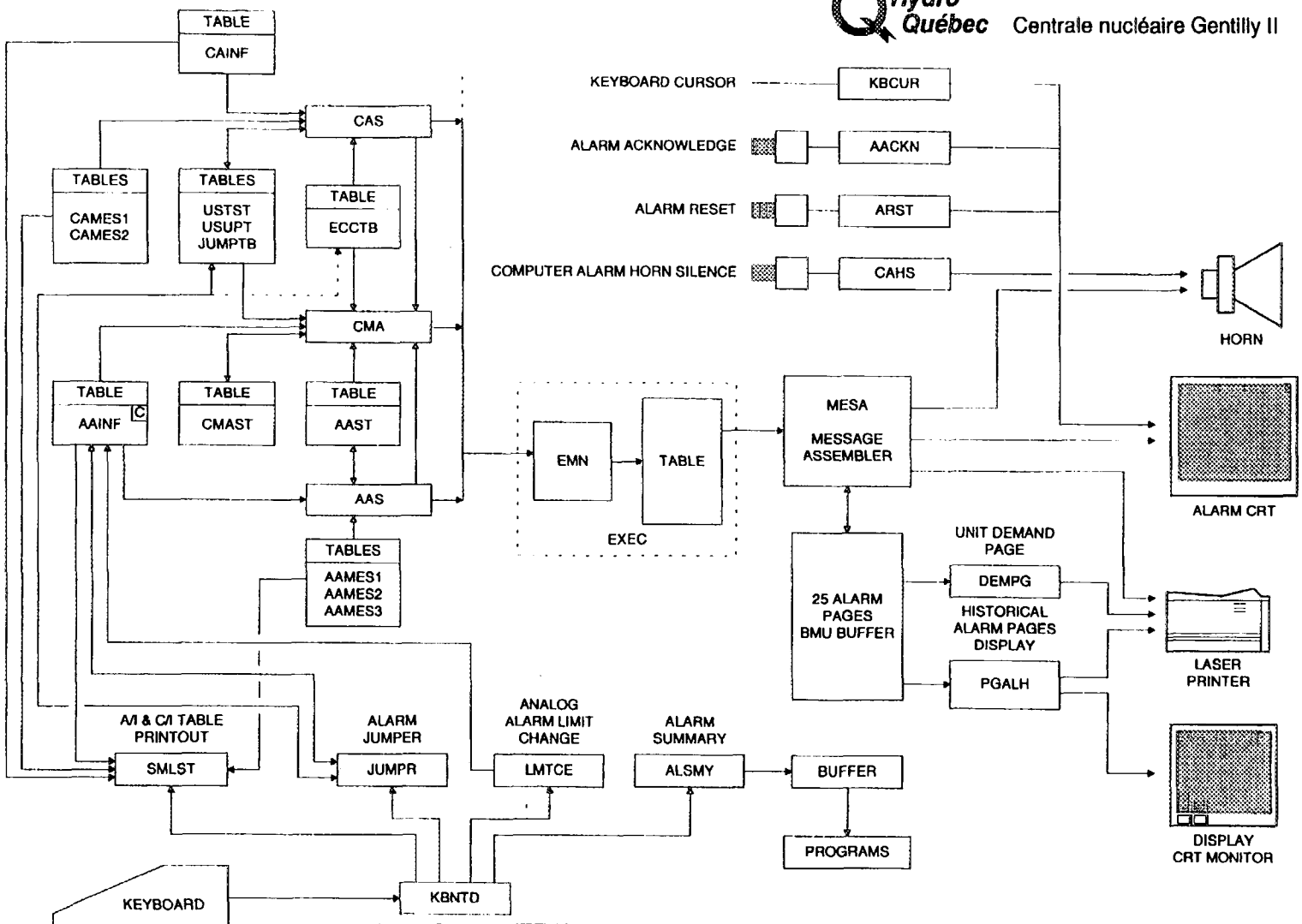


Figure 3.1-1 INTEGRATION OF COALESCENCE (CMA) IN ANNUNCIATION SYSTEM

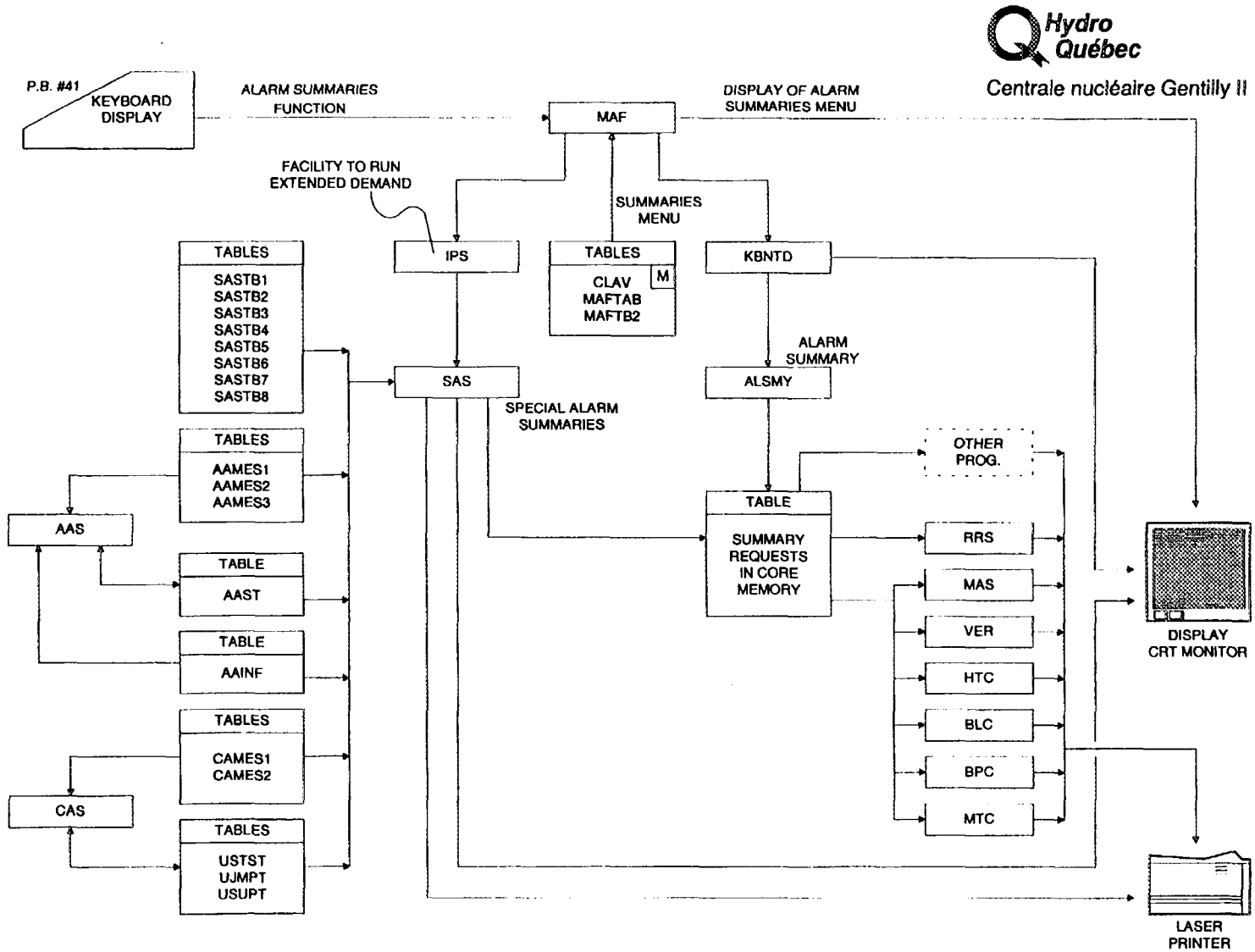


Figure 3.1-2 SPECIAL ALARM SUMMARIES (SAS)

ORDX SPECIAL ALARM SUMMARIES

0 ALL SUMMARIES
1 AFTER SDS#1 TRIP
2 AFTER REACTOR POWER REDUCTION

SS#1	FILTERED	MISSING
A/I	0	15
C/I	0	51

DATE/HR	12 SEP 1996	11:40:27

SUMMARY COMPLETE

ENTER : INDEX
(OR : INDEX/12345 FOR SPECIFICATIONS)

G02 0029

Figure 3.1-3 SPECIAL ALARM SUMMARIES INTERFACE

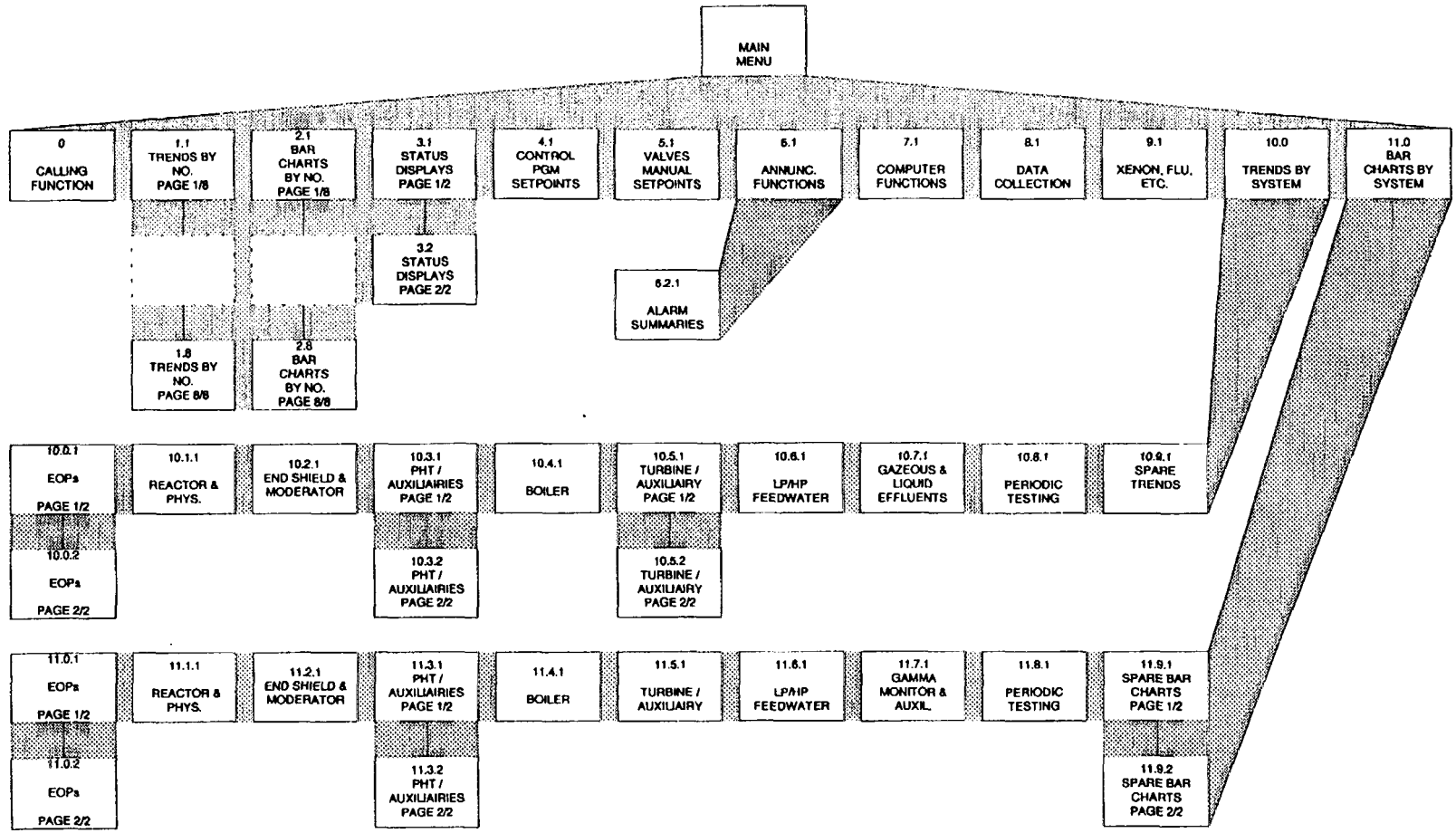


Figure 3.2-1 MAF - CALLING FUNCTION MENU INTERFACE: MENU LINKAGE

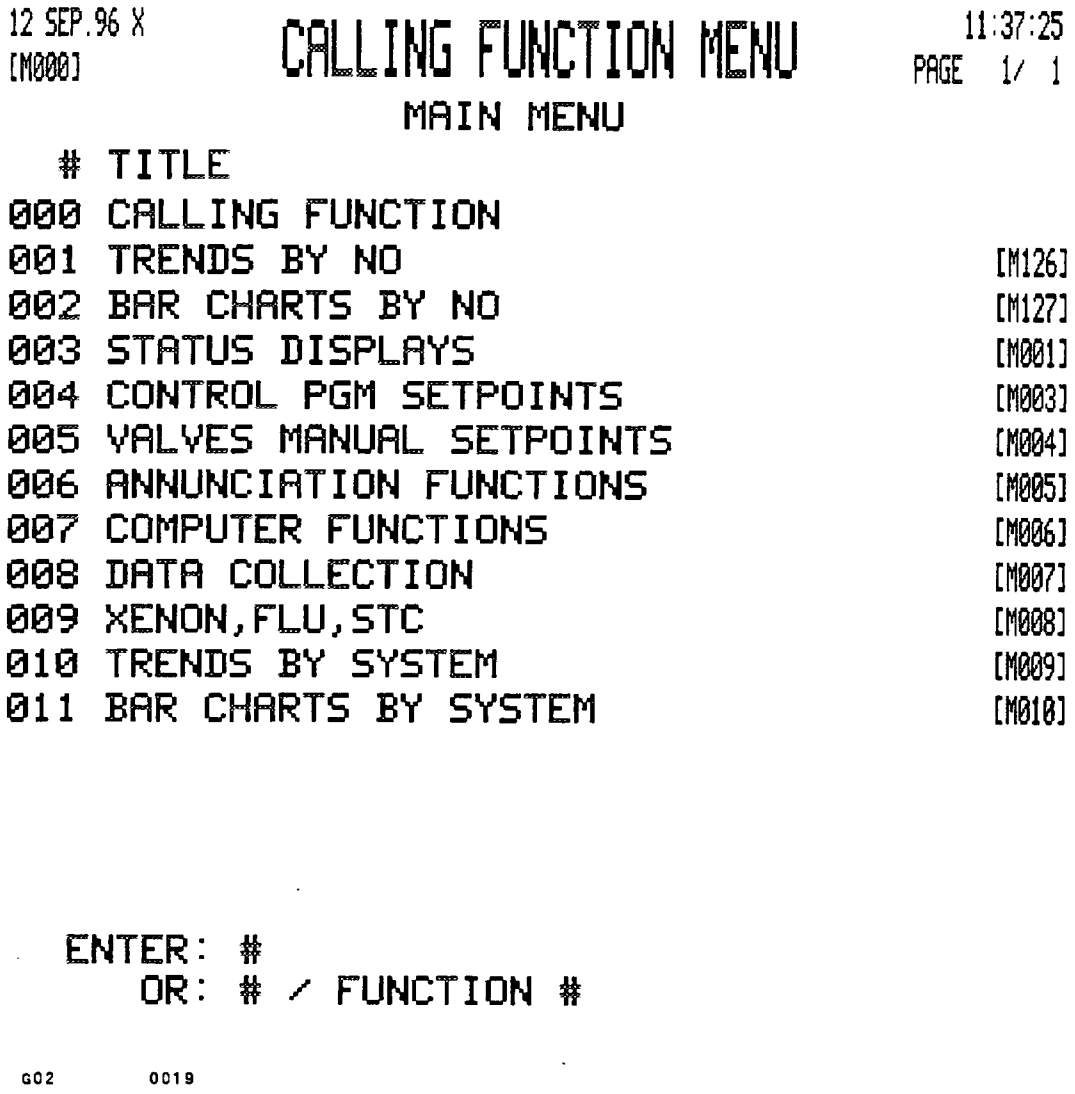


Figure 3.2-2 MAF - MAIN MENU

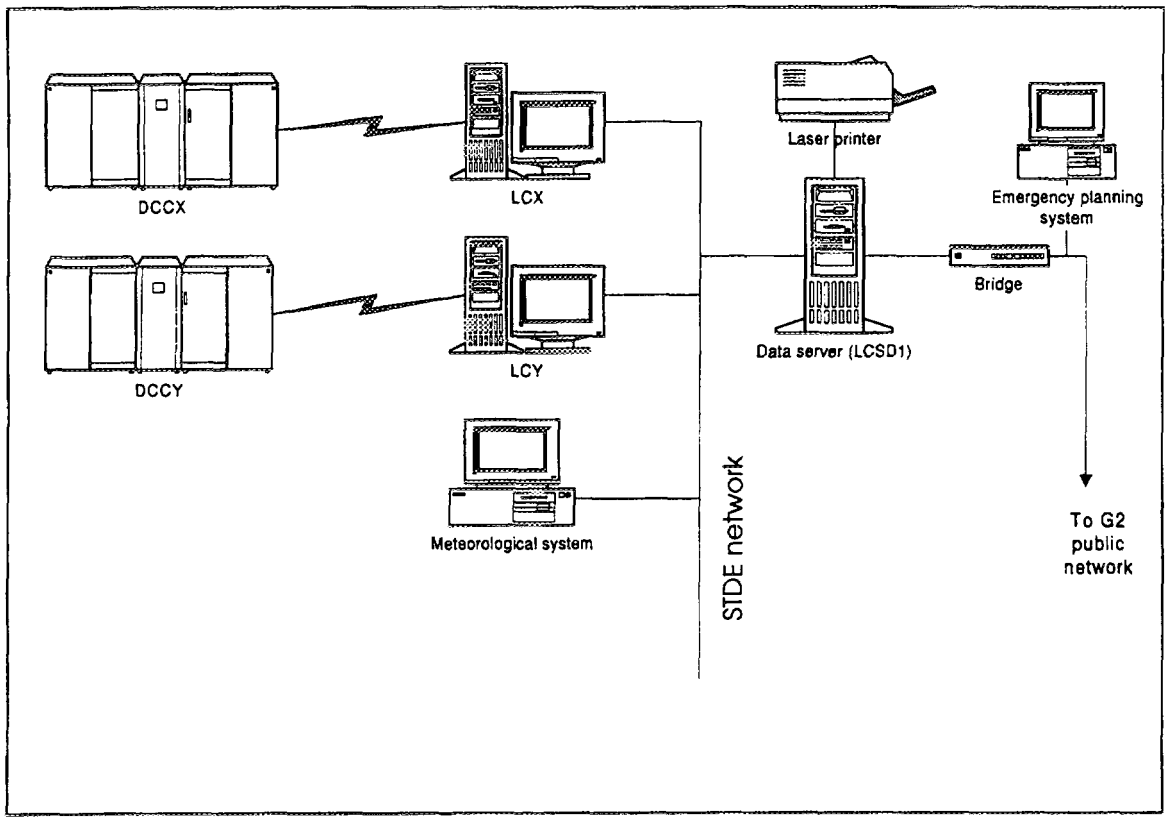


Figure 3.4-1 Actual network

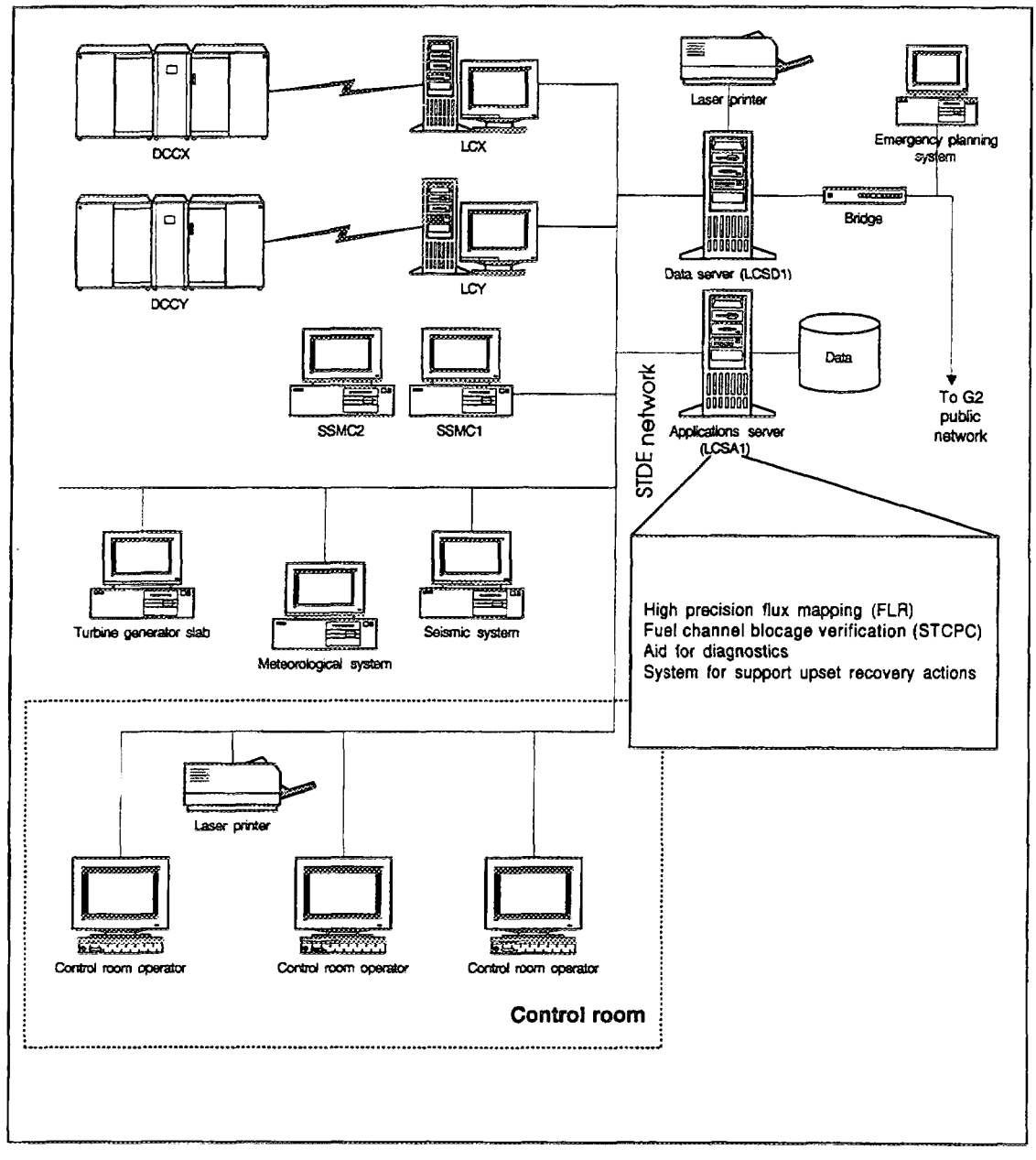


Figure 4.3-1 Projected network

DARLINGTON ANNUNCIATION: USER INFORMATION NEEDS, CURRENT EXPERIENCE AND IMPROVEMENT PRIORITIES

T. Long and E.C. Davey
Ontario Hydro and AECL
Ontario, Canada

ABSTRACT

The Darlington Nuclear Generating Station (DNGS) is located approximately 40 kilometers east of Toronto, Ontario on the coast of Lake Ontario. The station consists of four 935 MW(e) pressurized heavy water CANDU type units with a nominal power output of 850 MW(e) per unit. The station was designed and is operated by Ontario Hydro and provides electricity to meet the commercial, industrial and residential needs for 3 million people. Units 1 and 2 began commercial operation in 1990, followed by Unit 3 in 1991 and Unit 4 in 1992. Since commissioning in 1991, the station has continually achieved annual production of greater than 80% of capacity.

At Darlington, as in most other industrial enterprises, the plant annunciation systems play a key role in supporting operations staff in supervising and controlling plant operations to achieve both safety and production objectives. This paper will summarize the information needs of operations staff for annunciation of changing plant conditions, describe the operational experience with current plant annunciation systems, discuss areas for annunciation improvement, and outline some of the initiatives being taken to improve plant annunciation in the future.

1. INTRODUCTION

Operations staff at the Darlington nuclear power plant must assimilate and understand information from many sources to effectively manage plant operations. Over the life of the station, there has been an on-going evolution of operational practice and use of plant information systems to better support operational objectives. This evolution has been driven by:

- improvements to the understanding of the information needs of operations staff in support of basic plant operation,
- the creation of new information needs in response to new production and/or safety compliance needs,
- refinement of the information processing and display capabilities of existing control room information systems, and
- the introduction of new information system capabilities through retrofit systems.

The use and refinement of the control room annunciation systems has been part of this evolution.

The following sections will summarize the information needs of operations staff for annunciation of changing plant conditions, describe the Darlington operational experience with current plant annunciation systems, discuss areas for annunciation improvement, and outline some of the initiatives being taken to improve plant annunciation in the future.

2. INFORMATION NEEDS OF OPERATORS FOR ANNUNCIATION

2.1 Plant Supervisory Control

Within Ontario Hydro, the authorized nuclear operator (ANO) is assigned full responsibility and authority to control all aspects of unit operation within administrative limits. The ANO is assisted in this role by other members of the shift team, maintenance and engineering staff, and station management.

To achieve specific safety and production objectives, most middle and lower level plant functions have been highly automated. Even so, functions are rarely allocated exclusively to automation exclusively. In most cases, the performance of every function is shared between automation and humans on some basis (e.g., Operators establish setpoints for processes and perform general process surveillance on a periodic basis. Automation provides continuous control of process values to setpoint and immediately alerts operations staff to discrepancies in operation).

To carry out their responsibility, meet production and safety goals, and work effectively with automated systems; operators must be supported by information and control systems that allow them to actively supervise a highly automated process system, be responsively informed of off-normal conditions, and have the capability to intervene and substitute compensatory functions if automated functions should fail. Thus, successful supervisory control requires the cooperative control and monitoring of plant functions by both operators and automation [1].

In addition to direct supervision of unit operation, operators are expected to perform additional duties in support of station operation. The overall responsibilities of a control room operator can be classified into seven broad task areas:

- establishing and effecting operational objectives, both safety and production, for the shift (planning),
- developing and maintaining plant awareness (monitoring),
- handling plant disturbances and transients,
- controlling the plant state,
- supervising work protection and work control,
- maintaining plant availability (directing maintenance), and
- supporting administrative activities.

Current operational experience and former studies [2,3] indicate that more than 80% of the operator's time on shift is occupied by tasks other than those involved with direct process supervision and control of the unit. Even during instances when the unit is directly monitored, it

is only practical for operators to maintain an awareness of a very small subset of the available plant parameters. Consequently, operators depend on the plant annunciation systems to alert them to plant changes requiring intervention and to assist them in maintaining an up-to-date awareness of all important changes in plant conditions.

2.2 The Role of Annunciation

The role of annunciation is to ensure that control room staff are promptly alerted to and supported in their response to important changes in device, equipment, system or plant conditions that may impact on operational goals. In fulfilling this role, annunciation must perform three functions:

- detect and may predict the occurrence of plant changes,
- alert users to plant changes important for the current operating situation such that:
  - only operationally relevant plant changes are annunciated
  - the demands imposed on user's attention to recognize the plant changes fits with the demands of other concurrent control room tasks, and
- points users to additional plant information to understand and respond to the changes [4,5].

There are two kinds of changes in plant conditions that the annunciation should alert operators to:

- *Fault alarms* - challenges to current operational goals that represent potential or current problems in the plant (e.g., process disturbances or equipment faults), and

- *Status alarms* - changes in equipment, system or plant conditions that do not represent a challenge to current operational goals (e.g., confirmation of the completion of an automatic action).

Operators require timely information on both types of plant changes. Information on impending and current problems is required so operators can interpret what operational goals are challenged, and plan and prioritize compensatory actions. Information on other changes in plant conditions (i.e., not problems) is required to maintain an up-to-date awareness of the plant configuration. Such an understanding is essential for planning and prioritizing the response to impending or current problems (i.e. faults).

2.3 Situations To Be Supported

The annunciation system must support operators during all phases of plant operations. As a result, the annunciation system must successfully perform its functions across a wide variations in the rate of alarm generation/clearing and number of alarms active and across a wide variation in plant modes. A summary of the alarm state characteristics representative of different operating conditions and operational emphasis at the Darlington plant is provided in Table I [6].

Both typical and extreme values are shown to indicate the range of alarm state characteristics that must be accommodated.

Table 1. Alarm State Characteristics by Operating Phase

Operating Condition	Rate of Alarm State Changes		Number of Alarms Active	
	Typical	Extreme	Typical	Extreme
Stationary Conditions				
Full power operation	< 3/min	> 20/min	< 10	> 50
Shutdown	< 5/min	> 20/min	> 40	> 150
Changing Conditions				
Startup	> 5/min	> 50/min	< 40	> 150
Shutting Down	> 5/min	> 50/min	<50	> 300
Outages	< 5/min	> 20/min	> 150	> 250
Upsets (0-3 min)	> 50/min	>200/min	> 200	> 1000
Upsets (>3 min)	> 25/min	>100/min	> 150	> 800

2.4 Users to be Supported

In all operating phases, the ANO is the primary user of the annunciation system. Under normal operating conditions, the ANO is assisted by one additional person (a Supervised Control Panel Operator or SCPO) who is trained in monitoring the unit and alarm interpretation but is not permitted to undertake control actions. The SCPO may independently use information from the annunciation system as part of his/her normal duties associated with work control, system surveillance and system testing.

During plant upset conditions, additional staff join the unit crew to respond to the upset. Two ANOs from adjacent units, if available, join with the unit ANO and assist with stabilizing the unit under the unit ANOs direction. In addition the Shift Supervisor joins the response team to oversee response activities and provide an independent assessment of plant overall safety state. All of these individuals rely on information from the annunciation system to support their response activities.

2.5 Annunciation Information Needs

Information provided by the annunciation system should be designed to support operators in their tasks with respect to achieving operational safety and production goals. These tasks include maintaining plant awareness, interpreting alarms, diagnosing problems, and planning, prioritizing and effecting a response to problems; as well as for normal control activities. The following characteristics represent desirable properties of annunciated information:

Detection

- Detect all changes important to the achievement and preservation of plant operational goals.

- Time-stamp all changes whether relevant or irrelevant to support both control room diagnosis and later off-line analysis.

- Distinguish between alarm conditions that represent true plant changes and those that represent instrumentation failures.

Relevance Determination

- Base the determination of the operational relevance of plant changes on:

  - the physical state of the plant, systems and equipment, and
  - the transient state of the plant, systems and equipment (e.g., do not annunciate changes that are expected to occur briefly during a transient unless they are still present when they would be expected to have returned to normal).

Alerting

- Annunciate all plant changes relevant to the achievement of plant operational goals for the current operating situation:

  - DO NOT annunciate any plant changes that are irrelevant (i.e., those that are either expected or unimportant) to the achievement of plant operational goals for the current operating situation, and
  - Make information on all plant changes, including detected irrelevant changes, accessible on demand.

- Match the demands for operator interaction with the annunciation system with the demands of other tasks in the control room.

- Annunciate relevant plant changes with both discrete and easily identifiable "audible" and "visual" presentation components.

- Annunciate as "Expected but not occurred" fault alarms, those plant changes expected to occur during a particular event or transient or after a particular operation (e.g. a reactor trip) that do not actually occur.

Display

- Display plant changes in a manner consistent with human perceptual and cognitive capabilities to effectively use the information while simultaneously attending to other tasks.

- Display plant changes (e.g., fault alarms) in a manner such that their priority with respect to the operational goals for current equipment, system and plant state is obvious to the operator (i.e. present plant changes consistent with the plant situational context).

- Organize the presentation of plant changes consistent with the way operators use the information (e.g., separate fault from status alarms to simplify plant fault state determination, organize fault alarms by priority consistent with way operators order their response to problems and organize status alarms in a chronological time sequence to give the operators a picture of the evolution of the change in equipment, system and plant state).

- Display plant changes such that any new alarms, any return to normal alarms, any unacknowledged alarms and any acknowledged alarms are easily visually discriminable.

- To improve display efficiency, dynamically replace multiple individual alarms representing the same alarm condition in different information channels with a single higher level message that conveys all of the pertinent information that would have been obtained from each of the individual component alarms (i.e., alarm coalescing).

- Continuously display the current number of relevant and irrelevant fault alarms to assist operations staff in maintaining overall plant state awareness.

- Continuously display the current "plant mode" on all annunciation CRT screens to assist operations staff in maintaining overall plant state awareness.

- Provide at the operator's desk direct access from primary alarm displays to supporting information on each alarm (e.g., instrument source, conditioning factors, alarm response procedures). All of this should also be easily accessible for the annunciator window tiles.

- Provide operator customizable views of both the current and past alarm state of the plant to support alarm interpretation, upset diagnosis and display support for specific control room tasks (e.g., the ability to look in history for a particular alarm or group of alarms and their chronological evolution and the ability to look at all current alarms; whether relevant or irrelevant in various configurations of a current alarm summary).

- The physical configuration of the annunciation CRT display hardware should support BOTH the manner in which the ANO operates normally (alone) and the way the ANOs operate as a team during a transient.

Control

- Provide at the operator's desk console, a simple means to alter alarm setpoints and/or alarm jumper status; using proper station change control procedures.

Consistency

- There must be clear, understandable, defendable, documented, consistent methodologies (with rationale) for each of the following:

- CRT and Window annunciator tile message texts,
- Use of colour (for CRT annunciation and Window annunciator tiles),
- Use and selection of alarms requiring Window annunciator tiles,
- Abbreviations and acronyms, and
- Hysteresis and deadband determination.

- The separate annunciation systems that are used for shutdown system one and shutdown system two should operate consistent with normal annunciation system (i.e. should reflect all of the listed features and requirements from Section 2.5 "Annunciation Information Needs").

While not an operational information need, there is a clear requirement to have an effective and responsive means for effecting changes to annunciation systems so that the systems can be kept up to date with station operational needs. Factors that initiate the need for annunciation system changes include changes in production goals, regulatory requirements, technology or operating experience. The following characteristics represent desirable properties to support change:

- Provide effective information management tools to allow annunciation system software and hardware upgrades and changes to be made easily in a cost efficient manner; and consistent with station change control procedures. The kinds of changes to be accommodated include:

  - new alarm creation and alarm deletion,
  - changes to alarm text or logic,
  - changes in plant mode specification (e.g., determining parameters),
  - changes in relevance determining factors, and
  - changes in priority determining factors.

3. DARLINGTON ANNUNCIATION EXPERIENCE

3.1 Facilities and Functions

The Darlington control room contains separate control areas for each of the four reactor generating units, common services (e.g., electrical supplies), and on-power fuel handling systems. This has resulted in a division of alarm management responsibilities and the need for coordination of alarm management activities between staff supervising different control areas. The remainder of this paper will focus on alarm management associated with the operation of each reactor generating unit.

The control area for a Darlington generating unit includes both panel and console displays and controls (see Figure 1). The panels are organized on a system-basis and each panel contains annunciation indicators at the top and conventional indicators (e.g., edge meters, status lamps), computer displays, and equipment controls (e.g., handswitches and analog controllers) throughout the balance of the panel area. The operator desk console area provides four

computer-based displays to support integrated supervision and control of the unit. Operators use the computer displays as their primary source of information during supervision of stable plant operation and execution of startup, shutdown and power-change maneuvers [7].

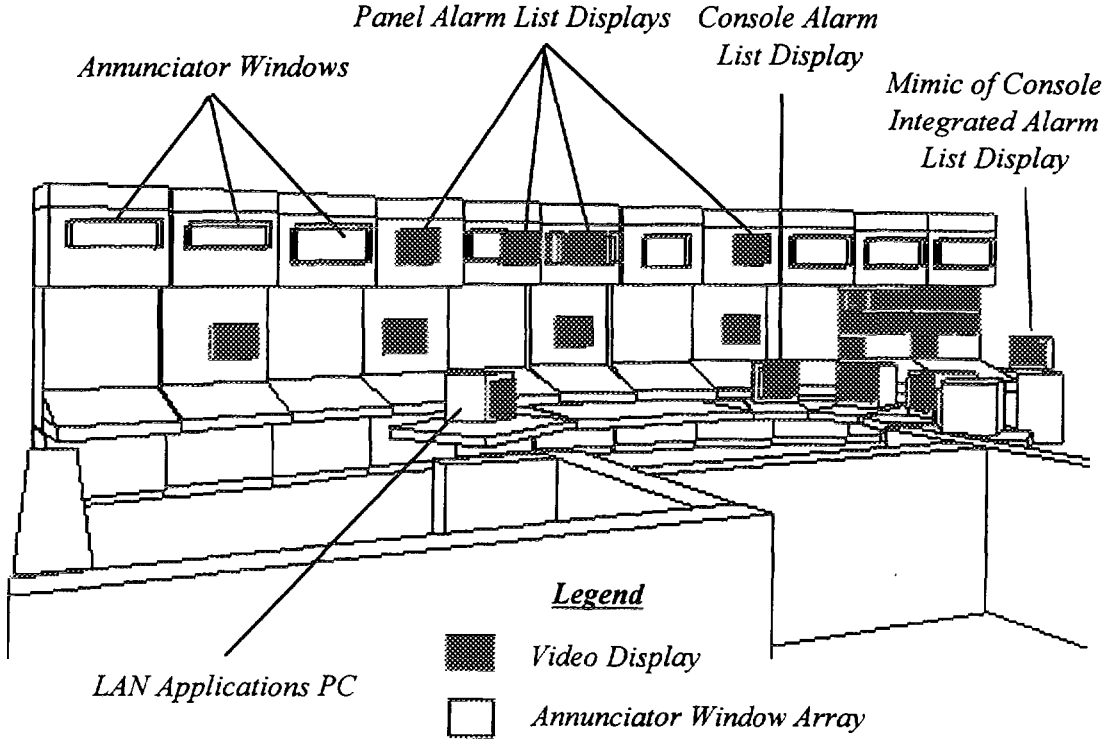


Figure 1: Darlington Generating Unit Control Area

There are two sources of annunciated information within each unit:

- computer-generated alarms displayed within panel and console displays, and
- alarms displayed on annunciator tiles at the top of each panel.

The computer-generated alarm displays enable changes in the status of more than 8000 analog, contact inputs and calculated variables to be individually annunciated. Four panel displays each provide a chronological listing of alarms associated with specific plant functions, one for each of:

- heat transport, emergency coolant injection and shutdown systems,
- reactor and moderator systems,
- electrical systems, and
- feedwater, turbine and common processes systems.

Each display has a presentation capacity of about 20 messages each. If more annunciation messages are available for display at one time, the most recent messages overwrite the oldest ones, irrespective of priority or relevance.

At the console, operators can display an integrated chronological listing of the most recent alarms from all 4 panel annunciation CRTs, or view alarm histories or current alarm summaries in various configurations. Printed alarm logs are also available.

The computer-generated alarm displays were intended as the primary annunciation support for normal use. The annunciator tiles were intended as a backup system to provide more limited safety related annunciation support on the unavailability of the computer-based annunciation.

3.2 Operational Experience

Overall the computer-based annunciation system supports operations staff well in understanding the alarm state of the unit during conditions when only a few alarms are present (e.g., normal stable operation and controlled power maneuvers).

Additional support for operators in linking individual annunciation messages with support material, such as alarm response procedures, is still desirable even during normal operations. Currently the Darlington computer-displayed annunciation messages contain no basic identifying code as to the operating manual where alarm detail information can be found (see Figure 2). This presents an additional mental burden on operators and can lead to operational inefficiencies associated with access and search for the appropriate reference material.

During conditions when many alarms are active and/or the alarm generation rate is high, the computer-based annunciation displays are less useful, for example:

- irrelevant alarms routinely overwrite displayed operationally relevant alarms as result of minimal relevance conditioning,
- the chronological listing of alarms shows only the most recent alarms rather than the most important to the operating situation, and
- the indicated and fixed priority of alarms based on the full power operating state may not be appropriate for the various other non-full power operating situations.

X PHT D20 RECOVERY 3382-P1 HS OFF NORMAL
X HT PUMP 1 TRIPPED
X STEPBACK HT PUMPS TRIPPED
Y ION CHBR CH A LOG PWR RATE IRR
Y MTC HX1 OUTLET TEMP LOW
X BLEED CONDENSER PRESSURE HIGH
X SDS1 MONITOR COMPUTER MESSAGE
X CDSR COOLING SPRAY STRNR DIFF PRESS HI

Figure 2: Example of Darlington Computer-displayed Alarm Messages

In such circumstances (e.g., upsets and outages), alternative alarm management strategies are employed.

During plant upsets, the panel and console alarm lists can be 'flooded' with alarm messages making the computer alarm displays temporarily unusable. Consequently, the station upset response strategy directs operations staff to use the backup panel annunciators to track changes in the plant safety and production state, until the demands of the transient on the ANO relax such that printed alarm summaries can be taken and carefully reviewed to identify all the relevant alarms to address. In such instances, the ANO must locate the few key relevant alarms buried within the hundreds of relevant and irrelevant alarms listed on the summary printouts. While this approach has proven operationally acceptable, it provides a much more limited indication of the alarm state of the unit and leads to delays between alarm occurrence and operations staff recognition. The annunciator tiles are limited in number (i.e., 100s versus the 1000s of potential plant CRT alarms), and primarily safety-related. Thus, they do not provide as full annunciation support associated with the production side of the plant.

During outages, several hundred or more alarms can be active and most are irrelevant or inappropriately prioritized. Again, operators must take periodic printed alarm summaries to assist in maintaining an awareness of the full alarm state of the plant.

In many operating conditions, a majority of the alarms operators are alerted to are operationally irrelevant. The presence of these alarms provide an unnecessary distraction and can further complicate the task of understanding the true alarm state of the unit. A conditioning capability exists within the computer-based annunciation program but has not been extensively utilized due to the perceived effort required to analyze conditioning relationships.

4. PRIORITY AREAS FOR IMPROVEMENT

The previous discussion has highlighted some of the operating situations and tasks where improved annunciation support would be desirable. Based on operational experience, the following areas represent priority areas for annunciation improvement:

4.1 Access to Reference Information

Simplification of the secondary tasks operators must perform to locate and access alarm reference information could substantially improve alarm response management. Providing direct references to the location of reference information within alarm messages or electronic links between alarms on console displays and the display of reference information are two means of providing improved support for this task.

4.2 Presentation of Unit Alarm State

An improved real-time presentation of the alarm state of the unit is required that better matches the way operators use alarm information is needed. Separating fault and status alarms into

separate displays and listing fault alarms by priority is one display organization that has been shown to provide better operator support.

4.3 Suppression of Irrelevant Alarms

In upsets and outages, the majority of the alarms operators are alerted to are operationally irrelevant and complicate the task of understanding the true alarm state of the unit. Recent annunciation development work sponsored by the CANDU Owners Group has demonstrated that substantial operational benefits can be obtained with limited application of alarm conditioning [8].

4.4 Dynamic Prioritization

The importance for most alarms is a function of the plant operating state. Thus the indication of an alarm's priority should change as the plant operating conditions change. Such a dynamic prioritization approach would better assist operations staff in determining the most important problems to deal with across all operating conditions.

4.5 Operator Selectable Alarm State Views

To support the use of alarm information in specific tasks, operators and other staff should have the capability to customize the organization of console alarm displays using either current or historical alarm data. Such custom views can simplify user alarm search, identification tasks and troubleshooting occurrences or transients.

4.6 A Consistent Annunciation Strategy in all Alarm Generating Systems

Operators rely on information from several alarm generating systems in managing unit operations and there is no consistency in annunciation strategy and alarm presentation conventions from system to system. This provides an additional burden for operating staff when simultaneously interpreting information from multiple alarm generating systems. A consistent annunciation strategy and conventions should be established and worked towards as systems are routinely upgraded. (This is especially important for the Darlington annunciation systems for Shutdown system one and Shutdown system two).

5. STATION INITIATIVES FOR IMPROVEMENT

There have been several initiatives undertaken throughout the station life to improve the effectiveness of station annunciation. The initiatives discussed in this paper are in addition to the on-going operations and engineering efforts to improve annunciation message texts, response procedures and creation of new alarms to support specific operational needs. Specific initiatives are described below.

5.1 Quality Improvement Program Man-Machine Interface Review

During 1991 a small team of operations and engineering representatives performed a comprehensive review of 'problems' associated with the control room operator interface. This review organized problems with reference to specific operator tasks and prioritized recommendations for improvement. Over forty specific improvements to the annunciation systems were identified. The findings and recommendations from this study have been used to guide the development of improvements to the control room interface and annunciation over the past few years. However most of the identified areas for annunciation improvement have not been addressed as of yet.

5.2 Improvements to Historical Alarm Recall and Search

An enhancement to historical alarm recall and search was installed to simplify the operator's task in locating alarm records of interest within alarm logs. The original historical alarm recall and search capability was limited to a sequential paging method that imposed high interaction demands on users and was tedious to use. The new recall and search capability allows users to locate alarms of interest in a number of useful methods and configurations (e.g. by group or date/time period specification).

5.3 Improvements to Real-Time Annunciation Display

Several display improvements to improve the ability of operators to monitor the alarm state of the unit. A real-time chronological listing of all active alarms was created for console display to complement the use of the four panel alarm lists. This combined alarm list display substantially helps operators understand the integrated alarm state of the unit.

To improve alarm monitoring during safety system testing, a display that mimics the console chronological listing of all active alarms was added to the right end of the safety system panels. This display allows the alarm state of the unit to be monitored while the operator is performing safety system testing tasks.

5.4 Participation in CANDU Owners Group Annunciation Improvement Program

Darlington has always been a strong supporter of and key contributor to the CANDU Owners Group (COG) annunciation improvement program. When the annunciation concepts being developed began to show operational promise, several in-station demonstrations of the concepts were arranged to solicit comments from a broad mix of station staff. These familiarization demonstrations culminated in a series of demonstrations in 1995 March where a Darlington 'Loss of Class 4 Power' upset was demonstrated to all operations staff over a period of two days.

Based on the in-station support for the concepts demonstrated, a series of 20 simulator exercises was conducted during early 1996 to compare the relative annunciation support provided by the existing annunciation system and new COG annunciation concepts. Ten operations crews

participated as subjects in these exercises. The results showed the COG annunciation concepts offer substantial operational benefits over a range of plant operation phases [8].

5.5 Annunciation Retrofit Feasibility Study

During 1995, AECL in conjunction with Darlington staff investigated the technical feasibility and cost/benefit of applying the CANDU Annunciation Message List System (CAMLS) annunciation improvements for retrofit to the Darlington annunciation system. The study had three main tasks:

- to propose a Darlington annunciation retrofit strategy based on CAMLS concepts,
- to specify the hardware and software options for implementation, and
- to estimate the costs of implementation and the financial benefits to be realized from the annunciation improvements.

The findings from this study indicated a payback period of 3 years for a proposed retrofit implementation.

5.6 Improvements to Message Components and Formatting

A manual of standard acronyms and abbreviations has been established and applied to all plant alarms to improve alarm message consistency across plant systems. Message formatting was also standardized so that fields within alarm messages align from message to message. The improved alarm messages will be put into operational use later this fall.

5.7 Linking Alarms to the Location of Supporting Reference Information

A "system acronym" has been added to the beginning of each Darlington CRT alarm message indicating the operating manual where reference information (e.g., alarm response procedure) for the alarm is located. This improvement will remove the need for operators to memorize and rapidly recall the operating manual for each alarm. However, operators will still be required to tediously search through the manual to locate the appropriate alarm reference information. The improvement will be put into operational use later this fall.

5.8 Improvements to Shutdown System Annunciation

This project in ongoing and is currently still at the design stage. ANO input is actively being employed for the project.

6. CONCLUSIONS

This paper has outlined how the plant annunciation systems play a key role in supporting operators in supervising and controlling plant operations. While some fundamental needs for annunciated information are being met by the current Darlington annunciation systems, there is still room for much improvement in several key areas. Darlington staff are continuing to evolve

the understanding of the need for annunciation and how improvements to the current annunciation systems can be incorporated to better meet safety and production needs. We are confident that, in weighing cost effectiveness, cost consciousness and current initiatives for attaining "Nuclear Excellence in operations", further improvements to Darlington annunciation will be implemented to better support operations staff in their tasks to supervise unit operations.

7. ACKNOWLEDGMENT

Many people have contributed to the understanding of the role of annunciation in supporting Darlington station operations and the initial development and continuous improvement of the station annunciation systems. First, the authors would like to acknowledge the experience and insights shared by colleagues in operations who depend on the station annunciation systems from shift-to-shift. Second, we would like to acknowledge the contributions of Debbie Scott-Gillard, System Engineer for Annunciation, who has championed several annunciation improvements over the years and who provided helpful comments and suggestions for the preparation of this paper.

REFERENCES

[1] SMITH, J.E., "Modern Control Room Design Experience and Speculation", Proceedings of the 2nd ASME/JSME Nuclear Engineering Conference, San Francisco, California, 1993.

[2] WILLIAMS, M.C., "The Role of the Control Room Operator", Proceeding of the Joint Conference on Human Factors in Control Room Design and Operation, Canadian Nuclear Association, Toronto, Ontario, 1982.

[3] KORTLANDT, D. and KRAGT, H., "Ergonomics in the Struggle Against 'Alarm Inflation' in Process Control Systems - Many Questions, Few Answers", Eindhoven University of Technology, Department of Industrial Engineering report Journal A, Volume 19, No. 3, Eindhoven, Netherlands, 1978.

[4] DAVEY, E.C. and GUO, K.Q., "Towards Defining the Functional Role for 0CANDU Annunciation", Proceedings of the IEEE 5th Conference on Human Factors and Power Plants, Monterrey, California, 1992.

[5] DAVEY, E.C., FEHER, M.P. and GUO, K.Q., "An Improved Annunciation Strategy for CANDU Plants", Proceedings of the American Nuclear Society Conference on Computer-based Human Support Systems: Technology, Methods and Future, Philadelphia, Pennsylvania, 1995.

[6] Personal experience of the authors and operating colleagues at Darlington NGS.

[7] FENTON, E.F. and DUCKITT, W., "The Darlington Control Room and Operator Interface", Proceedings of the Human Factors Society 35th Annual Meeting, San Francisco, California, 1991.

[8] FEHER, M.P., DAVEY, E.C. and LUPTON, L.R., "Validation of the Computerized Annunciation Message List System", Proceedings of the IAEA Specialist Meeting on Experience and Improvements in Advanced Alarm Annunciation Systems in Nuclear Power Plants, Chalk River, Ontario, 1996.

SESSION II

REGULATORY PERSPECTIVE

CONTRIBUTION OF COMPUTERIZATION TO ALARM PROCESSING: A FRENCH SAFETY VIEW

Williams Cette
Institut de Protection et de Sûreté Nucléaire, IPSN/DES
Fontenay-aux-Roses, France

ABSTRACT

Following the TMI accident and according to the requirement of the French safety authority, very important studies were performed by the French utility, Electricité de France (EDF), and assessed by the Institute for Nuclear Safety and Protection (IPSN) on reactor operation in conventional control rooms, particularly on alarm processing. These studies dealt with the man-machine interface, as well as design and exploitation requirements, presentation and management of alarm signals, and associated operating documents. The conclusions of these studies have led to improvements in French conventional control rooms. The current state of these control rooms and links between alarm sets and operating documents will be shortly presented in the first part of the paper.

More recently, the computerized means implemented in the PWR 1400 MWe control rooms (N4) profoundly modified reactor operation. In particular, major advances concern alarm processing in comparison with conventional control rooms. The N4 plants provide a more rigorous approach in processing and presentation of alarms than in the past. Indeed, EDF wanted to have less alarms switched on during plant upsets and to make them more characteristic of a specific situation of the process. For example, computerization makes it easier to validate or inhibit alarms according to the situation, to allow the operator to manage alarm presentation and to propose on-line alarm sheets to the operators etc. This approach in comparison with conventional control rooms, and the IPSN assessment will be presented in the second part of this paper.

1. INTRODUCTION

One of the lessons learned from the Three Mile Island accident, was that control action staff must be provided with pertinent information on the state of the installation and must be given instructions which enable them to make the best use of the information they have available to them in order to manage incidents and accidents effectively. In France, post-TMI deliberation has led to two major areas of improvement in operating safety. These consist of :

- the setting in place of incident and accident operating instructions, classified in French by the letters I (incident), A (accident), H (beyond design basis) and U (ultimate), and more recently, Emergency Operating Procedures (EOP's) using the state-oriented Approach (APE): symptom-oriented EOP's,

- review of the control room design. The most recent ones (N4 series) which have been totally computerized take into account equipment and system fault alarms and situation information, and restore alarm signals which are filtered and processed according to the situation.

2. THE ROLE OF ALARM SIGNALS

The General Operating Rules (RGE) approved by the French safety authority, specify the operating conditions to be met so that the installation complies with the hypotheses adopted in the design studies. The alarm signals play a part in meeting these operating conditions set by the General Operating Rules and, in particular, contribute:

- **regarding normal operation of the unit :**
  - to guaranteeing that the unit remains within the normal operating range planned at the design stage and specified by the Technical Specifications for Operation (STE),

- **regarding incident and accident prevention :**
  - to guaranteeing the availability of equipment and systems which are important for safety particularly by means of the equipment unavailability alarms required by the Technical Specifications for Operation,

- **regarding control of incidents and accidents:**
  - to detecting entry into the field of incident operation (implementation of the protection system) and accident operation (implementation of the safeguard systems),
  - to diagnosing the incident or accident,
  - to guiding the operators towards the appropriate control action to limit the consequences of the incident or the accident to an acceptable level.

3. CONVENTIONAL 1300 MWE REACTOR CONTROL ROOM

3.1 Operating Requirements Associated with Alarm Signals

All alarm signals usually indicate a fault which needs to be corrected either by an operator or automatically. An automatic action and an instruction for action are usually associated with the notion of an alarm. Under the provisions made by EDF on the 1300 MWe series and in accordance with the regulations, the operating requirements corresponding to the alarm signals present in a French 1300 MWe reactor control room are generally organized on the basis of :

- **Main System Affected**
  - Which main system is affected determines where the alarm windows are placed within the control room (that of other information and other controls belonging to this system) and the equipment classification (that required by the design studies for this system). This classification requirement leads to a requirement level in terms of periodic tests.

- **Operator Reaction Time**
  - The alarms are ranked in accordance with how urgently an operator must react when the alarm signal appears. The appropriate action must be able to be carried out within a given time limit, and if not, it must be automated (protection system and safeguard system etc.). Each degree of urgency is given a corresponding color:
  - red (urgent manual treatment of the fault)
  - yellow (manual treatment of the fault which may be deferred),
  - white (basic automatic action which must be monitored to ensure it functions properly),
  - green (automatic action : safeguard, protection, load rejection etc.).

The 276 red alarm signals are presented on windows, the 2,900 others are on screens.

- **Use in Accident Control Action: Alarm Signals Labeled "D"**
  - Alarm signals labeled "D" are used for accident diagnosis. If such an alarm signal appears, the operator must take the orientation document which will either direct him to an operating instruction or towards an alarm sheet, depending on the severity of the situation.

This category of alarm signals labeled "D", in addition to the four color categories, came into being with the development of the I, A, H and U incident and accident control action procedures, taken from lessons learned from the TMI accident.

The IPSN has noted, during its analysis of event-oriented accident control action procedures for the 1300 MWe series, that the requirements for periodic tests and for requalification associated with the system to which the alarm signal belongs, only take the "normal operation" and "accident prevention" aspects described above into consideration, since the "control of incidents and accidents" aspect appeared after the design studies. Therefore, the classification level for the equipment does not always correlate to the operating requirements which are associated with the alarm signals used for diagnosing the accident.

Following this analysis, the French safety authority requested EDF to consider the matter, with the following aims in mind:

- to rank the alarm signals according to their safety roles in accident control action,

- to specify the associated operating requirements for the different categories of alarms, particularly those affecting operating redundancy, and the exhaustiveness of periodic tests.

EDF will be giving consideration to this matter in the context of the next safety reassessment of the 1300 MWe series units.

3.2 Improvements of the Emergency Operating Procedures

In order to improve processing of incident or accident situations, improvements have been made in the use of alarm signals. They make the post-accident control action less dependent on the initial diagnosis, and thus on the alarm signals which detect entry into incident or accident control action.

The symptom-oriented SPI operating instruction used by the Safety Engineer, in conjunction with the event-oriented accident instructions applied by the operators, introduces a redundant and diversified diagnosis which could lead the operators to apply the U1 emergency operating instruction.

More recently, the progressive setting in place of the physical thermal-hydraulic symptom-oriented approach EOP's, with the implementation in particular of a periodic diagnosis of the state of the unit and re-orientation integrated into the operating instructions available to the operators, means it is always possible to operate the unit properly, even should an incident or accident situation arise.

4. PROCESSING ALARMS IN THE CASE OF THE N4 SERIES

4.1 General Introduction

4.1.1 Changes in Regulations

Following the TMI accident, consideration by the safety authority in France has led to the establishment of directives relating to the safety characteristics and obligations to be applied in the N4 series nuclear units, specified in orientation letter CAB No. 1121 - MZ of 6 October 1983. The existence in the general provisions to be applied, of provisions relating to installation control action constitutes an innovation. Certain obligations and characteristics apply to alarm processing:

A) The provisions made as regards installation control action must in a general way aim to help the personnel as extensively as possible enabling them to carry out their control action task under optimum conditions and, in particular, must aim to :

   a) ensure the operators have reliable and clear information on the state of the installation, based on instrumentation from an appropriate range with implantation which minimizes the risk of errors,
   b) provide the operators with the means to present information on the state of the installation for accident or incident conditions, in a clear summary form to assist them in establishing a diagnosis of the installation. They must also be provided with the appropriate instructions, adapted to the use of these means, enabling appropriate work deadlines to be met,
   c) make it possible to maintain the parameters which represent the state of the installation in the limits specified for each operating system envisaged, and, at the

same time, to implement the means for adequate action when these parameters reach certain pre-determined levels, and

d) record the necessary information to make it possible to follow, reconstruct and analyze the situations in which the installation is found, particularly in the event of an anomaly.

B) The following provisions are proposed by EDF to this end and are acceptable in principle:

e) analysis of the states of core cooling which enable the diagnosis means available to the operators to be increased, and the effectiveness of the actions to ensure core cooling under optimum conditions to be improved,

f) a data processing system which helps the personnel in normal or disturbed operation of the installations,

g) redundant monitoring of the proper development of the post-accident phase is carried out by a person who is independent from the operators."

4.1.2 Technological Changes

The provisions made by the operating organization with regard to the safety characteristics and obligations set in general terms by the letter CAB 1121 MZ mentioned above, have led to the current control room of the N4 series. One of the innovations of the N4 series consists of the main man-machine operating interface "KIC" which is totally computerized.

The computerized operating interface is made up of four workstations, each one consisting of:

- three graphic screens which show portions of the systems and the computerized alarm sheets and instructions,
- four alarm screens,
- a screen to show discord between the order and the report, and
- various touch-sensitive screens, keyboards and a track ball.

The implantation of these different components was validated on a simulator of N4 series control room development phase. In the event of failure of the "KIC", a "conventionally" implemented auxiliary panel makes it possible to bring the unit back to a safe state whatever its thermal-hydraulic situation. A conventional alarm signal control panel located on the auxiliary panel presents around 300 alarm signals, in particular the alarm signals labeled "D" used for diagnosing incident and accident situations.

4.2 Processing Alarm Signals in Normal Operation

Computerizing the control action system makes it possible, among other things, to filter the alarm signals so that only those which represent the thermal-hydraulic conditions of the process are presented. Thus, the way alarms are processed on the N4 series includes considerable innovations in comparison with the previous series. More particularly, the operations offered by computerization make the following possible:

- inhibition processes for non-pertinent alarm signals and adaptation of these processes to the operating context,
- better functional ranking of the alarm signals,
- use of more selective display mechanisms and an alarm dialogue enabling them to be sorted in different ways,
- on-screen display of the alarm sheets and direct access to the controls from these alarm sheets.

As a result of these options, EDF has established design principles for the N4 series which are more advanced than those of previous series and are briefly explained in the following sections.

4.2.1 Processing Alarm Signals According to Situation

Besides the basic inhibitions for non-pertinent alarm signals, for example the "very low level" alarm signal inhibiting the "low level" alarm signal, the way the situation is processed makes it possible to inhibit the alarm signals which are not useful for the unit's state.

The situations' definition is based on the criteria taken into account for the Technical Specifications for Operation (STE): fullpower, shutdown, safety injection system, load rejection, etc.

At a given moment, the unit is in a single normal, incident or accident operating state. By design there may only be one single situation which validates the alarm signals at a given moment.

The operator is informed if this calculated general situation change. He is aware at all times of the situation determined by the "KIC". However, the operator is still able to modify the situation taken into account for processing the alarms. In this case, the alarm signals present are validated both by the situation calculated by the "KIC" and that chosen by the operator. If the situation calculated is incident or accident, the processes automatically take this new situation into account.

In order to overcome possible inconsistency, the IPSN considered it important to ensure at best that the alarm signal validating situations were consistent with the standard states of the Nuclear

Steam Supply System in the sense of the Technical Specifications for Operation. Modifications in this area were made by EDF (cf. § 4.3.1.1.).

4.2.2 Principles Behind Alarm Category and Severity Organizational System

The principle of dividing alarms into color categories which came from the conventional control rooms, has been reapplied to the N4 series. The computer processing of alarm signals made it possible to introduce the notion of alarm severity into the N4 series. A sub-category specifies, for red, yellow and green alarm signals, the severity of the alarm, using a number from 1 to 3 in decreasing order of severity.

The following table summarizes the various principles behind the alarm category and severity system:

<table>
<tr><th></th><th>SEVERITY 1</th><th>SEVERITY 2</th><th>SEVERITY 3</th></tr>
<tr><td>GREEN
(automatic action)</td><td>Orders to start up Containment Spray and Safety Injection Systems.
IKIC and « entry in symptom-oriented EOP's »</td><td>Orders for an emergency shut-down</td><td>Orders to trip the turbine, of load rejection, load reduction, and Main Steam and Feedwater Flow Control System isolation</td></tr>
<tr><td>RED
(urgent manual treatment of fault)</td><td rowspan="2">Risk of calling safeguard systems into operation or of passing into a beyond-design-basis situation</td><td rowspan="2">Risk of losing availability (emergency shutdown load rejection) or of losing safeguard system availability</td><td rowspan="2">All other cases</td></tr>
<tr><td>YELLOW
(manual treatment of the fault which may be deferred)</td></tr>
<tr><td>WHITE
(automatic action)</td><td colspan="3">Basic automatic action, the proper development of which must be monitored by the operator.</td></tr>
</table>

In addition, the alarms are given a name associated with the origin of the fault, i.e. alarm concerning the main coolant system, the secondary coolant system or the overall system.

4.2.3 Presentation of Alarm Signals to Operators

The alarm signals are presented on the four alarms screens at the workstations following the diagram below:

SCREEN A1 Screen displaying ***RED*** alarm signals	**SCREEN A3** Screen displaying and for holding ***GREEN AND WHITE*** alarm signals
SCREEN A2 Screen displaying ***YELLOW*** alarm signals	**SCREEN A4** Screen for holding ***RED AND YELLOW*** alarm signals

The alarm signals are presented to the operators in the form of lists in decreasing order of severity on the screens A1 to A3. Several alarm lists may be displayed on an A4 screen, i.e. sorted by severity, by time, by main system, by-alarm signals inhibited by another alarm signal or by the situation context etc.

Generally speaking, the operations associated with the alarm dialogue are subject to ergonomic assessment during the testing phase on the S3C simulator (control room and instrumentation and control). The IPSN has been involved with this testing phase. These tests have led, in particular, to a distinction being made between managing and seeing alarm signals.

4.2.4 Alarm Signal Management

The workstation controls provide various operations such as, an alarm signal erasing request, consideration request, display of the alarm sheet or of the equipment sheet for equipment fault alarms etc.

Taking an alarm into account makes it possible to display the associated alarm sheet on the control action screen and to have direct access to the controls from that alarm sheet. The holding of an alarm signal only applies to an alarm signal taken into account. It changes the screen for a red or yellow alarm signal.

The testing phase on the S3C simulator, with which the IPSN was involved, showed that the alarm dialogue and the presentation principles adopted would enable the operators to act the most important alarms within five minutes in normal situations, the time between when a category 1 red alarm signal appears and when the alarm sheet is displayed being on average around one minute.

In incident situations, the most significant alarm sheets are displayed in the first two minutes.

4.3 Processing Alarm Signals used in Post-Accident Control Action

Several major changes regarding the way alarm signals are processed during incident or accident control action have appeared in the N4 series. They regard :

- The introduction of a single alarm signal detecting the entry into an accident situation,
- The operating requirements of alarm signals associated with their uses in EOP's,
- The presentation of alarm signals in accident situations,
- The creation of indicators for re-orientating control action in accident situations.

4.3.1 Detection of an accident situation: « entry in symptom-oriented EOP's » alarm

The symptom-oriented EOP's are based on the actual state of the reactor and take into account the thermal-hydraulic changes in the process. A single point of entry in symptom-oriented EOP's guides the operators towards the orientation operating instruction for incident or accident situations, whatever the initiating event may be.

The «entry in symptom-oriented EOP's» alarm signal is a green alarm signal of severity 1 which leads the operators to apply the control action instruction for guidance in incident or accident situations (cf. § 4.3.4). It summarizes all the basic alarm signals which detect an incident or accident situation and calls upon, while it is working, processes for inhibition and for validation according to the situation.

4.3.1.1 Generation of the "Entry in Symptom-Oriented EOP's" Alarm Signal

Certain non-redundant information is used for the cold and intermediate shutdown states because it is associated with the decay heat removal system train in service. The IPSN analysis revealed that this absence of redundancy in generating situations was likely to lead to inappropriate inhibition of the "entry in symptom-oriented EOP's" alarm signal.

Consequently, EDF modified the alarm process in order that the "entry in symptom-oriented EOP's" alarm signal appear even if non redundant information fail. However, there is a risk that an alarm signal will appear outside of its validating situation context. The IPSN decided that this factor was satisfactory.

Following analysis by the IPSN, various modifications were made to the definition of the situation to make them as close as possible of the standard states specified in the Technical Specifications for Operation (cf. § 4.2.1).

The IPSN also considered that it would be appropriate for the operating organization to make sure there was no common mode between the information used to develop a classified alarm

signal and to develop the validating situation, as this common mode could result in the spurious appearance of an "entry in symptom-oriented EOP's" alarm signal.

4.3.1.2 Validation of the "Entry in Symptom-Oriented EOP's" Alarm Signal

Following discussions with the IPSN, and keeping in mind the complexity involved in developing the "entry in symptom-oriented EOP's" alarm signal, EDF validated this alarm signal in three complementary stages:

- **Validation of the individual alarm signals** which lead to entry into the state-oriented approach. This stage consists of exhaustively validating that the "KIC" is properly informed of each labeled "D" alarm signal. This stage was carried out in test programs on the plant. It is to be noted that the computerized alarm sheets which are associated with these alarm signals guide the operators towards entry in symptom-oriented EOP's even if the "entry in symptom-oriented EOP's" alarm signal is failed.

- **Validation of the development logic**. Different conditions were applied on entry into the logic process (appearance/disappearance of individual alarm signals, leaving a state-oriented approach, validating situations, situation invalidity etc.) and the proper behavior on leaving was checked.

- **Tests of each entire train at the plant**. This stage complements the previous stages and was carried out during hot tests (including blackout tests). These tests resulted in the creation of a new type of "entry in symptom-oriented EOP's" alarm signal which appears simultaneously on all the workstations.

4.3.2 Operating Requirements Associated with Alarms in Post-Accident Control Action

Taking into account post-accident control action in the safety studies at the design stage made it possible to establish the essential information, controls and alarm signals to be safety grade.

For the computerized operating interface, this classification only comes into play for the periodic test requirements, as the "KIC" computerized control system does not have the qualification requirements of a safety computer system.

As a complex computerized system as the « KIC » cannot be safety graded, the IPSN have required a set of provisions making it possible to ensure the system operates satisfactorily, these include:

- periodic tests where the "KIC" and the auxiliary panel are used to validate each other,
- creation of signs-of-life images for the "KIC" computerized operating interface, and
- creation of a diversified "KIC anomaly" alarm signal, located on the auxiliary panel.

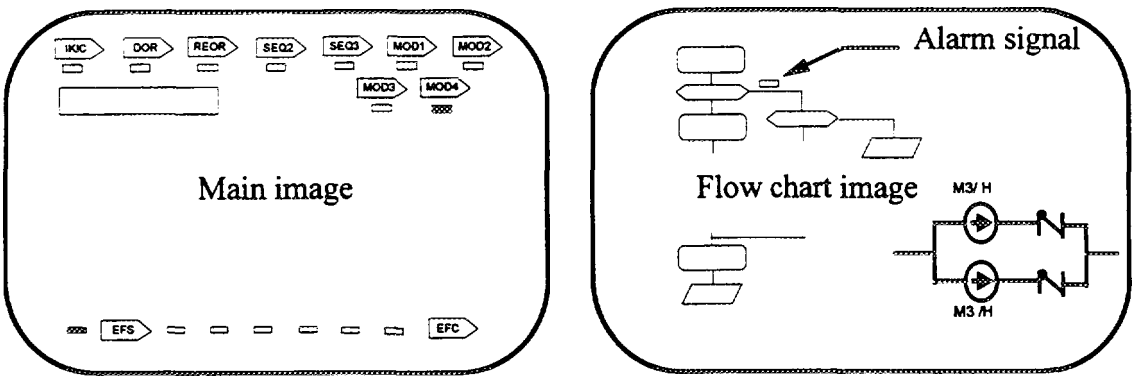
4.3.3 Presentation of Alarm Signals in Incident or Accident Situations

The incident instructions are completely computerized. The operators are thus able to carry out their instructions and give the corresponding orders directly from the flow chart images. The accident instructions are partially computerized. Orientations and re-orientations for control action are on flow chart image (see § 4.3.4.). For the other parts of the instructions, a main image guides the operator in his choice of control action sequences. There is also a paper copy of the control action sequence flow chart.

Other than for detecting an incident or accident situation (point covered in §4.3.1.), the alarm screens are no longer used during management of an incident or accident as the use of alarm sheets has been assigned to normal operation. The alarm signals required to respond to the computerized instruction tests are thus given on the flow chart images as and when necessary.

In case of a difference between the response to the instruction test given by the operator and the response calculated by the « KIC », the color of the test instruction changes and thus display an alarm signal to the operator.

The analysis revealed that in some cases the equations used in the computerized instruction tests were different from those used for their associated alarm signals. Thus EDF has checked all these equations to ensure a good correspondence between instruction tests and alarm signals.



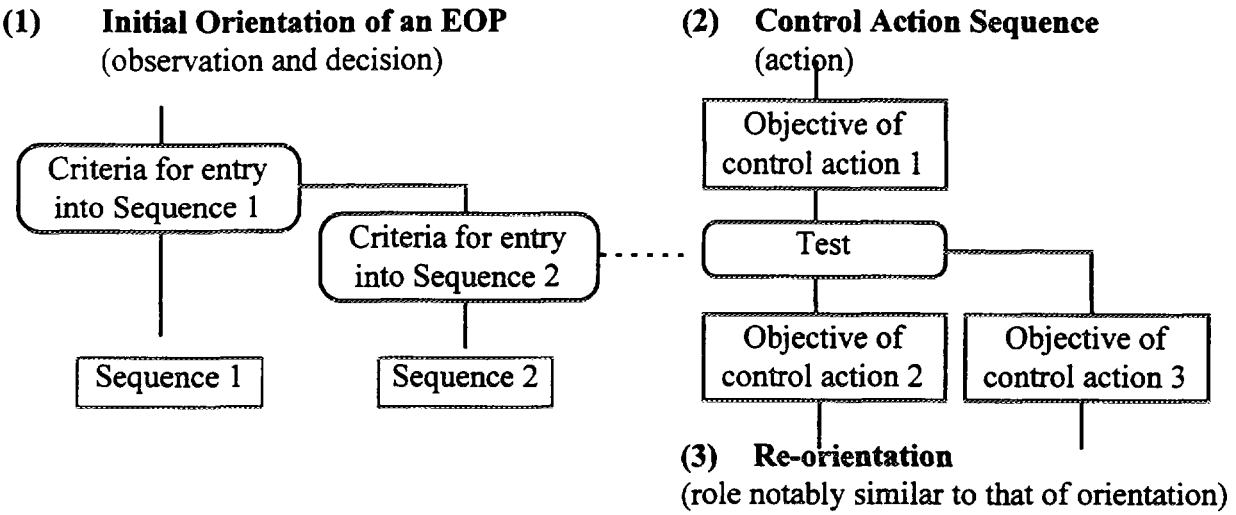
Different indicators available on the main control action image in incident or accident situations indicate to the operators, among other things, in order of importance:

- malfunctioning of one of the components (keyboard, screen etc.) of the workstation,
- malfunctioning of the control action computer system: IKIC indicator corresponding to the green IKIC alarm signal of severity 1 presented on the alarm screen,
- a necessary re-orientation of the control action in progress (DOR and REOR indicators),
- the loss of a support function of the systems important for safety (e.g. power supply), and
- the loss or malfunctioning of an important system (Containment Spray System, main system pumps etc.).

These indicators or alarm signals appear as the result of the calculation of complex equations which integrate a set of possibilities (combinations of information from different sensors, taking into account of invalidity, departure from the range, loss of power supply etc.).

4.3.4 Indicators for Re-Orienting Control Action in Incident or Accident Situations

The symptom-oriented EOP's for the unit make it possible to periodically diagnose the state of the unit, and can thus re-orient the operators. Each of the symptom-oriented EOP's which corresponds to a given state of the installation is itself divided up into sequences. On completing a part of the EOP being carried out, the operator moves to a re-orientation operating module between EOP's and then between sequences of the same EOP.



These re-orientations, totally computerized on the N4 series, control a re-orientation indicator (DOR or REOR indicator). To assess the validation of the computerized instructions, the IPSN analyzed the types of anomalies encountered (setting parameters, controlling, lack of information, representativeness of information, operating mode etc.) by detection means (checking by the development team and outsiders, computer checking tools, S3C simulator, plant tests etc.), in particular focusing its analysis on actual validation at the plants which constituted the last link in the validation chain.

Taking into account the discussions with the IPSN and in order to perfect the validation of these indicators, EDF will use a new tool simulating the behavior of an operator following the computerized EOP's «SCOOP», connected to an N4 process simulator.

4.4 Detection and Management of Faults in the Computer System

The development of a computerized control system as complex as that of a nuclear power station can not be guaranteed to be without software faults, both at the systems level and at the application level. The IPSN has checked the provisions which enable the anomalies at the development level to be reduced, in particular:

- quality assurance (development methodology, management of modifications etc.),
- validation (pertinence of tests, representativeness, experience feedback etc.).

It is therefore important to check that the computerized system is safe in the event of software or hardware failure (isolation of elements affected, reconfiguration, informing operators, alternative operation etc.). The analysis of potential malfunctions as well as of means of detection and managing a software or hardware breakdown in the computerized system have hallowed to assess the system's tolerance against failures and more generally, the safety of the installation.

From those analysis, new alarm signals relating to the different malfunctions of the "KIC" computerized control system appeared on the N4 series, in particular :

- alarm signals relating to the loss of a software or hardware component (or sub-component) of the instrumentation and control system,
- alarm signaling a fault in one of the workstation components (keyboard, screen etc.),
- IKIC alarm signal: malfunction affecting control actions on the "KIC", and
- creation of signs-of-life images for the "KIC" computerized operating interface.

New control provisions relating this system to cope with these different anomalies were introduced:

- periodic tests where the "KIC" and the auxiliary panel validate each other,
- sheets to cope with residual anomalies,
- reconfiguration of workstations (loss of alarm screen, keyboards etc.), and
- IKIC instruction which makes it possible to move the operating team if the workstation fail and if necessary to transfer the computerized control stations to the auxiliary panel.

Numerous tests on simulators and the analysis of malfunctions which occurred in the plant testing phase have made it possible to validate all of these provisions, which have partly stemmed from the results of the analysis made by the IPSN.

5. CONCLUSION

The analysis carried out by the IPSN of the alarm signals presented in a conventional 1300 MWe reactor control room showed the need to rank the alarm signals in accordance with their role in operating safety.

Regarding the N4 series, the main conclusions the IPSN can draw from its analysis are:

- The computerized processing of alarm signals provides considerable help in managing alarms during normal operation. In particular, better functional ranking of the alarm signals by introducing classification according to severity and the use of more selective display mechanisms, in theory should provide a noticeable improvement in the

processing of anomalies by the operators, which will however only be truly able to be gauged through experience feedback.

- The creation of a single alarm signal detecting the entry into incident or accident situations, and the creation of a control action re-orientation indicator which were made possible thanks to computerization and the use of symptom-oriented emergency operating procedures, provide a significant improvement in the management of incidents and accidents.

- Taking into account the importance of the computerized operating system «KIC» for the installation's safety, various provisions make it possible to cover any failure of the «KIC» particularly:

  - hardware redundancy and software self-tests of the «KIC» computerized system,
  - hardware and operating independence of the protection and safeguard system,
  - diversified announcement on the mimic in the event of a protection or safeguard order,
  - diversified "KIC anomaly" alarm signal located on the auxiliary panel,
  - human redundancy and acquisition of information provided by the safety engineer or the shift supervisor at the auxiliary panel in incident or accident situations.

  These provisions are stemming particularly from:

  - quality assurance at the design stages,
  - both ergonomic and technical validation very soon included in the design process,
  - considerable thoroughness in the analysis of potential malfunctions.

ADVANCED ALARM SYSTEM DESIGN AND HUMAN PERFORMANCE: GUIDANCE DEVELOPMENT AND CURRENT RESEARCH

John M. O'Hara
Brookhaven National Laboratory
Upton, New York

ABSTRACT

This paper describes a research program sponsored by the U.S. Nuclear Regulatory Commission to address the human factors engineering (HFE) aspects of nuclear power plant alarm systems. The overall objective of the program is to develop HFE review guidance for advanced alarm systems. Guidance has been developed based on a broad base of technical and research literature. As part of the development effort, aspects of alarm system design for which the technical basis was insufficient to support guidance development were identified and prioritized. Research is currently underway to address the highest priority topics: alarm processing and display characteristics.

1. INTRODUCTION

The need to improve the human factors engineering (HFE) of alarm systems has led to the development of advanced systems in which alarm data are processed beyond the traditional "one sensor - one alarm" framework. While this technology promises to provide a means of correcting many known alarm system deficiencies, there is also the potential to negatively impact operator performance [1]. In addition, there is general agreement that an "international lack of guidance and requirements for alarm systems exists" and new guidance for the review of advanced alarm system designs is needed [2].

This paper describes a research program sponsored by the U.S. Nuclear Regulatory Commission (NRC) to address the HFE aspects of nuclear power plant alarm systems. The objective of the study is develop HFE review guidance for advanced, computer-based alarm systems. As part of the development effort, aspects of alarm design for which the technical basis was insufficient to support guidance development were identified and research to address the most significant issues was initiated. The paper will report on the status of these guidance development and research efforts.

2. DEVELOPMENT OF ALARM SYSTEM REVIEW GUIDANCE

The basic guidance development methodology is illustrated in Figure 1. The methodology places a high priority on establishing the validity of the guidelines in a cost-effective manner. Validity is defined along two dimensions. "Internal" validity is the degree to which the individual guidelines are based upon an auditable research trail. "External" validity is the degree to which the guidelines are subjected to independent peer review. The peer review process is considered a good method of screening guidelines for conformance to accepted human engineering practices. These forms of validity can be inherited from the source documents that

form the technical basis for new guidance development or they can be established as part of the guidance development process itself. Primary source documents (see Figure 1) are those that already possess internal and external validity. However, existing primary source documents alone do not provide a sufficient basis on which to develop comprehensive advanced alarm system guidance, thus additional sources of information are necessary. For these sources, guidance validation has to be established.

Guidance development proceeds as shown in Figure 1. Primary source documents are considered first. Secondary source documents are those with either internal or external validity. While tertiary documents, such as HFE handbooks, provide good information for specific topics, they often do not possess internal or external validity. Guidelines are developed from tertiary documents with relatively little effort in comparison to the final three sources shown in Figure 1.

Basic literature and industry experience are used where guidelines cannot be obtained from the other sources. Results are evaluated from basic literature including articles from refereed technical journals, reports from research organizations, and papers from technical conferences. Industry experience is obtained from published surveys. It is a valuable information source for identifying performance issues and tested design solutions. Although information from industry experience may lack a rigorous experimental basis it does have the benefit of high relevance to the practical application of alarm systems within the nuclear setting.

In addition to alarm literature, guidance is also developed based upon the application of the high-level design review principles [3] to alarm system characteristics. These principles were developed based upon an assessment of the human-performance issues associated with advanced technology systems and on human-system interface (HSI) design and evaluation literature.

Using this guidance development method, draft alarm review guidance was developed based on all sources in the hierarchy of information listed in Figure 1 except the last category (original research). Original research is appropriate when the technical bases does not exist in the available literature or practice, or when additional experimentation is needed to provide supporting evidence. It has the advantage of being focused on specific issues of interest. Because these needs existed with regard to the introduction of advanced alarm systems in nuclear power plants, a program of original research was also deemed necessary. Such a program is currently underway and the guidance will be expanded when the results become available (See Section 3 below).

Each guideline contains the specific acceptance criteria to be used by the NRC reviewer and the source(s) of information upon which the guideline was established. The latter provides a basis for evaluating the internal validity of the individual guidelines. The technical bases vary for each guideline. Some guidelines are based on technical conclusions from a preponderance of empirical evidence, some on a consensus of existing standards and others on judgement that a guideline represents good practices based upon the information reviewed.

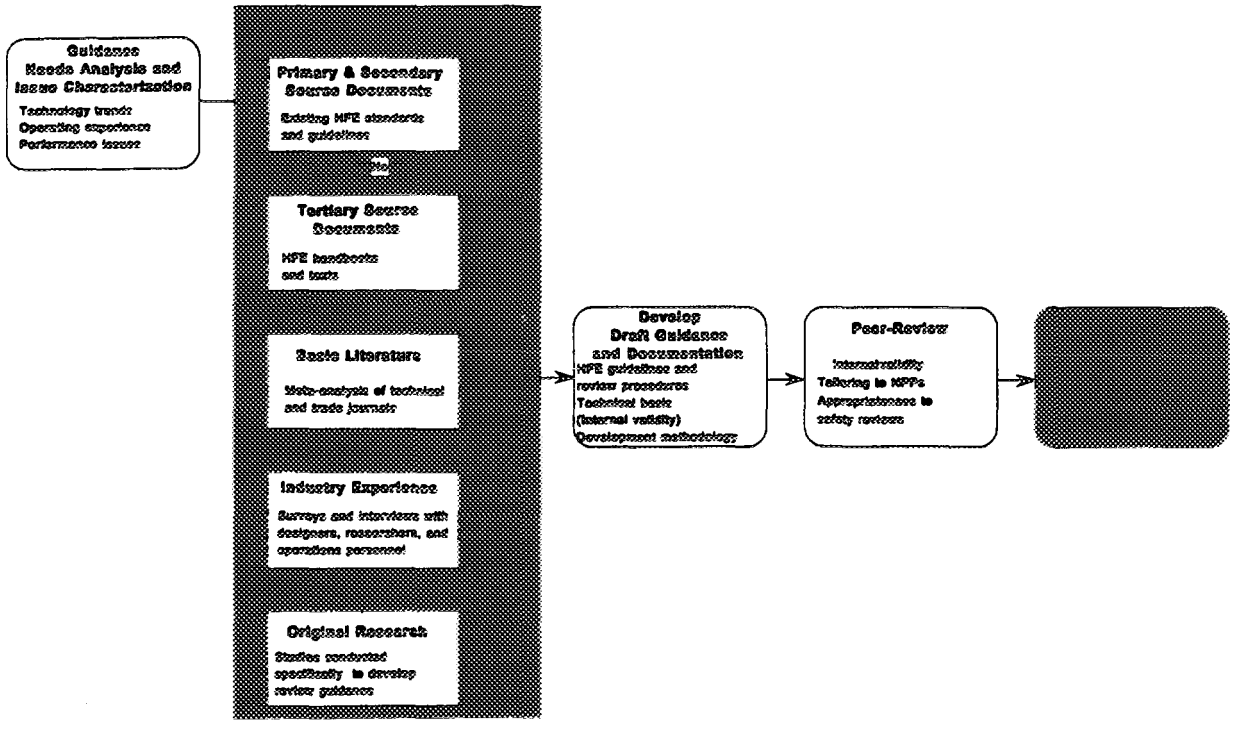


Figure 1. Guidance Development Methodology

The draft guidelines were then evaluated by several independent peer-reviewers who assessed: (1) the internal validity of the guidance, (2) the relevance of the guideline to the nuclear plant setting, and (3) the appropriateness of the guideline for NRC safety reviews. This peer review constitutes the external validation of the guidelines. A revision to the draft guidance based on the reviews was accomplished. The detailed guidance development methodology and technical basis is documented in NUREG/CR-6105 [3] and the guidance itself is integrated into NUREG-0700, Revision 1 [4].

2.1 Guideline Contents

The scope of the guidance includes both conventional and advanced alarm systems. The review guidelines are organized into the following ten sections:

General Guidelines - This section addresses the functional criteria for the alarm system and the general principles to which it should conform, such as consistency with the main control room HSI. Alarm system validation is also addressed.

Alarm Definition - This section addresses the selection of plant parameters and their setpoints.

Alarm Processing and Reduction - This section addresses the review of alarm processing, from simple processes such as signal validation to more complex alarm reduction processing strategies.

Alarm Prioritization and Availability - This section addresses alarm prioritization criteria and implementation, and alarm availability, i.e., the method by which the results of alarm processing are made available to the operating crew through filtering, suppression, and/or coded prioritization.

Display - This section addresses general alarm display guidelines, display of importance/urgency, display of alarm status, display of shared alarms, alarm message content and format, coding methods, and alarm organization.

Control - This section addresses controls including silence, acknowledge, and reset.

Automated, Dynamic, and Modifiable Characteristics - This section addresses the implementation of operator defined alarms and setpoints as well as other alarm features that may be modified.

Reliability, Test, Maintenance, and Failure Indication - This section addresses alarm system reliability to assure that (a) the alarm system provides alarm information to the operators in a reliable manner, (b) the crew can periodically test alarm functions and components, (c) the alarm system can be maintained with minimum interference to the operators' ability to receive and understand alarm messages, and (d) the system provides indication of alarm system failures.

Alarm Response Procedures - This section addresses the scope, content, and format of alarm response procedures (ARPs). In addition, operator access to ARPs is addressed.

Control-Display Integration and Layout - This section addresses the layout of control and display components, and their integration with other aspects of the HSI.

Individual guidelines are presented in a standardized format (see Figure 2). For many guidelines additional information (e.g., examples and clarifications) is provided to support use and interpretation of the review criterion. The additional information field may also contain a "discussion" regarding the technical basis and/or relevant research contributing to the guideline development. In such cases specific studies are cited that provide the supporting research. The discussions were removed from the additional information field when the alarm guidelines were incorporated into NUREG-0700, Revision 1.[4] Thus, when the guideline in Figure 2 was incorporated into NUREG-0700, the discussion section was deleted. It is available, however, in NUREG/CR-6105, which documents the technical basis to the alarm guidelines.

3. CURRENT RESEARCH

During guidance development, several human performance issues associated with advanced alarm systems were identified. They were organized into four topical areas: general issues, processing methods and related issues, display of alarm data, and alarm system controls. The issues were prioritized to determine which were most significant, using two dimensions: potential impact on operator performance and need for issue resolution to support near-term

NRC reviews. Estimates of each issue's impact on crew performance were obtained from the ratings of nine subject matter experts (SMEs) in nuclear plant systems, operations, and HFE. The SMEs rated (on three-point scales) the importance of the issues in terms of plant safety, human error, situation awareness, and operator workload. An evaluation of expected review needs was conducted to determine the near-term likelihood that the NRC staff would perform a review of an alarm system design incorporating features addressed by the issues. Based upon this analysis, those issues associated with alarm processing and display were given the highest priority. These issues are discussed in Section 3.1 below and the experiments currently underway to address them are discussed in Section 3.2.

4.2-3 Nuisance Alarm Avoidance
The determination of alarm setpoints should consider the trade-off between the timely alerting of an operator to off-normal conditions and the creation of nuisance alarms caused by establishing setpoints so close to the "normal" operating values that occasional excursions of no real consequence are to be expected..
ADDITIONAL INFORMATION: When determining setpoints, consideration should be given to the performance of the overall human-machine system (i.e., operator and alarm system acting together to detect process disturbances).
Discussion: Process control operators are in a monitoring environment that has been described in signal detection terms as an "alerted-monitor system" (Sorkin et al., 1985 and 1988). This is a two-stage monitoring system with an automated monitor and a human monitor. The automated monitor in a NPP is the alarm system which monitors the system to detect off-normal conditions. When a plant parameter exceeds the alarm criterion, the human monitor is alerted and must then detect, analyze, and interpret the signal as a false alarm or a true indication of a plant disturbance. Both the human and automated monitors have their own specific signal detection parameter values for sensitivity and response criterion. For the human monitor, both parameters are strongly affected by alarm system characteristics including set points, the presence of nuisance and false alarms, and alarm density. A significant issue associated with alerted-monitor systems is that optimal overall performance of the alerted-monitor system is a function of the interaction of both components. Optimizing the signal detection parameters for one component of the system may not optimize performance of the entire two-stage system. An alarm setpoint philosophy frequently employed is to attempt to optimize the detection of signals by the automated monitor subsystem. The response criterion is set to minimize missed signals. This, however, increases the false alarm rate, thus increasing the noise and lowering the operators' confidence in the alarm system. In addition, this guideline is consistent with the high-level design review principles of Cognitive Compatibility and Timeliness (see Appendix A).
SOURCE: NUREG-6105, NUREG-0700.

Figure 2. Example of an Alarm Guideline

3.1 Processing and Display Issues

3.1.1 Alarm Processing

3.1.1.1 Alarm Processing Characteristics

One of the most important objectives in the design of advanced alarm systems is to reduce the large number of alarms that typically occur during plant disturbances. Alarm processing is intended to accomplish this objective. The issues related to alarm processing fall into two general topics: alarm processing techniques and alarm availability.

Alarm signal and condition processing techniques were developed to support operators by reducing the number of alarms which may be encountered at one time, identifying which alarms are significant, and reducing the crew's need to infer plant conditions. Alarm signal processing refers to the method by which signals from plant sensors are automatically evaluated to determine whether any of monitored plant parameters have exceeded their setpoints and to determine whether any of these deviations represent true alarm conditions. Alarm signal processing includes techniques for analyzing normal signal drift and signal validation. Techniques for analyzing normal signal drift and noise signals are used to eliminate alarms that would occur because parameters momentarily exceed the setpoint limits. Signal validation is a group of techniques that compare signals from redundant or functionally related sensors to identify and eliminate false signals that may result from malfunctioning plant instrumentation such as a failed sensor. Alarm conditions that are not eliminated by the alarm signal processing may be evaluated further by alarm condition processing before they result in the presentation of alarm messages to the operator.

Alarm condition processing refers to the rules or algorithms that are used to determine the operational importance and relevance of alarm conditions. A wide variety of condition processing techniques have been developed and each affects the information provided to operators. For the purposes of this discussion, four classes of techniques are defined:

Nuisance Alarm Processing - These techniques essentially eliminate alarms that are irrelevant to the current mode of the plant. For example, a low temperature signal that is an alarm for a normal operating mode is irrelevant when it occurs during startup.

Redundant Alarm Processing - These techniques analyze alarms to determine which are less importance because they provide information that is redundant with other alarms. For example, in causal relationship processing only causes are alarmed and consequences are considered redundant. In addition to reducing the actual number of alarms, however, these processing methods may adversely affect the information used by the operator for confirmation that the situation represented by the "true" alarm has occurred, for situation assessment, and for decision-making.

Significance Processing - These techniques analyze alarms to determine which are less important in comparison to other alarms, e.g., in an anticipated transient without scram event, alarms

associated with minor disturbances on the secondary side may be less significant.

Alarm Generation Processing - These techniques analyze existing alarms and generate new alarms that (1) provide higher-level information, (2) indicate when "unexpected" alarms occur, and (3) indicate when "expected" alarms do not occur. These techniques present an interesting paradox. Generation features may help mitigate problems that reflect the overloaded operator's incomplete processing of information by directing their attention to conditions that are likely to be missed. However, since additional alarms are created, the issue of alarm overload may be exacerbated.

The impact of the various processing methods and the degree of alarm reduction should be evaluated for their relative effects on operator performance. An understanding of this relationship is essential to the development of alarm system improvements and review guidance. System complexity should also be considered. The operator, as the system supervisor, should easily comprehend alarm information, how it was processed, and the bounds and limitations of the system. An alarm system combining multiple processing methods may be so complex that it cannot be readily interpreted by operators in time-critical situations.

Alarm availability refers to the method by which the results of alarm processing are made available to the operating crew (rather than *how* they are presented, which is alarm display). Three techniques have been used: *filtering* (alarms determined by processing techniques to be less important, irrelevant, or otherwise unnecessary are eliminated and are not available to the operators); *suppression* (alarms determined by processing techniques to be less important, irrelevant, or otherwise unnecessary are suppressed and not presented to the operators, but can be accessed by operators upon request or by the alarm system based upon changing plant conditions); and *prioritization* (all alarms are presented to operators based on prioritization schemes).[1]

There are tradeoffs between these approaches; thus an issue remains about when the various options should be employed. Filtering reduces the possibility that unimportant alarms will distract operators; however, it may remove information used for other purposes. In addition, the designer must be certain that the processing method is adequately validated and will function appropriately in all plant conditions. Suppression also removes potentially distracting alarms; however, since they are accessible on auxiliary displays, additional workload may be imposed by requiring operator action to retrieve them. Prioritization does not conceal any information from operators. However, the operator must perceptually "filter" alarms, e.g., scan for red alarms, and thus, a potential exists for distraction from less important alarms.

3.1.1.2 Related Research

Several studies examined the effects of alarm processing techniques on operator performance.

---

[1]Note that the definitions of "filtering" and "suppression" are the author's; the terms are often used interchangeably in the literature.

The HALO (Handling Alarms with Logic) alarm system was developed by the Halden Reactor Project. In an initial study, inexperienced students were trained with the system and were asked to identify disturbances in a simulated pressurized water reactor [5]. Alarm information was presented as (1) unfiltered message lists, (2) filtered message lists, or (3) filtered message lists with an overview display. Alarm information was presented in static displays rather than dynamic simulation. Diagnosis time and accuracy were the primary dependent variables. The results indicated that accuracy was improved with filtering, but the benefit was transient specific. No significant difference was found for response times. Also no differences were observed between the filtered message list used alone and the filtered list used with the overview display.

Comparisons of performance using alarm systems with and without filtering during simulated transients were also made in subsequent studies [6-8]. The filtering system reduced the alarms by approximately 50 percent and the filtered alarms were not available to the operator. The performance measures included detection time/percentage and diagnosis time/percentage correct. Process variables and subjective evaluations were also measured. Seven two-operator crews used the three systems (listed above) in 12 simulated scenarios. Alarm filtering had little effect on performance. It was observed that the detection of events decreased from 81 percent to 51 percent when the event occurred late in a scenario rather than early in a scenario. None of the systems tested helped to mitigate the problem. One problem with interpreting the results of this study is that the display type and use of alarm filtering were experimentally confounded. Thus, no conclusions with respect to the *independent* effects of display mode or filtering can be made.

In another study using a verbal protocol analysis taken in real time from three operators during simulated malfunctions, no evidence was found that an alarm filtering system had a positive effect on their performance, although the operators expressed support for it.

In a test of the Dynamic Priorities Alarm System (DPAS), the number of high-priority alarms was reduced through mode, multi-setpoint, and cause-consequence processing [10-11]. Alarms were displayed on a combination of tiles and video display units (VDUs). Color was used to distinguish status and alarm information. Performance with and without the new system was compared. Nine crews of three experienced operators used the systems during simulated scenarios involving single and multiple failure events. Operator performance measures included time to identify initiating event, time to identify second malfunction, time to take control action, and alarm utilization frequency. No difference between the systems was found for initiating event identification; however, detection time for second malfunctions was significantly reduced in three of the four scenarios when the alarm handling system was available. DPAS significantly reduced the time required to take a control action in two of the four test scenarios. The finding that second malfunction detection time was reduced with the alarm system is not consistent with the findings from the HALO study reported earlier where secondary event detection was not enhanced.

The Electric Power Research Institute (EPRI) compared tile and VDU-based alarm presentations [12]. In one VDU condition the typical alarms associated with reactor and turbine trip were suppressed. The alarm suppression reduced by 50 percent the number of "maverick" alarms (those not typically occurring during a plant trip) operators missed. Operators expressed concern

about suppression of alarms because their timing helps them understand the event.

With respect to filtering, several studies have found that operators use the alarm system to obtain status information and that under some conditions, they prefer to have status alarm information presented to them rather than to have status information eliminated [13-16]. The issue of whether to include status indications in an alarm system is related to the criteria for alarm selection and the capabilities provided by other HSIs for displaying status indications.

3.1.1 Summary

Two studies failed to find an effect of alarm processing [7,9]. One study found no effect for the detection of initial disturbances, but improved detection performance during a secondary malfunction [11]. Another study found a positive effect on detection of unusual alarms, and questioned the trade-offs between information loss and situation assessment [12]. These differences could be due to many factors such as type of processing used, degree of filtering achieved, method of data display, and user familiarization with the system. The effects could also be transient dependent, e.g., dependent on the specific scenario, on the operator's ability to recognize familiar patterns, or on plant type. While the focus of most research has been on alarm reduction, alarm generation effects on performance have not been completely addressed. Also, individual alarm processing methods have not been compared to determine which methods best support operator performance.

A key issue is the type and degree of processing. While it is clear that processing techniques can reduce the number of alarms [17-18], their impact on operator performance is the most important effect of interest. An industry survey found that a typical filtering objective was to reduce the number of alarms by 50 percent [18]. However, that amount of filtering may not significantly improve operator performance [6-7]. In terms of operator information processing, it is probably inappropriate to specify alarm reduction in terms of numbers of alarms (a metric often used to assess alarm reduction schemes). Operator information processing demands are not necessarily a function of the absolute number of alarms, but rather their rate, their recognizability as familiar patterns, their predictability, and the complexity of the ongoing task. A goal for improved operator performance needs to be established. With respect to availability, the conditions under which alarms should be filtered, suppressed, or prioritized needs to be determined.

3.1.2 Alarm Display

3.1.2.1 Alarm Display Characteristics

The alarm systems in traditional U.S. nuclear power plants tend to be stand alone systems; that is, the alarm information is not integrated with other plant information. Operators consult other plant indicators for specific information. General trends in display design, however, are for increased integration of information. This trend has extended to alarm information for two principal reasons. First, computer-based information systems can access and present a very large quantity of data. However, the information is presented in a compact display space providing significantly less display area (contrast the display area available in a conventional and advanced

control room design). Because more information needs to be presented in less space, there is a need for greater integration and layering of information and for presentation of this information at higher levels (aggregates of lower level information). The second reason is that it is thought that the cognitive processing of information is supported by integration of information into a single object [19] or display [20]. Such displays are thought to enhance parallel processing (lowering cognitive workload), enable operators to better understand the relationships between display elements, and ultimately to develop a more rapid and accurate awareness of the situation.

Alarm displays can be considered as reflecting two dimensions: spatial dedication (whether an alarm is always displayed in the same physical location or in variable locations); and display permanence (whether an alarmed is always visible or visible only when in an alarmed state). These dimensions can be combined to produce a wide variety of alarm display formats, such as:

Spatially-Dedicated Continuously-Visible (SDCV) Alarm Displays - The presentation of alarms through lighted tiles is an example. Tile-like VDU displays have also been developed. The tiles do and the VDU may provide a display of information in a permanent location.

Temporary Alarm Displays - Many VDU alarm message lists are examples of a temporary alarm display. Messages only appear when the alarm is in a "valid" state. Depending on the design, temporary alarms may or may not appear in spatially dedicated locations.

Integrated Alarms - Alarm information can be presented as an integral part of other displays, such as process displays. For example, if alarms are built into a system mimic display, trouble with a component such as a pump can be depicted by a change in color or flashing of the pump icon. These displays may be in a fixed or variable location and are typically not permanent displays.

To serve the different functions of the alarm system, multiple display formats may be required. Thus the display format of alarm information in advanced systems and the degree to which that information is presented in separate or integrated fashion with other process information are important safety considerations. The role, relative benefits, and design of each type of alarm display format in the presentation of alarm information is an issue.

3.1.2.2 Related Research

EPRI investigated alarm system display characteristics incorporated into (1) alarm tile displays, (2) VDU displays, and (3) combined tile and VDU alarm display systems, (additional display characteristics were also evaluated) [12]. Fifteen licensed operators participated in the tests using an alarm system simulator. Performance measures included the speed and accuracy with which operators could extract information from the alarm system and operators' opinions on ease of use and other subjective parameters. The results indicated that the grouping of alarms by system and function improves performance (consistent with other finding) [21]. The tile display resulted in earlier, more rapid information acquisition. The VDU was best utilized as an adjunct to the alarm tile display to highlight alarms that were unusual for a given transient.

Similarly, in another study [22] experienced operators evaluated an advanced control room design and indicated that VDU alarm displays were sufficient when few alarms were presented but not during accident or transient conditions. As a result of this study, the control room design was modified to include both tile and VDU-based display formats.

In a study examining parallel versus sequential alarm presentation, three types of alarm displays were evaluated: (1) a tile display, (2) a VDU-based model similar to the tile display, and (3) a VDU-based sequential textual alarm presentation [13]. Chemical plant trainees served as participants in a laboratory study. Operator errors and difficulty ratings were the main dependent variables. The results indicated that the sequential presentation of alarms was inferior both in terms of operator performance and subjective ratings. The differences between presentation modes was greater during high alarm density conditions. The ability to recognize a pattern of alarms was offered as an explanation for the advantage of the parallel alarm presentation. In a survey of plants having both tile and VDU message alarm displays available, operators found the use of VDU alarms acceptable during normal power operations when the number of alarms is small, but preferred tile displays during plant disturbances when the number of alarms was large [15]. VDU alarm messages were difficult to manage during plant disturbances. In fact, the authors state that "there is clear evidence that VDU message lists are a poorer method of presenting alarms than the conventional annunciators." In the plants surveyed, while VDU-based displays were the primary method of alarm presentation, an increasing trend toward conventional alarm presentations was observed. More recently, VDU alarm message flooding (when many more alarm messages are coming in than can be presented on the VDU) has been identified as a problem in Canadian plants [16,25]. Operator problems with VDU-based message displays in high-density situations were noted in other field observations as well [26].

Operator preference for SDCV displays has been found in other NPP studies and chemical plants [27,12-13]. Wickens found increased memory load for temporary message displays and a loss of spatial organization of information which facilitates information processing [28]. One of the issues associated with VDU alarm displays relates to difficulties operators have with alarm message lists, especially in systems where the messages scroll across the screen. When the rate increased, the number of missed alarms increased [29]. This finding is, of course, dependent on the alarm display and types of message design implemented.

A major attraction of the VDU-based presentation is the flexibility to present alarm information in a wide variety of ways. Several studies have gone beyond message lists and examined graphics-based presentations. The Halden studies [6-7] discussed in the previous section compared: (1) an unfiltered text-based version of a tile-like alarm VDU display, (2) a filtered text-based alarm VDU display, and (3) a filtered text/symbolic-based alarm VDU display. In the latter condition, top-level schematic overviews of the plant were presented. When an alarm was activated, symbols representing the appropriate subsystems would blink. The operator could then move to a second-level display which was an enlarged schematic presented on a separate VDU. Flashing symbols indicated the problem system. Text-based alarm messages were provided. There were no significant differences between the three systems on measures of diagnosis, checks, and action, but detection time was faster with the textual presentation. While operators found the graphic displays helpful, navigating between the displays was slow and

cumbersome. In addition, operators requested that process data be included in the overview display. Again, however, display type and processing were confounded in this experiment.

In another study, operator performance with an advanced display system was compared with a tile-based display [24]. The advanced display system provided process data on an overview display and a "forced-to-look" feature which prompted the operator to examine new alarms. A blinking alarm on the overview could only be accepted by calling up the appropriate process format. Ten subjects (four operators and six project staff volunteers) took part in the study. The systems were compared under a variety of transient conditions. The results indicated that although the advanced alarm display provided better performance in the selection of process displays, there was no clear advantage of either system for detecting abnormal events or for locating a deviant parameter. It was concluded that the alarm system should be integrated into the information system.

3.1.2.3 Summary

In summary, even though SDCV displays are preferred by operators and may have a performance advantage under high-alarm conditions, placing all alarms on such displays (potentially many thousands of alarms in advanced plants) has been associated with operator overload. VDU-displays have not been completely successful alternatives, however. Message lists have been demonstrated to be problematic in high-alarm conditions and, although the research is limited, integrated graphic displays have not been shown to improve performance. These findings emphasize the importance of display design, i.e., poorly designed VDU displays can have safety concerns that need to be understood so as to provide a basis for the development of regulatory guidance. It is likely that both SDCV and message list alarms can play an important role in advanced systems but the allocation of alarm functions to each needs to be addressed.

3.2 Alarm System Experiments

In order to help resolve these issues an experiment is underway to evaluate the impact of alarm system design characteristics on plant and operator performance in order to contribute to the understanding of potential safety issues and to provide data to support the development of design review guidance. Three alarm system design factors are being evaluated: (1) processing methods, (2) availability of processing results, and (3) alarm display format.

As stated earlier, prior research has produced no consensus regarding the effects of processing methods on operator performance. While industry objectives for alarm reduction often focus on the number of alarms reduced, relating degree of reduction to the type of alarm information that is processed has not been accomplished. The degree of alarm reduction achieved is a function of the alarm processing techniques that are applied. For this study, a variety of alarm processing methods are employed that are representative of near-term applications, and therefore, near-term regulatory review considerations. Alarm reduction is accomplished using two methods: one that minimizes nuisance alarms to achieve moderate alarm reduction; and one that employs redundant processing to achieve maximum reduction. In addition, a baseline condition of no alarm processing is being used to provide a basis of comparison.

The differential effect of two types of alarm availability is being evaluated: suppression and dynamic prioritization. As indicated, there are clear tradeoffs between these approaches; thus an issue remains about which method should be used or in what contexts the various options should be exercised. Suppression provides the potential benefits of removing alarm from the operators attention thereby reducing the need to process and respond to them. There are two potential drawbacks. First, since designers cannot anticipate all possible plant disturbances it is possible that some of the alarms suppressed may be important to decision making in certain contexts. Second, since suppressed alarms are accessible on auxiliary displays, additional workload is imposed by requiring operator action to retrieve them. When dynamic prioritization alone is used to present the results of alarm processing no alarms are concealed from operators. Instead, alarms that would have been suppressed are presented as low priority alarms. However, the potential limitation to this approach is that operator's are required to perceptually "filter" alarms, e.g., to scan for the red alarms. Thus, there is a potential that the detection of higher priority alarm is impaired by the distracting presence of less important alarms.

Alarm display design has been shown to have significant effects on operator performance but further research into the integration of SDCV displays and the design of alternative VDU display formats is needed. Three types of VDU-based alarm displays are being compared: a dedicated "tile-like" format, a mixed tile and message list format, and a mixed graphic and message list format. The graphic provides alarm information integrated into process display formats. These display formats enable the examination of two aspects of alarm display design: spatial dedication and degree of integration with process information.

Eight alarm system configurations, representing combinations of these alarm characteristics, are being evaluated during simulated nuclear plant transients. The tests are being conducted at the Human-Machine Laboratory (HAMMLAB) at the Halden Reactor Project in Norway. The plant model simulates a pressurized water reactor power plant with two parallel feedwater trains, turbines and generators. It is closely related to the plant model used in the large scale training simulator at the Loviisa nuclear power station in Finland. The participants are professional nuclear power plant operators from Loviisa. Six crews of operators are participating with two operators per crew.

The measurement of performance in the study is based upon a supervisory control model in which modifications to the human system interface (in this case the alarm system) effect plant safety through a causal chain from the operator's cognitive processes, to operator task performance, and ultimately to system and plant performance. Data related to plant/system performance, operator task performance, and operator cognitive processes (e.g., situation awareness and workload) is being measured. The subjective opinion of the operators is also being obtained.

The data will be analyzed to determine the effects, if any, on crew performance of the following alarm system characteristics:

- spatial dedication
- alarm integration
- alarm reduction
- type of alarm reduction
- alarm suppression
- scenario complexity.

In addition, the analysis will examine whether alarm availability interacts with processing type.

4. CONCLUSIONS

There are two major conclusions from this research program to date. First, the nuclear and human factors communities have developed a significant database upon which HFE review guidance for advanced alarm systems was developed. Information supporting guidance development came not only from available guidance documents, but also from published reports of research and operational experience. Further, advanced alarm systems, particularly those utilizing computer-based interfaces share many HSI characteristics in common with the rest of the control room. Thus HFE principles associated with VDUs, graphics displays, dialog structures (such as menus and command language) and computer input devices (such as touch screens, keyboards, and trackballs) are applicable to alarm systems. Second, there remain notable human performance issues. Research is underway to address the issues associated with alarm processing and display.

ACKNOWLEDGEMENTS

This research is being sponsored by the U.S. Nuclear Regulatory Commission. The views presented in this paper represent those of the authors alone, and not necessarily those of the NRC.

REFERENCES

[1] J. O'Hara and W. Brown, "Advanced Alarm Systems and Human Performance,"BNL Report A3967-1-6/96, U.S. Nuclear Regulatory Commission, Washington, D.C. (1996).

[2] W. Kennedy, "Lessons Learned in Process Control From the Halden Reactor Project," *NUREG-1361*, U.S. Nuclear Regulatory Commission, Washington, D.C. (1989).

[3] J. O'Hara, W. Brown, J. Higgins, and W. Stubler, "Human Factors Engineering Guidelines for the Review of Advanced Alarm Systems," *NUREG/CR-6105*, U.S. Nuclear Regulatory Commission, Washington, D.C. (1994).

[4] J. O'Hara, W. Brown, W. Stubler, W., J. Wachtel. J., and J. Persensky, "Human-system interface design review guideline," *NUREG-0700, Rev. 1*, Washington, D.C.: U.S. Nuclear Regulatory Commission (1996).

[5] E. Marshall, "A Preliminary Evaluation of the HALO System for Handling Alarms," *HWR-83*, Halden Project, Norway (1982).

[6] S. Baker, E. Hollnagel, E. Marshall, and F. Owre, "An Experimental Comparison of Three Computer-Based Alarm Systems: Design, Procedure and Execution," *HWR-134*, Halden Reactor Project, Norway (1985).

[7] S. Baker, D. Gertman, E. Hollnagel, C. Holmstrom, E. Marshall, and F. Owre, "An Experimental Comparison of Three Computer-Based Alarm Systems: Results and Conclusions," *HWR-142*, Halden Reactor Project, Norway (1985).

[8] E. Marshall and F. Owne, "The Experimental Evaluation of an Advanced Alarm System," in *Advances in Human Factors in Nuclear Power Systems*, American Nuclear Society, LaGrange Park, Illinois (1986).

[9] Y. Fujita and T. Sanquist, "Operator Cognitive Processes Under Abnormal Plant Conditions with Conventional and Advanced Control Room Designs," in *1988 IEEE Fourth Conference on Human Factors*, Institute of Electronics and Electrical Engineers, New York, NY (1988).

[10] Y. Fujita, "Improved Annunciator System for Japanese PWRs: Functions and Evaluation," in *Man-Machine Interface in the Nuclear Industry*, International Atomic Energy Agency, Vienna, Austria (1988).

[11] Y. Fujita, "Improved Annunciator System for Japanese Pressurized-Water Reactors," *Nuclear Safety*, 30, 209-221 (1989).

[12] R. Fink, R. Williges, and J. O'Brien, "Appropriate Choice of Alarm System Technologies: EPRI Research," in *1992 IEEE Fifth Conference on Human Factors and Power Plants*, Institute of Electrical and Electronics Engineers, New York, NY (1992).

[13] H. Kragt and J. Bonton, "Evaluation of a Conventional Process-Alarm System in a Fertilizer Plant," in *IEEE Transactions on Systems, Man, and Cybernetics*, 13, 586-600 (1983).

[14] Y. Fujita and S. Kawanago, "An Improved Annunciator System for Japanese PWRs," in *Transactions of the American Nuclear Society, 54*, 191-192 (1987).

[15] MPR Associates, "Power Plant Alarm Systems: A Survey and Recommended Approach for Evaluating Improvements," *EPRI NP-4361*, Electric Power Research Institute, Palo Alto, California (1985).

[16] E. Sheehy, E. Davey, T. Fiegel, and K. Guo, "Usability Benchmark for CANDU Annunciation - Lessons Learned," in *Proceedings of the Topical Meeting on Nuclear*

Plant Instrumentation, Control, and Man-Machine Interface Technologies, American Nuclear Society, LaGrange Park, Illinois (1993).

[17] F. Cory, B. Ettinger, R. Fink, A. Zarechnak, and J. Ketchel, "Control Room Annunciator System Replacement Specification and Evaluation of Alarm Suppression and Diagnostic Schemes," in Proceedings of the Topical Meeting on Nuclear Plant Instrumentation, Control, and Man-Machine Interface Technologies, American Nuclear Society, Inc., LaGrange Park, Illinois (1993).

[18] D. Gertman, F. Owne, E. Marshall, and A. Verle, "Survey on Computerized Alarm and Annunciator Systems," *HWR-176*, Halden Project, Norway (1986).

[19] D. Kahneman and A. Triesman, "Changing Views of Attention and Automaticity," in R. Parasuraman and R. Davies (eds.) *Varieties of Attention*, Academic Press, New York, NY (1984).

[20] K. Bennett and J. Flach, "Graphical Displays: Implications for Divided Attention, Focused Attention, and Problem Solving," *Human Factors*, 34, 513-533 (1992).

[21] R. Fink, "A Procedure for Reviewing and Improving Power Plant Alarm Systems," *EPRI NP-3448*, Electric Power Research Institute, Palo Alto, CA (1984).

[22] K. Matsushita et al., "Improvement of PWR Control Room Design," in *Man-Machine Interface in the Nuclear Industry (Tokyo Conference Proceedings)*, International Atomic Energy Agency, Vienna, Austria (1988).

[23] H. Kragt, "A Comparative Simulation Study of Annunciator Systems," *Ergonomics*, 27, 927-945 (1984).

[24] C. Reiersen, E. Marshall, and S. Baker, "A Comparison of Operator Performance When Using Either an Advanced Computer-Based Alarm System or a Conventional Annunciator Panel," *HPR-331*, Halden Project, Norway (1987).

[25] R. Moore, J. Popovic, and J. Pauksens, "Alarm Annunciation in CANDU 3 Control Room Design," in *Proceedings of the Topical Meeting on Nuclear Plant Instrumentation, Control, and Man-Machine Interface Technologies*, American Nuclear Society, LaGrange Park, Illinois (1993).

[26] D. Corsberg, "Effectively Processing and Displaying Alarm Information," in *1988 IEEE Fourth Conference on Human Factors and Power Plants*, Institute of Electrical and Electronics Engineers, New York, NY (1988).

[27] W.L. Rankin, T.B. Rideout, T.J. Triggs, and K.R. Ames, "Computerized Annunciator Systems," *NUREG/CR-3987*, U.S. Nuclear Regulatory Commission, Washington, D.C. (1985).

[28] C. Wickens, "Attention," in Hancock, P. (ed.), *Human Factors Psychology*, Elsevier Science Publishers, New York, NY (1987).

[29] P. Hollywell and E. Marshall, "An Experiment to Support the Design of VDU-Based Alarm Lists for Power Plant Operators," in N. Stanton (ed.), *Human Factors in Alarm Design*, Taylor and Francis, Ltd., London, England (1994).

HUMAN FACTORS IN ANNUNCIATION SYSTEMS - RECOMMENDATIONS FOR A CANADIAN REGULATORY FRAMEWORK

J.D. Beattie, S. Rochford and K.J. Vicente
Humansystems Incorporated
Ontario, Canada

ABSTRACT

Under a contract with the Atomic Energy Control Board (AECB) of Canada, brief reviews were conducted of the annunciation systems in Canadian nuclear power plant control rooms; of regulatory practices in other countries and relevant international guidelines; and of the human factors literature related to annunciation systems. Based on these reviews, a framework is proposed for regulatory criteria which could be applied to new annunciation system designs.

1. INTRODUCTION

The work summarized in this paper was carried out under a brief contract with the Atomic Energy Control Board (AECB) of Canada (June to August, 1996). The outcome was a recommended framework for human factors regulatory criteria which could be applied to annunciation systems in nuclear power plant control rooms. We wish to stress that the recommendations do not necessarily represent the regulatory position of the AECB, which has yet to be formulated.

1.1 Overview of Tasks Conducted

The AECB is aware that there are a number of advantages as well as some serious limitations to the annunciation systems currently installed in Canadian plants. Since both the technology available and the understanding of human performance and cognitive capabilities and limitations in the area of annunciation have changed since these systems were designed, the next generation of annunciation systems is expected to be a substantial evolution from the existing ones.

To acquire a more thorough understanding of human factors (HF) issues pertinent to the design of annunciation systems, the AECB set four tasks to be conducted as part of this contract.

1.1.1 Assessment of Current Canadian Annunciation System(s)

Review and assess the advantages and limitations of the annunciation systems in Canadian nuclear power plant control rooms (CRs), considering both normal and upset situations.

1.1.2 Perform a Review of Licensing Practices in Other Countries

Review HF regulatory practices, with respect to annunciation, in other countries; identify the position of the IAEA in the area of HF and annunciation; and identify key HF guidelines or

standards which would apply to the regulatory assessment of a new Canadian annunciation system, including the adequacy of the R&D development process.

1.1.3 Global Literature Review of Developments in the HF of Annunciation

Perform a global literature review of research and development in the area of HF and annunciation in nuclear power; identify areas of significant development in the HF of annunciation; and document the HF cognitive and perceptual basis for these developments.

1.1.4 Develop a Proposed Set of HF Annunciation System Criteria

Based on the results of the reviews, develop criteria which could be used to assess whether any proposed annunciation system adequately supports CR operator cognitive processing for monitoring, trouble shooting and decision making in both normal and upset conditions.

2. REVIEW OF CANADIAN SYSTEMS

To assess the advantages and limitations of current Canadian annunciation systems, a brief review was conducted of the design and operation of the system in use at Ontario Hydro's Darlington NGS. This is the most recently commissioned station in Canada, but also has sufficient operating experience that the limitations of the annunciation system have been recognized.

2.1 Design Basis

CANDU annunciation systems have evolved from station to station, without radical or fundamental changes. Those changes which have been made have come about along with improvements in computer and human-machine interface technologies (e.g. better CRT displays, use of colour, greater historical storage and retrieval capacity, reducing the reliance on printed message records, etc.). There have been no thorough system or task analyses of operator needs. On the other hand, there have been numerous attempts to extract lessons from operational experience (as contained in a variety of reporting mechanisms as well as in feedback sought from operators themselves), and to try to address the major deficiencies. These efforts are invariably subject to the limits imposed by hardware, software, required engineering effort, and the limited understanding among designers of how operators perform tasks in various operating situations.

Changes at Darlington since initial commissioning have likewise been based primarily on feedback of experience with the system, and have been limited by practical and technological constraints. Attention has been paid, however, to trying to ensure that all operating situations (including post-event analysis, outage management, testing, and maintenance as well as fault and upset conditions) are considered when assessing where improvements are needed. The process of identifying and implementing improvements is an ongoing one, and includes participation by a human factors specialist at every stage.

2.2 Design

Overall, the annunciation system comprises a number of computer-driven CRT message displays, several arrays of back-lit windows (located on the top section of each control panel), accompanying audible tones, and a message storage and retrieval facility accessible through the operator's central console.

The CRT message displays are regarded as the primary component of the annunciation system, i.e. the most comprehensive source of annunciation information. There are currently approximately 4000 annunciation points on each of the four units. The back-lit windows constitute the set of annunciations judged to be the minimum necessary for safe operation should all the CRT message displays become unavailable. These tend to be the most important under most circumstances, so they also serve as a prominent and spatially distributed display of important annunciation events which supports and helps direct attention to the CRT annunciation message screens. Generally speaking, the location of back-lit windows is on the control panel for the corresponding system. There are approximately 300 windows on each Unit main control panel. The initiation of any window annunciation also generates a CRT annunciation message.

There are four message display CRTs in the top sections of the main control panels. Each CRT normally displays messages from a number of systems, most of them related to its panel location, so that there is at least a degree of spatial coding in the message display. The presentation of messages on each screen is chronological, with each new message appearing below the previous one, and overwriting from the top when the screen becomes full. A dashed white line always appears immediately below the most recent message; for a full screen, the newest message at any given time is the one immediately above the dashed white line, and the oldest is the one immediately below it.

Colour coding of alarm messages is by 3 Priority levels, coded as red, yellow, and cyan. When the condition generating a message returns to normal (RTN), the message is overwritten in green (or a new message is generated, if the original is no longer on the screen). There is a further category of messages, called status messages and coded as white, for which RTN does not apply:

Annunciation messages from the special safety systems (shutdown systems SDS1 and SDS2, and the emergency coolant injection system, or ECI) are treated somewhat differently. Only the major and group-level messages from these systems are passed to the main DCC-based annunciation message system (they appear with Reactor Regulating System messages, etc.). Detailed messages and less important messages must be accessed through the appropriate monitoring computer CRT on the SDS and ECI panels.

At the operator's console, an overall chronological display of all messages is available. It functions similarly to those already described. It also allows the display to be "frozen" and then searched back (and forward again, as desired) to earlier (overwritten) messages. There are a number of other annunciation utilities available as well; for example, summaries of active alarms, for display or printing, can be requested from a menu screen.

Some measures exist to reduce the potential number of messages which are generated in a major upset. There is a capability for suppression of all Priority 3 messages from the main panel CRTs during the first 2 minutes following a number of predefined events. These include such events as reactor trip, turbine-generator trip, ECI activation, and reactor setback and stepback. However, the operator can choose not to use this feature, and most apparently do so. They generally prefer to deal with the potential flood of messages , rather than take the (perceived) risk of suppressing a message which might be important in a particular circumstance. It is also possible, by activating a spring-return switch, to initiate a 2-minute Priority 3 suppression at any time; again, this is very rarely done.

There is also a basic conditioning capability. The triggering of any alarm message can be made dependent on whether certain plant conditions are satisfied. Up to 16 such conditioning points can be defined, but this capability has not been fully used.

Annunciation messages are not routinely printed. However, the operator can request, at any time, a printed page of the latest messages. There is also an automatic printout of messages following a major upset. Originally, this printout included the first two minutes following the triggering event; it has been altered to include some messages form before the triggering event, to serve as an aid in diagnosis.

2.3 Advantages

There are clear benefits from many of the annunciation system features described above, and several notable advantages compared to older, more "traditional" systems. Many of these are referred to in the preceding discussions; this section summarizes the most important ones.

The multiple annunciation screens provide a valuable degree of flexibility with respect to where messages are viewed, and they provide backups should one or more screens fail. They also increase the overall message display capacity of the system. Their spatial distribution on the main control panels (along with that of the window annunciators) provides useful immediate cues to the source of newly arriving messages, which can be especially helpful when they are arriving at high rates.

The colour-coded prioritization of CRT messages, even though it is not sensitive to different plant states, does help to focus attention on the most important messages.

The provision of annunciation information at the operator console as well as at the main panels facilitates operator monitoring from the console position (which also provides plant graphical displays), and the availability there of a range of utilities which support such functions as alarm summaries and historical retrieval are useful in many operating tasks. The retrieval functions also remove the dependence on the huge printed message logs generated at older plants.

The ability to condition messages by plant or system state, limited though it is, has the potential to reduce significant quantities of irrelevant messages in a variety of circumstances.

2.4 Limitations

Despite the advances, there are still many areas where the annunciation system has serious shortcomings, a fact which is well recognized at Darlington (and by the nuclear industry at large).

2.4.1 SDS Annunciation

Considerable dissatisfaction arises from the treatment of SDS messages, which can be very distracting in some circumstances. For example, during unit upsets or reactivity changes associated with fueling, many messages may be generated by the SDS computers. Because many of these are not sent directly to the DCCs, they initiate instead a general window annunciation, which must be repeatedly acknowledged. Most of these messages are not informative or helpful.

2.4.2 Message Quantity

The problem of too many messages potentially flooding the screens in a large upset persists, despite the attempts at improvements in this respect. Conditioning has not been used to its full potential, partly because of the difficulty and the level of effort this would require. Cycling alarms and nuisance alarms are still too numerous.

Part of the problem is that most operators are apparently uncomfortable with existing message reduction schemes (such as suppression of Priority 3 messages), preferring to deal with the additional quantity rather than missing a message which could be important in a particular situation, even though judged globally as minor.

2.4.3 Prioritization

In general, there is an awareness that a dynamic context-sensitive prioritization scheme, based on a larger number of major events and plant modes than are now used for suppression and conditioning, could greatly improve the usefulness of the annunciation system during a large upset.

2.4.4 Outage Management

During scheduled maintenance outages, which are often very high workload periods for operators, the annunciation system has not been tailored to support essential tasks such as heat sink surveillance. Moreover, as maintenance work and associated testing progress, the problem of nuisance alarms and cycling alarms can be severe; to avoid this with the current system would require a huge administrative overhead for jumpering, etc. A good conditioning scheme (i.e. one that accurately recognizes the shutdown state) could contribute greatly to solving this problem.

2.4.5 Window Annunciation

The desire for more prioritization applies to the window annunciation as well, where apart from the use of red windows for special safety system activation there are no distinctions.

2.4.6 Additional Information

There are still classes of information not currently accessible to operators which they believe would be helpful. They have also suggested that there should be more states associated with some points, rather than just single alarm limits (for example, greater use of "margin" alarms).

2.4.7 Additional Functions

Another area where operators see a need for annunciation system improvements is in the support it provides for post-event analysis, reporting, review with supervisors, etc.

The engineers responsible for configuration management of the annunciation system see a need for more online utilities for managing and verifying major updates.

3. REVIEW OF LICENSING PRACTICES IN OTHER COUNTRIES

3.1 France and the UK

In France and the UK, regulation is non-prescriptive, and is based on assessments of licensee submissions against internal assessment guides, position statements, and/or general principles, rather than formal published standards or requirements.

In the UK, the process involves a dialogue with the licensee which continues until all issues have been resolved. Areas of interest include the structure and presentation format of the message displays, alarm reduction techniques, training and instructions required for operators, and even very basic questions such as the scrolling of existing messages when new messages arrive (which was actually an issue at Sizewell B, for example).

3.2 International Atomic Energy Agency (IAEA) and International Electrotechnical Commission (IEC) Contributions

HF-related documents published by the International Atomic Energy Agency (IAEA) include a number of technical reports and the proceedings from numerous conferences and specialists' meetings. They do not have direct regulatory force, but many relate to current topics in HMI design, including annunciation systems.

The International Electrotechnical Commission (IEC) has published a high level standard on nuclear plant control room design [1] which contains a short section on design objectives for annunciation systems, and presents a systems-based view of HF in control room design.

3.3 United States Nuclear Regulatory Commission (USNRC) Policies

The United States Nuclear Regulatory Commission (USNRC) takes a more prescriptive approach to regulation, and publishes substantial amounts of technical documentation (as NUREGs). However, annunciation systems are not categorized as safety-critical systems, and thus do not receive the same level of regulatory attention as other plant systems that do have such a classification. There is also an important distinction to be made between guidance

(recommended practice) and regulation (mandatory requirements). For example, NUREG-0700 [2], which provides a variety of HF guidelines for traditional CRs, is a guidance document; whereas the installation of a Safety Parameter Display System (SPDS) is an example of a regulatory requirement. As far as we know, annunciation systems specifically are not subject to any mandatory regulation.

Under US Code of Federal Regulations 50-59, any proposed design change must be evaluated by the utility against its standard safety analysis report (SSAR). If this evaluation reveals no unresolved safety questions, the utility is allowed to introduce the proposed change without first obtaining USNRC approval. Because of utilities' lack of awareness of the potential impact of control design changes on system safety, and because alarm systems are not classed as safety-critical, it is not uncommon for a CR design change that is significant from a HF point of view to be implemented by the utility without first obtaining USNRC approval.

3.3.1 Older Guidance Documents

There are two older guidance documents that have traditionally been used by the USNRC to review and evaluate CR designs, including annunciation systems:

- The original version of NUREG-0700 [2] contains some guidance that is pertinent to the design of annunciation systems and to other CR design issues as well. Because it only addresses HF issues associated with traditional technology (e.g. analogue, hard-wired instrumentation), it is of very limited value in reviewing advanced control rooms (ACRs) or CR upgrades based on computer technology.

- Chapter 18 of NUREG-0800 [3] provides a standard review plan for HF issues that the USNRC can use to conduct a review of regulation issues, such as SPDS and Control Room Design Reviews (CRDR). It suffers from the same limitations as NUREG-0700.

In an effort to update this guidance, the USNRC contracted Brookhaven National Laboratories (BNL) to conduct a number of studies.

3.3.2 Newer Guidance Documents

There are 4 documents that have recently been written by BNL for the USNRC that are very pertinent to the HF of annunciation systems:

a) NUREG-0711, "Human Factors Engineering Program Review Model".

b) NUREG/CR-5908, "Advanced Human-System Interface Design Review Guideline".

c) NUREG/CR-6105, "Human Factors Engineering Guidance for the Review of Advanced Alarm Systems".

d) NUREG-0700, Revision 1, "Human-System Interface Design Review Guideline".

NUREG-0711 [4] is perhaps the most important contribution of all, describing a HF program review model (PRM). The PRM is based on the belief that it is necessary to review the design process in addition to the usual process of reviewing the final design product. Consequently, the PRM provides a set of process criteria that can be used to evaluate the process by which a design is developed, and in particular, the way in which HF issues have been incorporated into the design life cycle. The criteria set out in this document are very broad, being based on a systems approach to HF design.

Another relevant document is NUREG/CR-5908, whose purpose is to compile together the available HF guidance that is pertinent to computer-based interfaces, thereby addressing the limitations associated with NUREG-0700. Volume 1 [5] provides a detailed discussion of the gaps in the available guidance for evaluating ACRs and retrofits based on computer-based technology and proposes a methodology for addressing those gaps. Volume 2 [6] describes the guidelines that were compiled using the methodology described in Volume 1. In addition, a set of procedures for using these guidelines to conduct ACR design reviews is also described. These procedures are integrated with the global design process specified by the PRM in NUREG-0711.

NUREG/CR-6105 [7] documents the results of a project specifically geared towards the development of guidance to support the USNRC review of advanced alarm systems. It describes the methodology that was used to develop the alarm guidelines, presents the guidelines themselves, and provides a procedure for the review of an alarm system.

Finally, NUREG-0700 (Rev. 1) [8], currently in draft form, is intended to take the place of the original NUREG-0700 by incorporating the latest research findings that are relevant to the design of ACRs based on computer technology as well as guidelines that are most pertinent to traditional CRs. NUREG-0700 (Rev. 1) is best viewed as an integration document that incorporates the results of all of the newer documents that have been described in this subsection. The document consists of two parts. Part 1 provides a set of criteria that the USNRC can use to evaluate an applicant's own Human-System Interface design review process. Part 2 of NUREG-0700 (Rev. 1) contains a set of detailed HF guidelines that can be used to evaluate both advanced and conventional CRs. Section 4 contains alarm review guidelines (taken from NUREG/CR-6105).

While the work conducted by O'Hara and colleagues is very impressive in scope as well as depth, it is inherently limited by the state of knowledge of the field. More bluntly, it is difficult to develop guidelines for questions whose answers simply are not yet known. Particularly with the topic of alarm systems, the state of knowledge is such that the research findings available are meager with respect to the broad range of questions that designers face. Thus, even the new version of NUREG-0700 (Rev. 1) does not provide a great deal of guidance for the design of advanced alarm systems, primarily because many important issues remain to be investigated.

3.3.3 Future Work

The USNRC and BNL have developed a research plan to answer some of these outstanding questions [9]. Three experiments on alarm systems are to be conducted at the OECD Halden

Reactor Project in Norway. Experiment 1 will evaluate the effect of display type on human performance, independently of any alarm processing techniques. Experiment 2 will evaluate the impact of alarm processing techniques on human performance. In particular, the effect of alarm reduction techniques and differential availability of alarm processing results will be investigated. Finally, Experiment 3 is designed to evaluate the impact of alarm generation (i.e., higher-order alarms derived from lower-level alarms) on human performance. All experiments will include scenarios that are well-defined by procedures (rule-based scenarios) and those for which procedures are not readily available (knowledge-based scenarios). The current estimate is for these experiments to start in the fall of 1996. Regardless of the specific outcomes obtained, these experiments will represent an important contribution to the current impoverished level of understanding of the impact of advanced alarm systems on human performance in nuclear power plants.

4. LITERATURE REVIEW: HUMAN FACTORS OF ANNUNCIATION

4.1 Scope

This section presents the results of a literature review of HF issues in the design of annunciation systems for nuclear power plants. The time available was greatly constrained and the review was thus limited in scope; however we have attempted to present the most significant techniques and findings pertinent to the design of advanced annunciation systems for nuclear power plants.

4.2 Purpose: What is the Role of an Annunciation System?

A possible measure of the maturity of research in this area is whether there is an agreement in the literature as to the purpose of an alarm system. We have found that it is useful to distinguish between the *designed* purposes that an annunciation system is intended to fulfill by designers, and the *operational* purposes that it actually fulfills for operators, in practice.

4.2.1 Designed Purpose

There is a surprising lack of consensus among designers as to what role an annunciation system should be designed to serve in a CR. We found a considerable variety of definitions in papers [10 -16]. While there is certainly some common ground across the various definitions, there are also significant differences as well. Some of the important areas of disagreement include:

- Does the alarm system include normal status, as well as off-normal occurrences?
- Does it include expected as well as unexpected indications?
- Does it, by itself, explicitly support decision making and response planning activities?

Some researchers have even suggested that the alarm system should also be responsible for diagnosing the state of the plant, and in some cases even response planning, thereby integrating fault detection with fault diagnosis and compensation into a single automated system. This

viewpoint was prevalent in the Disturbance Analysis System (DAS) work conducted in the 1980s (see [17 - 19] for reviews).

The problem seems to be that the label "alarm system" is used in such a way that it confounds a number of different characteristics that are, in principle at least, conceptually independent. It is important to untangle these characteristics so that the full range of design possibilities is clearly revealed.

4.2.2 Operational Purposes

There are relatively few well-documented field studies investigating how NPP operators actually use alarm systems. A recent exception is the work by Vicente and Burns [20, 21] which documents the strategies that operators at Pickering B use to monitor the state of the plant. Although this study was not focused exclusively on alarms, the results show that the alarm system plays a very prominent role in operator cognitive monitoring. Interestingly, many of the results obtained by Vicente and Burns [20, 21] are consistent with a field study conducted years earlier by Kragt and Bonten [22] in a fertilizer plant, which was specifically focused on operators' use of a conventional alarm system.

Both of these studies reveal that the alarm system plays a very important, multi-faceted role in helping operators monitor plant status. Instead of continuously monitoring the plant via a large number of instruments, operators frequently rely on the alarm system to bring their attention to goal-relevant events in ways that were not anticipated by designers. Moreover, the alarm system is used for a myriad of purposes that have nothing to do with alarms, in the sense of an abnormal event. Kragt and Bonten [22] summarize this by stating that the alarm system was used primarily "as a monitoring tool and not as an alarm system requiring action" (p. 586). Because many of these uses were not intended and not systematically supported, this may compromise the alarm function of the system.

These operational purposes are very important because they differ considerably from most, if not all, of the definitions of the designed purposes of alarm systems described in the previous subsection.

Several preliminary conclusions can be drawn as a result. First, alarm systems are used for purposes that were not anticipated by designers and that the alarm system was not designed to support. Second, alarm systems are used for many purposes that are not associated with off-normal events. In fact, one of their primary operational purposes is to monitor the plant during normal operation, to help operators update their situation awareness of the plant [23]. (It should be noted, that both of these studies observed the usage of alarms over short periods, and thus the results obtained are more pertinent to the day-to-day usage of an alarm system rather than the usage during serious plant failures.)

4.2.3 Critical Analysis

The preceding subsections have argued that there is a lack of consensus in the literature as to what the designed purposes of an alarm system should be, and that the operational purposes for which alarm systems are actually used in practice go well beyond their designed purposes.

To explain these conflicting findings, one important distinction is that the role of an alarm system can differ as a function of the technology upon which it is based [10]. The purposes of an alarm system in a retrofit of a traditional CR will differ from those of an ACR. It is important to specify the type of context a particular design is intended for, and to design the purposes accordingly. The entire CR interface should be viewed as an integrated system for normal operation management, fault management, and outage management. The annunciation system is only one of the constituent subsystems of the overall system. Taking this approach allows one to recognize that other (possibly novel) subsystems can better serve some functions previously served by traditional annunciation systems.

Another factor is that different interfaces will be required to support operators under normal operations than under abnormal operations. Systems for the former mode are monitoring tools, not alarm systems (in the sense of detecting plant accidents). The characteristics of these interfaces will need to be different, although both can rely on the auditory modality.

Experience has shown that fault diagnosis should not be automated as part of an advanced alarm system. Instead, it is more prudent to limit the role of an alarm system to that of an information provider to a human operator who is responsible for making decisions with respect to fault diagnosis.

4.3 Alarm State Definition

A very basic question which apparently has not received a great deal of attention in the literature is what criteria should be used to define an alarm state. Traditional alarm systems have been based primarily on the single-sensor-single-alarm philosophy and alarms are often a very heterogeneous set of plant states, including: passage doors being open; actuation of automatic safety systems; individual parameters going out of their nominal range; and, large-scale accidents. The criteria for defining alarm states have largely been based on designers' intuitive notions of what states or events are important. There is very little discussion in the literature of how alarm states have been, or should be, defined.

The exception to this relative silence in the literature is the functional approach to alarm definition outlined by Goodstein [24], based on the abstraction hierarchy framework developed by Rasmussen [25]. Rather than just defining context-free limits on individual parameters, as the single-sensor-single-alarm approach does, the functional approach to alarming provides alarms at higher levels of abstraction by integrating lower level data in a functional manner. The result is a systematic approach to defining alarm states, and this approach has a number of other advantages as well.

As far as we know, these ideas have not been empirically evaluated in any rigorous way on a representative scale. Nevertheless, this approach seems to have influenced the design of several advanced alarm systems.

4.4 Alarm Processing Techniques

A number of advanced alarm techniques have been developed in response to the deficiencies of traditional alarm systems. One of the simplest is the use of lowpass filtering to eliminate the alarm "chattering" caused by a parameter oscillating in and out of its nominal operating range. Another is logical filtering, based on plant mode or other type of logic which can provide a form of context-sensitivity for alarm processing.

A third potential technique for alarm processing is the automatic prioritization of alarms. Alarms could be prioritized according to their threat to safety, and/or according to the available time for operator response.

A fourth alarm processing technique that has been proposed is derivation of higher-order alarms from lower-level signals or alarms.

Unfortunately, very few experiments have been conducted to evaluate these methods (at least under representative conditions), so the evidence available to demonstrate improved operator performance is quite meager. Based on what has been done, the only positive conclusions we can draw are that alarm prioritization can improve performance, and that model-based derivation of alarms seems to be a promising technique. Perhaps surprisingly, there is no evidence to indicate that alarm filtering improves operator performance. This does not mean that filtering may not be useful, but rather that it has not been shown to be so to date.

4.5 Alarm Presentation Techniques

Various issues concerning the presentation of alarm information have been addressed in the literature.

Some authors, most notably Gaver [26], have suggested that the auditory channel can be used much more than it has been. Instead of just presenting a sound that indicates that something is wrong, more complex auditory stimuli can be developed to provide more information about the nature of the problem, and perhaps even where to look to get more detailed information for diagnosis and compensation.

Another issue is whether lower priority or filtered alarms should be completely suppressed (and therefore not available to operators), or whether those alarms should be made accessible to operators but in a less salient manner.

A third issue is the desirability of integrating alarm information with process displays. This is made possible in a number of ways by the use of computer technology.

Another presentation technique that is intended to improve the informativeness of alarm systems is to organize alarms by function or system or task.

Finally, there is the issue of whether alarm information should be presented in a parallel, spatially dedicated fashion that is continuously visible or in a more serial fashion that may or may not be spatially dedicated or continuously visible [27]. The potential advantages of the parallel approach are that operators can get an overview at a glance, can diagnose faults through pattern recognition, and know where to find any particular alarm (because it is always in the same place). The potential advantages of the serial approach are that it is more flexible so that alarms can be integrated with process displays, and grouped in various ways according to context (e.g., the task being performed). Of course, hybrid systems are also possible.

As was the case with alarm processing techniques, very few empirical studies have been conducted to assess the value of these techniques. The limited evidence available suggests the following conclusions:

- the possibility of using rich auditory information in alarms should be explored
- complete suppression of alarms that are not of highest priority is inadvisable
- the results on integration of alarms and process displays are equivocal, although future work in this area is warranted since information retrieval performance may be enhanced through integration
- alarms should be organized according to function or system
- alarms systems should include a parallel, spatially dedicated presentation format to support interpretation at a glance and maintenance of an overview of plant state.

Note that it is possible (probably desirable) to combine a parallel, spatially dedicated presentation format and integration of alarms with process displays into a single design.

4.6 New Advanced Alarm System Developments

A number of vendors worldwide have developed, or are in the process of developing, new alarm systems that incorporate one or more of the advanced alarm techniques described earlier. The most obvious trend is towards integration of the alarm system with the remainder of the CR interface (e.g., overview panel displays, individual process displays). This integration is made possible by the move away from analog, hard-wired technology to digital, computer-based technology. It is important to note, however, that almost all of these new designs are hybrids in the sense that they consist of both traditional and advanced presentation media. Traditional tiles are usually used to provide an overview, whereas process displays and message lists on CRTs are used to provide more detailed information, thereby creating a hierarchical structure for the presentation of information. Another trend is towards the incorporation of advanced alarm processing techniques (e.g., filtering, prioritization), despite the fact that the value of these techniques has yet to be clearly established empirically (see above). Although all of these

systems are labeled "advanced", as far as we know, only one of them (the Mitsubishi design) has been empirically evaluated in a rigorous, representative manner with professional operators interacting with a full-scope simulator under a variety of challenging scenarios [28]. This is an important observation given the lack of industry experience with this type of technology.

5. FRAMEWORK FOR HF ANNUNCIATION SYSTEM CRITERIA

This section proposes a framework describing a set of criteria by which to evaluate the HF issues associated with annunciation system design. There are two qualitatively different types of criteria that can be adopted for any evaluation, *product criteria* and *process criteria*. Product criteria evaluate the outcome or final product, in this case the characteristics of the alarm system being proposed. Process criteria, on the other hand, evaluate the process by which the final product was obtained, in this case the information that was used and the decisions that were made in designing the alarm system being proposed. Although both are important, the criteria outlined below put a greater emphasis on process criteria than on product criteria. In fact, there seems to be a trend in this direction in the nuclear industry [29, 4]. There are several reasons why we adopted this approach:

- answers are not available for many important design questions pertaining to alarm systems
- there is very little operational experience on which to assess specific design features
- there are many different potential design concepts and techniques, making it difficult to come up with a common set of product criteria
- there are different types of contexts for which one may want to design an alarm system (e.g., retrofit, ACR, etc.)
- process criteria by which a design proposal can be evaluated can also serve to evaluate the R&D process
- the most efficient and reliable way of improving the HF issues associated with a particular design is to follow a design process that requires HF engineers to be involved early in the design life-cycle
- checklist or guideline product criteria are relatively shallow ways of evaluating a design proposal with respect to human performance and system safety

For all of these reasons, we decided to propose a set of criteria, outlined in the following sections, that emphasize evaluation of the design process but that also include evaluation of the final design product.

5.1 Relationship to Control Room Human-Machine Interface

An important general criterion is the extent to which the design of an annunciation system recognizes, is consistent with, and is integrated within the overall control room human-machine interface (HMI), of which it forms a part.

5.2 Design Basis

The annunciation system design process should take a systems approach, incorporating appropriately the recognized elements of human factors in systems design, as described in a number of industry documents (including, for example, [29, 8, and 1]). This implies an iterative process, whereby new concepts can be tested and modified as necessary before they are regarded as final. The use of mock-ups, prototypes, and simulations are among the mechanisms available to support this iteration.

Among the most important elements are:

- Definition of annunciation, and identification of the role and specific functions of the annunciation system
- System analysis and function allocation or assessment
- Task analysis of operator's use of annunciation
- Identification of limitations and strengths of existing or earlier systems
- Identification of constraints imposed by past experience and current developments
- Use of relevant guidelines, standards
- Recognition of impact on operator selection and training, staffing levels
- 'Feed-forward' to training and procedure development
- Verification and validation programs

5.3 Measurability of Overall System Performance

It is essential that evidence be collected to compare the performance with the proposed design with that obtained with more traditional annunciation systems. In some situations (e.g., replacement of an obsolete system), it may be sufficient to demonstrate that the new design does not lead a lower level of performance than the existing design. In other situations (e.g., ACRs), it may be more appropriate to require evidence indicating that the new design leads to a measurable improvement in performance compared to existing systems. In any case, the evaluation program should culminate with a dynamic evaluation in a full-scope simulator with a full CR (not just the alarm system) and professional operators [4]. Furthermore, the final evaluation should include

both rule-based and knowledge-based scenarios [9], and multiple faults which require operators to detect and track a subsequent fault, while they are still managing the initial fault.

A converging approach to measurement should be adopted, since any single measure or class of measures has limitations associated with it. In particular, measures should be selected for plant behaviour, alarm system behaviour, and operator behaviour.

5.4 Comprehensiveness of Applications

In evaluating a proposed alarm system, one should look for evidence to indicate how the design is explicitly tailored to the following modes:

- normal operation, includes normal transitions, and minor, anticipated failures
- maintenance and testing
- outage management, including shutdown and startup
- abnormal operations, ranging from process upsets to major accidents, including accidents which are unanticipated by designers and thus for which existing procedures do not readily apply.

5.5 Application of Sound Human-Machine Interface (HMI) Data and Design Principles

There are numerous published guidelines regarding the application of human factors data and design principles to HMI design. They are based on existing knowledge of human capabilities and limitations, as these pertain to annunciation system design.

These should be used in the context of overall human factors programs, by design teams which include suitable human factors expertise, so that their guidance can be used in accordance with the specific needs of individual projects.

5.6 Implementation as Proposed and as Designed

Annunciation systems should be implemented as proposed and as designed, and in the context (e.g. new plant or retrofit) intended, to ensure that the assumptions, analyses, etc. are valid.

5.7 Recognition of the Importance of Day-to-Day Evolution and Variation in Specific States of Components and Systems, and in Temporary Operating Practices

Finally, it is important that a proposed design take into account, and explicitly support operators in, the imperfect situations that will be encountered in a real plant, rather than the sanitized conditions usually found in a simulator. A real plant is an open system that is subject to unanticipated disturbances on different time scales [20]. On a day-to-day basis, certain components may not be in service or not working properly. On a longer time-scale, the operating

practices may evolve as the plant gets older. These disturbances have critical implications for performance and safety.

6. ACKNOWLEDGEMENTS

The authors would like to thank Suzanne Rochford, contract monitor, for her help with this project. Thanks also to Franck Bigot (IPSN), Eric Davey (AECL CRL), Mark Feher (AECL CRL), Felicity Harrison (AECB), Lawrence Lupton (AECL CRL), Jane Naisbitt (AECB Library), John Pauksens (AECL CANDU), and Craig Reiersen (NII) for their contributions and assistance. Special thanks are due to Debbie Scott-Gillard (Darlington NGS) and to John O'Hara (BNL).

REFERENCES

[1] IEC (1989). Design for control rooms of nuclear power plants (International Standard IEC 964). Geneva: International Electrotechnical Commission.

[2] USNRC (1981). Guidelines for CR design reviews (NUREG-0700). Washington, DC: USNRC.

[3] USNRC (1984). Standard review plan (NUREG-0800, Rev. 1). Washington, DC: USNRC.

[4] USNRC (1994). Human factors engineering program review model (NUREG-0711). Washington, DC: USNRC.

[5] O'Hara, J. M. (1994). Advanced human-system interface design review guideline: General evaluation model, technical development, and guideline description (NUREG/CR-5908, vol. 1). Washington, DC: USNRC.

[6] O'Hara, J. M., Brown, W. S., Baker, C. C., Welch, D. L., Granda, T. M., & Vingelis, P. J. (1994). Advanced human-system interface design review guideline: Evaluation procedures and guidelines for human factors engineering reviews (NUREG/CR-5908, vol. 2). Washington, DC: USNRC.

[7] O'Hara, J. M., Brown, W. S., Higgins, J. C., & Stubler, W. F. (1994). Human factors engineering guidance for the review of advanced alarm systems (NUREG/CR-6105). Washington, DC: USNRC.

[8] O'Hara, J. M., Brown, W. S., Stubler, W. F., Wachtel, J. A., Persensky, J. J. (1995). Human-system interface design review guideline (NUREG-0700, Rev. 1). Washington, DC: USNRC.

[9] O'Hara, J. M., Wachtel, J., & Persensky, J. (1995). Advanced alarm systems: Display and processing issues. In Proceedings of the Topical Meeting on Computer-Based Human

Support Systems: Technology, Methods, and Future (pp. 160-167). La Grange Park, IL: ANS.

[10] O'Hara, J. M., & Brown, W. S. (1991). Nuclear power plant alarm systems: Problems and issues. In Proceedings of the Human Factors Society 35th Annual Meeting (pp. 1233 - 1237). Santa Monica, CA: HFS.

[11] Lupton, L. R., Lapointe, P. A., & Guo, K. Q. (1992). Survey of international developments in alarm processing and presentation techniques. Paper presented at International Symposium on Nuclear Power Plant Instrumentation & Control. Tokyo, Japan.

[12] Easter, J. R., & Lot, L. (1992). Back-fitting a fully computerized alarm system into an operating Westinghouse PWR: A Progress report. In Proceedings of the IEEE Conference on Human Factors & Power Plants. Piscataway, NJ: IEEE.

[13] Woods, D. D. (1995). The alarm problem and directed fault attention in dynamic fault management. Ergonomics, 38, 2371-2393.

[14] Baker, S., Hollnagel, E., Marshall, E., & Øwre, F. (1985). An experimental comparison of three computer-based alarm systems: design, procedure, and execution (HWR-134). Halden, Norway: OECD Halden Reactor Project.

[15] Reiersen, C. S., Marshall, E. C., & Baker, S. M. (1987). A comparison of operator performance when using either an advanced computer-based alarm system or a conventional annunciator panel (HPR-331). Halden, Norway: OECD Halden Reactor Project.

[16] Stanton, N. (1994b). A human factors approach. In N. Stanton (Ed.), Human factors in alarm design (pp. 1-10). London: Taylor & Francis.

[17] Lees, F. P. (1983). Process computer alarm and disturbance analysis: Review of the state of the art. Computers and Chemical Engineering, 7, 669-694.

[18] Bray, M. A. (1989). Alarm filtering and presentation. Nuclear Engineering and Design, 113, 211-218.

[19] Kim, I. S. (1994). Computerized systems for on-line management of failures: A state-of-the-art discussion of alarm systems and diagnostic systems in the nuclear industry. Reliability Engineering and System Safety, 44, 279-295.

[20] Vicente, K. J., & Burns, C. M. (1995). A field study of operator cognitive monitoring at Pickering nuclear generating station - B (CEL 95-04), Toronto: University of Toronto, Cognitive Engineering Laboratory.

[21] Vicente, K. J., & Burns, C. M. (1996). Cognitive functioning of CR operators during normal plant operating conditions (AECB Final Report). Toronto: University of Toronto, Cognitive Engineering Laboratory.

[22] Kragt, H., & Bonten, J. (1983). Evaluation of a conventional process-alarm system in a fertilizer plant. IEEE Transactions on Systems, Man, and Cybernetics, SMC-13, 586-600.

[23] Mumaw, R. J., Roth, E. M., Vicente, K. J., & Burns, C. M. (1996). Cognitive contributions to operator monitoring during normal operations - Phase 2 (AECB Final Report). Pittsburgh, PA: Westinghouse Science & Technology Center.

[24] Goodstein, L. P. (1985). Functional alarming and information retrieval (Risø-M-2511). Roskilde, Denmark: Risø National Laboratory, Electronics Department.

[25] Rasmussen, J. (1985). The role of hierarchical knowledge representation in decision making and system management. IEEE Transactions on Systems, Man, and Cybernetics, SMC-15, 234-243.

[26] Gaver, W. W. (1986). Auditory icons: Using sound in computer interfaces. Human-Computer Interaction, 2, 167-177.

[27] O'Hara, J. M., & Brown, W. S. (in press). Advanced alarm systems and human performance (BNL Tech. Rep. A3967). Upton, NY: Brookhaven National Laboratory, Department of Advanced Technology.

[28] Fujita, Y. (1989). Improved annunciator system for Japanese pressurized-water reactors. Nuclear Safety, 30, 209-221.

[29] Beattie, J. D., & Malcolm, J. S. (1991). Development of a human factors engineering program for the Canadian nuclear industry. In Proceedings of the Human Factors Society 35th Annual Meeting. Santa Monica, CA: HFS.

ADDITIONAL READINGS

Baker, S., Gertman, D., Hollnagel, E., Holmström, C., Marshall, E., & Øwre, F. (1985). An experimental comparison of three computer-based alarm systems: Results and conclusions (HWR-142). Halden, Norway: OECD Halden Reactor Project.

Bennett, K.B., & Flach, J.M. (1992). Graphical displays: Implications for divided attention, focused attention, and problem solving. Human Factors, 34, 513-533.

Bye, A., Berg, Ø., & Øwre, F. (1994). Operator support systems for status identification and alarm processing at the OECD Halden Reactor Project - Experiences and perspective for future development. In N. Stanton (Ed.), Human factors in alarm design (pp. 147-164). London: Taylor & Francis.

Fink, R. (1984). A procedure for reviewing and improving power plant alarm systems (EPRI NP-3448). Palo Alto, CA: Electric Power Research Institute.

Gaver, W. W., Smith, R. B., & O'Shea, T. (1991). Effective sounds in complex systems: The Arkola simulation. In CHI '91 Conference Proceedings (pp. 85-90). Reading, MA: Addison-Wesley.

Gould, J. D. (1988). How to design usable systems. In M. Helander (Ed.), Handbook of human-computer interaction. Amsterdam: Elsevier.

Guerlain, S., & Bullemer, P. (in press). User-initiated notification: A concept for aiding the monitoring activities of process control operators. In Proceedings of the Human Factors and Ergonomics Society 40th Annual Meeting. Santa Monica, CA: HFES.

IAEA (1984). Safety-related instrumentation and control systems for nuclear power plants: a safety guide (Safety series no. 50-SG-D8). Vienna: International Atomic Energy Agency.

IAEA (1995). Control room systems design for nuclear power plants (IAEA-TECDOC-812). Vienna: International Atomic Energy Agency, International Working Group on Nuclear Power Plant Control and Instrumentation.

Kragt, H. (1984). A comparative simulation study of annunciator systems. Ergonomics, 27, 927-945.

Marshall, E., & Baker, S. (1994). Alarms in nuclear power plant CRs: Current approaches and future design. In N. Stanton (Ed.), Human factors in alarm design (pp. 183-191). London: Taylor & Francis.

MPR Associates (1985). Power plant alarm systems: a survey and recommended approach for evaluating improvements (EPRI NP-4361). Palo Alto, CA: Electric Power Research Institute.

O'Hara, J. M., & Wachtel, J. (1991). Advanced CR evaluation: General approach and rationale. In Proceedings of the Human Factors Society 35th Annual Meeting (pp. 1243 - 1247). Santa Monica, CA: HFS.

Patterson, R. D. (1982). Guidelines for auditory warning systems in civil aircraft (CAA paper 82017). London: Civil Aviation Authority.

Rasmussen, J. (1976). Outlines of a hybrid model of the process plant operator. In T. B. Sheridan and G. Johannsen (Eds.), Monitoring behavior and supervisory control (pp. 371-383). New York: Plenum.

Stanton, N. (1994a). Human factors in alarm design. London: Taylor & Francis.

Stanton, N. A., & Baber, C. (1995). Alarm-initiated activities: An analysis of alarm handling by operators using text-based alarm systems in supervisory control systems. Ergonomics, 38, 2414-2431.

Usher, D. M. (1994). The alarm matrix. In N. Stanton (Ed.), Human factors in alarm design (pp. 139-145). London: Taylor & Francis.

Vicente, K. J., & Tanabe, F. (1993). Event-independent assessment of operator information requirements: Providing support for unanticipated events. In Proceedings of the American Nuclear Society Topical Meeting on Nuclear Plant Instrumentation, Control and Man-Machine Interface Technologies (pp. 389-393). La Grange Park, IL: ANS.

Vicente, K. J., & Wang, J. H. (1996). Taking full advantage of process constraints in advanced interface design. In Proceedings of the 1996 American Nuclear Society International Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies (pp. 405-411). La Grange Park, IL: ANS.

Weiss, S. H., Regan, W. H., & Roe, J. W. (1988). Experience with operator aids for nuclear power plants in the United States of America. In Man-Machine Interface in the Nuclear Industry (pp. 323-329). Vienna: IAEA.

Woods, D. D. (1991). The cognitive engineering of problem representations. In G. R. S. Weir and J. L. Alty (Eds.), Human-computer interaction and complex systems (pp. 169-188). London: Academic Press.

Woods, D. D., Elm, W. C., & Easter, J. R. (1986). The disturbance board concept for intelligent support of fault management tasks. In Proceedings of the International Topical Meeting on Advances in Human Factors in Nuclear Power Systems. LaGrange Park, IL: ANS.

Zwaga, H. J. G., & Hoonhout, H. C. M. (1994). Supervisory control behaviour and the implementation of alarms in process control. In N. Stanton (Ed.), Human factors in alarm design (pp. 119-134). London: Taylor & Francis.

XA9744361

SAFETY ASPECTS OF THE MODERNIZATION OF I&C AND PROCESS INFORMATION SYSTEMS IN NUCLEAR POWER PLANTS WITH SPECIAL REGARD TO ALARM ANNUNCIATION

F. Seidel
Bundesamt für Strahlenschutz (BfS), Salzgitter

ABSTRACT

In particular for older German nuclear power plants there are projects to modernize I&C and process information systems. This modernization mainly aims at improvements in plant operation. For instance, using modern computing technology, the plant operation can be optimized, according to further details. Furthermore, the problem of spare-part keeping for out-dated components can be solved. For modernizing the I&C or the process computer system, safety-relevant aspects have to be taken into account. For instance, the compatibility of the system modification with the existing alarm annunciation concept shall be considered, and for each modernization step, the interfaces between the equipment of different safety significance shall be assessed and observed. The functions and the associated equipment have to be qualified in accordance to their safety significance. At present, the regulatory framework for computer-based instrumentation and control as well as for information systems is being elaborated in Germany and worldwide. Recently, the guidelines of the German Reactor Safety Commission have been extended with regard to the introduction and safety application of modern computer-based I&C in nuclear power plants. Furthermore, some of the essential requirements for design and qualification of modern I&C can be derived from the existing rules and standards. Particularly concerning the alarm annunciation system, this report summarizes safety-relevant aspects of the modernization of the instrumentation and control system as well as the process information system in nuclear power plants.

1. INTRODUCTION

To almost all of the older German nuclear power plants (NPPs) there are projects to modernize the instrumentation and control system (I&C) as well as the process computer system. The main objective of the modernization is the exploitation of the extended capabilities of *computer-aided I&C*, like, extended functionality for process controlling (introduction of complex models for process optimization), better service options (on-line self tests, automatic calibration) as well as the safe spare part supply.

Applied to *process information systems*, modern computer technology in particular can support tasks like the complex presentation of the plant status using operating mimic diagrams as well as protection goal oriented presentations to supply diagnostic and decisions in the case of disturbances and events.

High data processing - and data transmission velocity as well as higher storage capacity give incentives for using *modern process control computer systems* for NPPs [1]. In particular the following operational requirements can be better fulfilled using modern computer technology:

- operating data processing for further process optimization
- process presentation in surveys as well as in hierarchical order
- long-term process documentation and recording with high temporal resolution.

Because the computer-based alarm annunciation system - as one part of the process control computer - also processes and displays safety-relevant signals, safety aspects have to be taken into account in case of process control computer modernization. The essential aspects, as to our point of view, are described in the following.

2. FUNDAMENTAL REQUIREMENTS ON THE ALARM ANNUNCIATION SYSTEM IN GERMAN NUCLEAR POWER PLANTS

2.1 Tasks and Categorization of Alarm Signals

An alarm signal will occur either due to a deviation from normal operation as well as due to an irregular plant status, or it shows a disturbance of an electric or I&C device. The alarm annunciation system shows these disturbances visually and acoustically and thus supports the operating staff in the following tasks:

- controlling the function of automatic devices,
- identifying disturbances reliably and in time,
- activating reserve functions, in case a function has failed,
- initiating manual countermeasures for plant control during an accident or a disturbance, and
- recognizing and initiating requisite repair activities.

According to this tasks, alarm signals are classified in:

- alarm signal (possible danger),
- warning signal (impermissible deviation from the specified plant state),
- fault annunciation (disturbance without immediate danger),
- interlock annunciation (e.g., indication of isolations), and
- acknowledgment signal.

The safety-significance of an annunciation function is valued by:

- its necessity for recognizing and controlling disturbances and events,
- the consequence of its failure, and
- its urgency.

According to the German Safety Standard KTA 3501 and depending on their safety significance, alarms are categorized in three classes (S, 1, 2). Table 1 characterizes these classes and shows examples of application. For class S alarms, KTA 3501 gives the following definition:

> *"The class S alarm (safety-hazard alarm) is a signal of a safety subsystem; when it occurs, the operating personnel is required to initiate a protective action within a prescribed time period."*

The alarms of the classes 1 and 2 are of minor or without safety relevance, respectively. They indicate a disturbance in the safety system or the operating system, respectively. Disturbances which are indicated by fault- or disturbance signals of class 1, are to be eliminated. Limits for repair time are laid down in the plant technical specifications; e.g. the Operation Manual.

2.2 Basic Design Characteristics of the Alarm Annunciation System

The construction of the system for signal processing and annunciation is shown in Fig. 1 on principal.

The single alarm signals are decoupled from the level of instrumentation devices and transformed to single -, collective - or hold-back signals on the system level of signal conditioning.

The alarm annunciation system mainly consists of the conventional (hard-wired) annunciation system (KMA) and the computer annunciation system (RMA). The signals are processed according to the alarm annunciation concept (see chapter 2.1). Outgoing from RMA, signals are distributed to the control room displays as well as to local control stations. Actually in German NPPs, RMA including a process information system works in parallel to KMA.

Regarding safety-significant signals, the consistency of KMA - and RMA signals shall be continuously kept under surveillance during operation. In the case of inconsistencies, the signal of the KMA has priority and the corresponding computer signals are suppressed on the display.

The class-S alarms are transmitted via a dual-port connection from the KMA to the main control board and to the reactor protection panel. Alarm signals of other categories are transmitted via single channels.

According to the alarm annunciation concept and diverging from a hard-wired system, alarm signals of all classes are simultaneously proceeded by the process control computer. Therefore, in the case of an event-signal burst, the signals of lower priority shall be suppressed.

Process Information System PRISCA:

In some German NPPs the computer-aided process information system PRISCA is installed as part of the process computer system. Originally, PRISCA is developed for process supervision under normal operating conditions. For the operation under accidental conditions, PRISCA is

not comprehensively qualified. Additional qualification effort would be mainly imposed on the proof of software reliability and the robustness of all the associated instrumentation devices under accidental conditions. Therefore, PRISCA may only be used as an additional source of information under accident conditions, in addition to the KMA. A complete follow-up qualification of PRISCA seems to be too expensive and, up to now, has not been undertaken. Nevertheless, some of the PRISCA overview displays, showing parameters and trends to safety function supervision, have been qualified from the ergonomics point of view.

2.3 Design Guidelines for the Alarm Annunciation System

To questions concerning the safety application of new technology in NPPs, the Federal Ministry for the Environment, Nature Conservation and Reactor Safety (BMU) consults the Reactor Safety Commission (RSK) which gives statements and recommendations on basis of the RSK guidelines. Recently these guidelines have been extended to the safety application of computer-based I&C in existing as well as in future NPPs. A special chapter of the extended guidelines is dedicated to the categorization of I&C functions according to their safety significance as well as to the qualification requirements on software and hardware. The RSK guidelines give also main requirements on the human-machine interface [2].

The persisting standards of the German Nuclear Safety Standard Commission (KTA), have been formulated for I&C systems based on analog technique and for conventional control room technology. Requirements concerning the software qualification and qualification of screen-based control rooms are not given so far. In that context it should be mentioned, that in Germany the control room is not part of the safety system. Nevertheless, for approving the process computer modernization, specific requirements have to be derived from the persisting standards, e.g. from standards as KTA 3501 (Reactor Protection System and Monitoring Equipment of the Safety System) and KTA 3904 (Control Room, Emergency Control Room and Local Control Stations). Using the safety categorization of KTA 3501, the essential qualification requirements on the alarm annunciation functions S, 1 as well as 2 can be derived. For instance, the following main requirements are applied to class S signals, see also Fig. 2:

- Class S alarm equipment and the optical and the acoustic alarm facilities shall be designed against random failures. Therefore, class S alarm equipment shall be constructed to be redundant and independent of each other. Class S alarm signals may be decoupled from the protection system used for automatic actuation of protective actions.
- Class S alarm equipment shall be able to be tested during specified normal operation.
- Class S alarms shall be displayed as distinctly different from both class 1 as well as class 2 alarms.
- A class S alarm condition shall be continuously indicated, e.g. as registered, acknowledged, canceled. Therefore, the visual class S alarms shall be supplied from a non-interruptible emergency power supply with battery power storage operating in parallel to a rectifier facility.
- Class S alarms shall be stored.

2.4 Support of Manual Operation Under Accident Conditions

According to KTA 3501, the initiation of manual protective actions is only permissible if the period of time between recognizing the event and the initiation of protective actions is sufficient.

As a design feature of German nuclear power plants, the plant operation is highly automated. Even in case of operation under accident conditions, the plant is operated automatically into a safe shut-down state and maintained there at least over the first 30 minutes following a design basis event or a disturbance, so called "30-minute-criterion". The operator can use this time to forward the alarms and to derive long-term countermeasures from the operating manual, e.g. to determine the measures for maintaining the cold shut-down state.

The 30-minute-criterion applies in general. However, manual actions can be started already before the first 30 minutes after an event has occurred. This applies in particular in that case when the alarms indicate a transition to an accidental state, which is not covered by the design, and consequently, the safety can not be guaranteed by automatic protection measures only. Examples for manual measures that have to be initiated early are the manual tripping in case the scram fails (ATWS-case), switching procedures after a station black-out or after an impact from outside (e.g. earthquake).

According to the German plant design, no class S alarm should occur during the first 30 minutes after an initiating event occurs. To initiate and support long-term safety measures, alarm functions of highest priority may be demanded. According to the I&C concept, manual measures due to alarm signals have basically priority to automatic I&C functions.

3 SAFETY ASPECTS OF THE MODERNIZATION OF I&C SYSTEM REGARDING THE ALARM ANNUNCIATION SYSTEM

Normally, the modernization of I&C system as well as computer-aided process control system is not performed simultaneously and in a single step. Larger projects are subdivided into packages, each of them being implemented in one outage period [3]. Considering all modernization steps, the configuration management should guarantee that the processing, displaying and recording of safety-relevant signals are performed in compliance with the plant protection-goal concept as well as the general plant design.

The associated safety functions that have to follow on an alarm shall be guaranteed with the required reliability. Therefore during each step of the modernization of the I&C or the process information system, the following main aspects have to be considered:

- mutual adjustment of the I&C concept and the alarm annunciation concept,
- comprehensive documentation of all system modifications, and
- mutual adjustment of old and new system parts.

These adjustments refer to:

- safety-categorization of connected instrumentation and control- as well as alarm functions (depending on the significance of the system-engineering safety functions to be initiated or supported),
- interfaces between old and new plant parts,
- priority rules for automatic and manual measures, and
- alarm signal interpretation and acknowledgment.

If alarm signals shall be set off via modern computer-aided process information systems, it should be regarded that alarm annunciation is only a small part of the process information system's functionality. The alarm annunciation concept, however, ought to be compatible to the general information concept of the facility. Thus, it seems reasonable to redefine the information goals with the implementation of the modern control room technology.

For instance, the safety aspects of the I&C modernization are listed in detail according to a life-cycle proceeding model in [3].

4. SAFETY ASPECTS OF THE MODERNIZATION OF THE PROCESS INFORMATION SYSTEM

4.1 Example of a Modernization Concept

A modern computer-based information system offers extended capabilities to signal processing and interpretation, manifold options of screen display (e.g. a protection-goal oriented plant overview) as well as recording of process data over long periods of time with high resolution and with improved retrieval option (e.g. with regard to detailed event analysis). Therefore as a first aim, the modernized process information system with extended functionality can be used additionally as a diverse information source with lower priority than the KMA. After progressive software and hardware qualification and collecting operating experiences, the new process information system may get a higher safety significance.

The following basic concept is pursued in the current modernization projects that up to now have been planed and partly already implemented in Germany [4]:

- Before the process information system functionality is significantly expanded, its former functions are described in detail by re-engineering.
- Due to the high effort for construction, switch over and testing of the new process information system, a step-wise proceeding is reasonable that is oriented to the outage period.
- As a prerequisite for the safety significant use of the process information system a comprehensive qualification methodology is to be established regarding the safety categorization of the involved safety-relevant functions. Because of the complexity of the process information system, the time spending on the qualification process - particularly on the software reliability prove - will be rather high.

- Therefore, the new process information system is tested partly also during plant operation. In that phase, the signals of the new information system have no safety significance. New and old systems have to be decoupled. The period of parallel processing may take one or even several operational cycles.
- This parallel operation can be terminated and the old process information system may be decommissioned when the qualification procedure for the new system is successfully completed.

4.2 Basic Design Characteristics of the Process Information Systems

In the frame of licensing or approval of a modernized process information system, the following safety-relevant aspects have to be considered by regulatory body. These aspects are mainly covered by the standard KTA 3501.

- The safety-critical I&C (e.g. the I&C for reactor protection) shall be spatially separated and functionally decoupled from the process information system that has a lower safety significance. The reactor protection signals relevant to operator information shall be transmitted to the process information system in a non-interacting way (without feedback).
- The parts of the process information system that are used for transmission, processing and storage of safety-relevant information shall be designed according to the single-failure concept. As a rule, two process control computers with assigned stores and two data bus systems are implemented.
- The energy supply for the redundant parts of the process information system should be supplied from switching stations that are spatially separated from each other.
- The process information system should be continuously kept under surveillance using a comprehensive disturbance annunciation concept. A redundant failure - as well as disturbance recording is required according to KTA 3502. Among other things, the locking of electronic cabinet doors, temperature, energy supply and availability of the alarm functions shall be monitored during operation.

Furthermore, the following technical aspects of modernization should be taken into account:

- For network communication, proven industry-standard records with capabilities to keep under surveillance the network interactions as well as early failure recognition may be used.
- Optical storage disks with high storage security and capacity are appropriate to store an extensive amount of process data.
- An expansion of the information goals inevitably leads to higher requirements on the software and hardware for data processing and -storage. Therefore, design characteristics as data storage capacity and processing speed should be chosen with sufficient margins for further system development. On the other side, significant ergonomic problems could occur if the flood of data is not limited already in the design phase. To avoid a signal

burst in case of an event, the data amount should be limited (suppression of repeated as well as secondary signals).

4.3 Qualification of Process Information System

Up to now, computer-aided process information systems have been used for operating purposes only. These information systems are not yet comprehensively qualified for safety related purposes. Because modern process information systems offer the option to present overview displays with complex content and correlation, also a safety-related use is of great interest. In the case of operation under abnormal or accident conditions, such overview displays can support the operator in watching the protection-goals. Such a computer function is to be categorized as safety-relevant. The qualification requirements on I&C functions can be derived depending on the safety-significance using the RSK guidelines as recently extended [2].

Since most of the existing information systems have not been consequently developed and qualified according to a proceeding model (e.g. life-cycle model) a follow-up qualification can be rather extensive. In the frame of a follow-up qualification at least the items of chapters 2.2 and 4.2 should be considered, depending on the safety classification of the processed signals.

The operation of digital I&C and process computer systems shows worldwide satisfying experiences. Nevertheless, in the recent discussions about digital I&C system qualification, the sufficient reliability proof of digital systems is pointed out as a main issue, whereby realistic reliability goals are to be established. Considering this issue and the complexity of process computer systems, it should be investigated under which assumptions alarms coming from the process information system can be used for operation under accident conditions.

According to IEC 1226, the I&C equipment shall be qualified according to the categorization of the associated I&C function. However, with the achieved state of the art of qualification- and proof methodology this is not yet feasible in all details for such complex software-aided systems, like process computers.

Therefore the question is, whether computer processed safety alarms can be used as basis for manual safety actions, and if yes, how the qualification requirements can be met in accordance to the regulatory framework. Regarding this question, the extended RSK guidelines open the possibility to use alarm functions qualified in accordance to a lower safety category [2]. The main condition is, that the whole subset of alarm functions that are used to select and initiate the mentioned manual safety action meets the reliability demands of the associated safety function category. Following that idea, a manual safety function of the highest safety category, for instance, can be initiated on basis of different (redundant/diverse) alarm functions of a lower category.

Qualification Management for the Modernization Process:

Generally, several qualification measures are contributing to ensure the process information system quality (particularly the reliability) during modernization. For instance, computer

configuration, network structure, data security (access right privilege, data integrity), updates and documentation of the single modification steps are kept under surveillance.

With the help of a data maintenance system, the data integrity is also to be controlled during later operation and maintenance. Due to future plant modifications and associated maintenance activities, it is assumed that amount and composition of the data to be administered are varying in time. Therefore, the process information system qualification is a life-time task, the maintenance activity is to be considered in the frame of the whole software life-cycle including the phase of operation and maintenance.

Modification management should clearly distinguish between operating system modifications (e.g. changing of setpoints) and those due to further system development. All modifications shall be documented automatically and in a comprehensible way.

The proof of reliability for the automatic rapid switch from a failed or defective computer string to the remaining redundancy (as a rule in stand-by operation, possibly also flicking between bus - and storage units) is of particular significance for data security.

Technical - and software equipment to recognize failures as well as to identify and locate faults have to be tested extensively. At present, a method to formally prove the test coverage is being elaborated.

Software Qualification:

A main qualification effort is to be directed on the software, including user specific as well as standard software. As a main standard for software qualification, IEC 880 deals with the qualification of software to safety critical applications. Regarding software of lower safety significance, e.g. for process information systems, a supplement to IEC 880 is currently under discussion. Substantially, IEC 880 gives recommendations for a software qualification strategy, involving the application of a qualification proceeding model (e.g. the software life-cycle) as well as rules of software engineering. To consider some of these rules during software development automatically, the application of formal methods and graphical specification is recommended. Recently, the application of a qualification proceeding model and specification tools has been regarded as essential prerequisite for the successful proof of reliability, in particular to avoid systematic failures due to specification errors.

Aspects of Ergonomics:

In addition to the proof of reliability, safety-relevant information should be assessed considering the features of ergonomics. Regarding that, two of the main aspects are:

- It should be possible to recognize the safety-relevance of each screened alarm signal.

- In the case the alarm signal reliability can only be validated partially, e.g. with regard to the robustness of the corresponding instrumentation under accidental conditions, these alarms should be marked on the screen.

REFERENCES

[1] HEINBUCH, R., Erkenntnisse aus dem Betrieb mit bildschirmgestützter Informationsdarstellung und resultierende Anforderungen an zukünftige Warten in Kernkraftwerken, Jahrestagung Kerntechnik '91, Fachsitzung Bildschirmgestützte Mensch-Maschine-Kommunikation, Bonn, Inforum GmbH (1991) 19-37.

[2] RSK-Leitlinien für Druckwasserreaktoren, Kapitel 7, Elektrische Einrichtungen des Sicherheitssystems, Bundesanzeiger, August (1996).

[3] SCHNÜRER, G., WACH, D., SEIDEL, F., WEIL, L., „Upgrades of Digital I&C in German Nuclear Power Plants - Regulatory Aspects and Qualification Requirements", Modernization of Instrumentation and Control Systems in Nuclear Power Plants (Proc. IAEA Specialists' Meeting, Munich, 1995).

[4] KÖHLER, M., SCHÖRNER, O., Langfristige Sicherung der Funktion leittechnischer Einrichtungen, Jahrestagung Kerntechnik '96, Fachsitzung Fortschrittliche Betriebsführung deutscher Kernkraftwerke, Bonn, Inforum GmbH (1996).

SESSION III

NEW IMPLEMENTATIONS

DEVELOPMENT OF ALARM HANDLING METHODS FOR BOILING WATER REACTORS

Yukiharu Ohga, Hiroshi Seki, Setsuo Arita
Power & Industrial Systems R&D Division, Hitachi, Ltd.
7-2-1 Omika-cho, Hitachi-shi, Ibaraki-ken, 319-12 Japan

ABSTRACT

In nuclear power plants many alarms are activated under major plant transients. During such conditions, operators' work loads increase because they have to identify the important alarms from among the many activated alarms and they have to recognize causes of anomalies and the anomalies' effects upon plant components. Two methods relating to alarm handling were developed, alarm selection and presentation, with the aim of minimizing the potential for human errors.

From among the many generated alarms, it is effective for operation support to select the most important alarms according to the plant status. A method was developed to select important alarms in two steps: first, selection is based on the physical relationship between the alarms, and second, selection is according to the initial event. An approach combining a neural network and knowledge processing was proposed to identify the event rapidly. A prototype system was evaluated in the Kashiwazaki/Kariwa-4 Nuclear Power Plant during the startup test. The evaluation test confirmed that about 30% of the alarms are selected from among the many activated alarms.

The second method, dealing with presentation, supports operators in their selection and confirmation of the required information for plant operation. The method selects and offers plant information in response to plant status changes and operators' demands. The selection procedure is based on the knowledge and data as structured by the plant functional structure; i.e. a means-ends abstraction hierarchy model. A prototype system was evaluated using a BWR simulator. The results showed that appropriate information items are automatically selected according to plant status changes and information on generated alarms is presented to operators together with the related trend graph and system diagram. Answers are generated in reply to the operators' demands and operators can confirm the generated alarms on each plant function, such as systems and components.

1. INTRODUCTION

Human factors play an important role in operation under transient conditions in nuclear power plants. Consequently minimizing the potential for human errors is essential to enhance the plant availability. Many investigations have been devoted to providing support for operators.

To support operators under transient conditions, alarm handling is one of most important approaches. In nuclear power plants many alarms are activated during major plant transients. Under such conditions, operators' mental work loads increase because they have to identify the important alarms from all the activated alarms and they have to recognize the cause of anomalies and the influence upon plant components from the alarm and other plant information. Therefore, many investigations are being made on alarm handling. For example, the Halden Reactor Project is developing a new alarm system called CASH [1] and a toolbox for building specific alarm systems for different plants called COAST [2]. AECL developed an improved computerized annunciation system CAMLS for CANDU plants [3].

As one approach to handling alarms, we have developed two methods for alarm selection and presentation. The alarm selection method selects important alarms according to the plant status. As for alarm presentation, the information offering method was proposed which selects and offers plant information including alarm information in response to plant status changes and operators' demands. In the paper, evaluation results using prototype systems are described after presentations about the features of two methods. The concept of a new man-machine system applying these two methods is also shown.

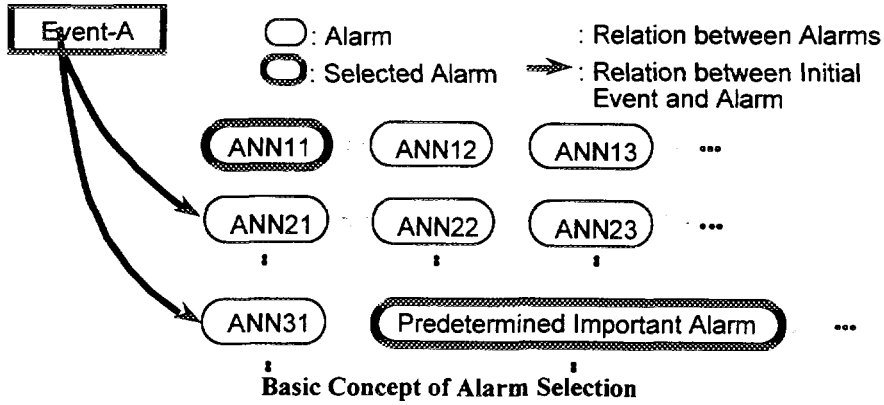
2. ALARM SELECTION METHOD [4, 5]

2.1 Method

2.1.1 Basic Concept

When a major transient occurs in nuclear power plants, many alarms are activated within a short period. Immediately after a transient occurs, it is considered that operators recognize a cause and influences of an anomaly mainly from alarm information. Therefore the alarms indicating cause and major influences to plant components should be selected as important alarms. The basic concept of alarm selection is shown in Figure 1.

To select alarms indicating anomaly cause, selection is performed using physical and logical relations between alarms. In the figure, ANN12 certainly occurs when ANN11 occurs. On this occasion, ANN12 is recognized as a secondary alarm and ANN11 is selected as a causal-side important alarm. In the selection process, the alarms on major plant components and process variables, such as "reactor scram," are determined beforehand as important alarms. They are always regarded as important even if they are decided as secondary alarms. These alarms indicate major influences of an anomaly.



Basic Concept of Alarm Selection

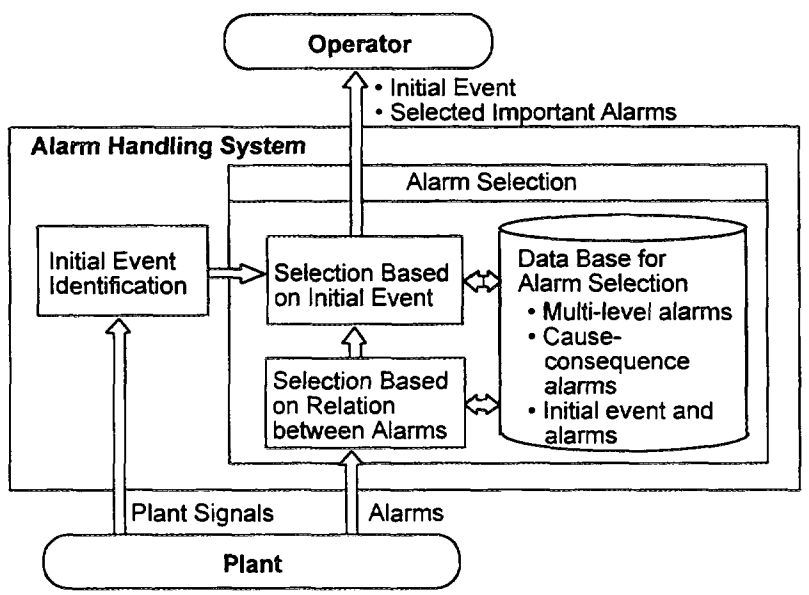
To further decrease operators' work loads, it is effective to offer them the transient cause, namely the initial event, directly. The alarm selection method identifies the initial event and displays it to operators. Additionally, alarms are further selected based on the identified event. Alarms which certainly occur when the identified initial event occurs are regarded as secondary alarms. For example, alarms ANN21 and ANN31 always occur when the initial event is EVENT-A, so that these alarms, once selected as important ones in the selection using the relations between alarms, are set as not an important alarm when the initial event is EVENT-A. This alarm selection is performed only for major plant transients accompanying a reactor scram when many alarms are activated.

2.1.2 Functional Composition

A functional composition of the alarm handling system is shown in Fig. 2. The system selects important alarms in two steps. In the first step, alarms are selected based on the logical and physical relations between them. This alarm selection is performed periodically. In the second step, alarms are further selected based on the initial event. This second alarm selection part is activated when the event identification result is input from the initial event identification part which identifies kinds of initial events causing a reactor scram. When a reactor scram does not occur or the event identification fails, only the selection in the first step is performed.

The data base for alarm selection is made based on three rules shown in the figure. As for multi-level alarms, the severer alarm is regarded as important. For example, the "Low-Low" alarm is selected when "Low" and "Low-Low" alarms are both activated. For cause-consequence alarms, the causal alarm is regarded as important. When "Pump Trip" alarm and downstream "Flow Rate Low" alarm are both activated, the "Flow Rate Low" alarm is regarded as a secondary alarm. As for the initial event and alarms, an alarm which certainly activates when the initial event occurs is regarded as a secondary alarm.

To have proper alarm selection, events must be identified rapidly and the results must be reliable. A method combining a neural network and knowledge processing [6] is used to realize this.



Composition of Alarm Handling System

2.1.3 Event Identification Method

The event identification method is shown in Figure 3. Identification is performed by using a neural network and knowledge processing. The neural network can rapidly identify the events from the change pattern of the analog data. Knowledge processing increases the reliability of results by confirming them based on different types of data.

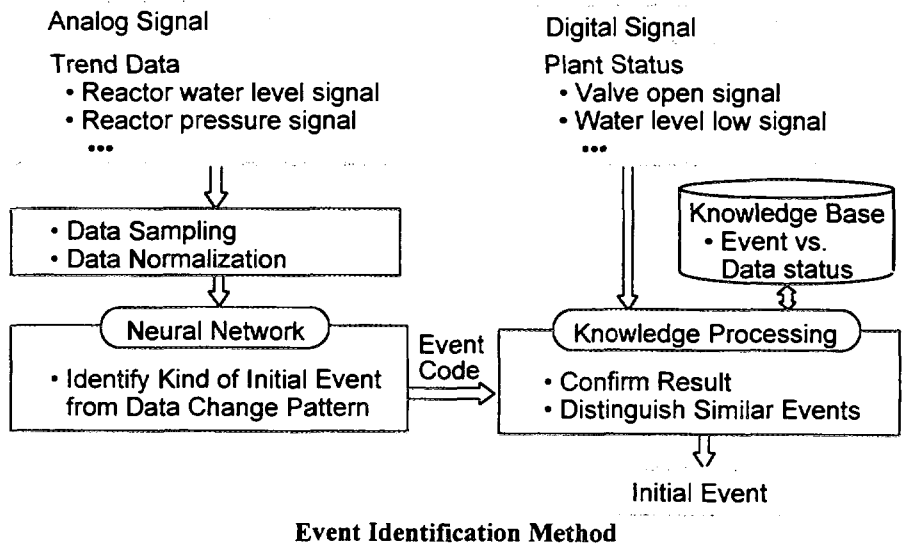
In the method, analog trend data are sampled and input to the neural network after normalization. Five kinds of analog data are selected for neural network input: reactor pressure, reactor water level, neutron flux, main steam flow rate, and feedwater flow rate. The data are sampled based on the trigger signal for data sampling to get a similar change pattern for each kind of event. For the signal a reactor scram signal is used. The data normalization is performed based on the value at the first sampling time to cope with the difference in the initial conditions before a transient occurrence. The neural network outputs the event code which corresponds to the candidate initial event.

The knowledge processing part confirms the neural network result using digital data on plant status, such as a valve open signal. This part compares the plant statuses with the knowledge base which prepares the values of digital data when each event occurs. Events that have similar change patterns of analog data and cannot be discriminated by the neural network can also be distinguished.

2.2 EVALUATION TEST

2.2.1 Test Condition

The prototype system for alarm selection was tested in Kashiwazaki/Kariwa-4 Nuclear Power Plant of Tokyo Electric Power Company during the plant startup test. In the evaluation, the test apparatus was connected to the plant facilities and the on-line performance was evaluated.



Event Identification Method

The evaluation tests were performed for three kinds of transients initiated deliberately during the plant startup test. These events are generator load rejection (initial power: 100, 75, 50%), the turbine trip (50%) and the MSIV closure (100%) events as shown in Table I. To confirm the performance of the event identification method, typical abnormal events, which include events in the plant startup test, are selected and trained by the neural network. The training events and event codes are summarized in Table I. Nine kinds of events are trained by the neural network using the simulated results of a transient analysis program for boiling water reactors (BWRs).

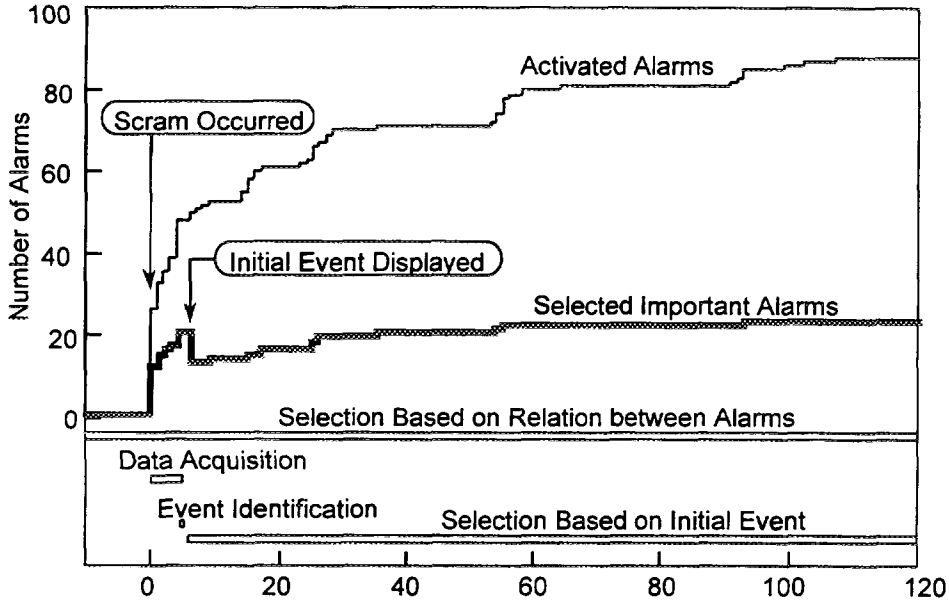
2.2.2 Result

The tests confirmed that events are identified and alarms are selected correctly. The change in number of alarms is shown in Figure 4 for the generator load rejection event with the processing status of the prototype system. The number of activated alarms rapidly increases after the reactor scram. The alarm handling system selects important alarms periodically based on the relations between alarms. After scram, the data for the event identification are acquired. The data from -10s to 5s based on the scram time are required. After the data are obtained the event identification is performed. When the initial event is identified, this result is displayed to the operator and alarm selection based on the initial event begins. At 120s the number of selected alarms is 24 which is about 30% of the total number of activated alarms, 88. In the other tests about 30% of the alarms are also selected from among the many activated alarms. The selected alarms were evaluated by the startup test operator of Tokyo Electric Power Company. As a result the selected alarms were judged adequate and the alarm selection and event identification results were effective to recognize the plant anomaly status rapidly.

As for event identification, three kinds of tested events were correctly identified from nine kinds of events in Table I by the neural network. In the tests, the output of the neural network was very close to the trained event code. The difference between the trained event code and calculated output using the plant data was less than 0.03. As for knowledge processing, the event

Table 1: Training Events and Tested Events

No.	Kind of Event	Event Code	Initial Power (%)	Tested Event
1	Generator load rejection with bypass valve (BPV) operational	1 0 0 0	100 75 50	Tested Tested Tested
2	Turbine trip	1 0 0 0	100 50	 Tested
3	Main steam isolation valve (MSIV) closure	0 1 0 0	100	Tested
4	Loss of feedwater heating	0 0 1 0	105	
5	Loss of feedwater flow	0 0 0 1	105	
6	Loss of off-site alternating current (ac) power	1 1 0 0	105	
7	Main steam pressure regulator failure	0 1 1 0	105	
8	Feedwater controller failure	0 0 1 1	105	
9	Generator load rejection with failure of BPV	1 1 1 0	105	



Alarm Selection Result (Load Rejection 100%)

confirmation was correctly performed. The load rejection and turbine trip events, which had been trained as one kind of event, were correctly discriminated.

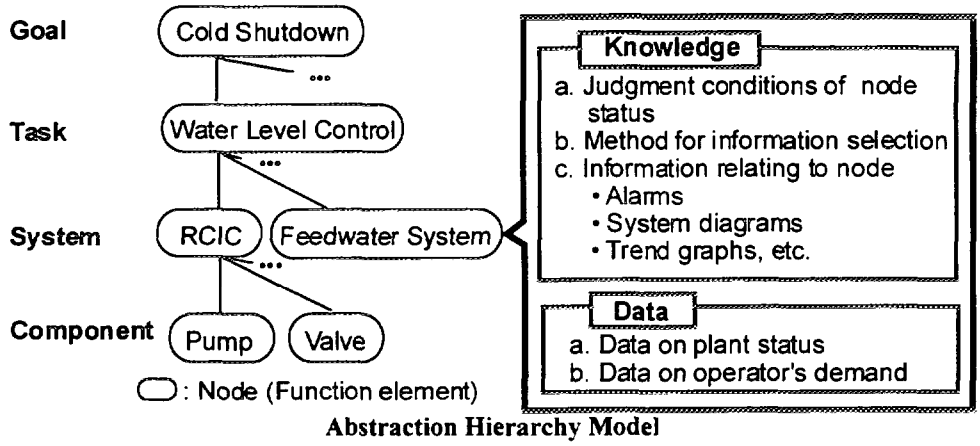
3. INFORMATION OFFERING METHOD [7]

3.1 METHOD

3.1.1 Abstraction Hierarchy Model

Under transient conditions, operators identify plant status and operate components and systems to mitigate influences of anomalies. The information required in the operation is not only the status of the components and systems, but also influences and causes of the status. When a malfunction occurs in a component, for example, operators must recognize the causes and influences of the malfunction as well as the status of the failed component. Therefore three kinds of information on status, influence and cause should be selected and offered to operators.

In the method knowledge and data required to select the information are structured using the abstraction hierarchy concept [8]. Plant functions are represented hierarchically and knowledge and data are prepared for each function element, namely node, as shown in Figure 5. In the paper this is called the abstraction hierarchy model. Cold shutdown of a plant, namely the goal, is achieved by tasks, such as reactor water level control and reactor pressure control. For water level control, the reactor core isolation cooling system (RCIC), etc. are prepared in a plant. Functioning of the RCIC system is realized by pump and valves, etc. As the knowledge, judgement conditions of node status and method for information selection are prepared. Information relating to the node includes the related alarms, system diagrams, trend graphs, etc.

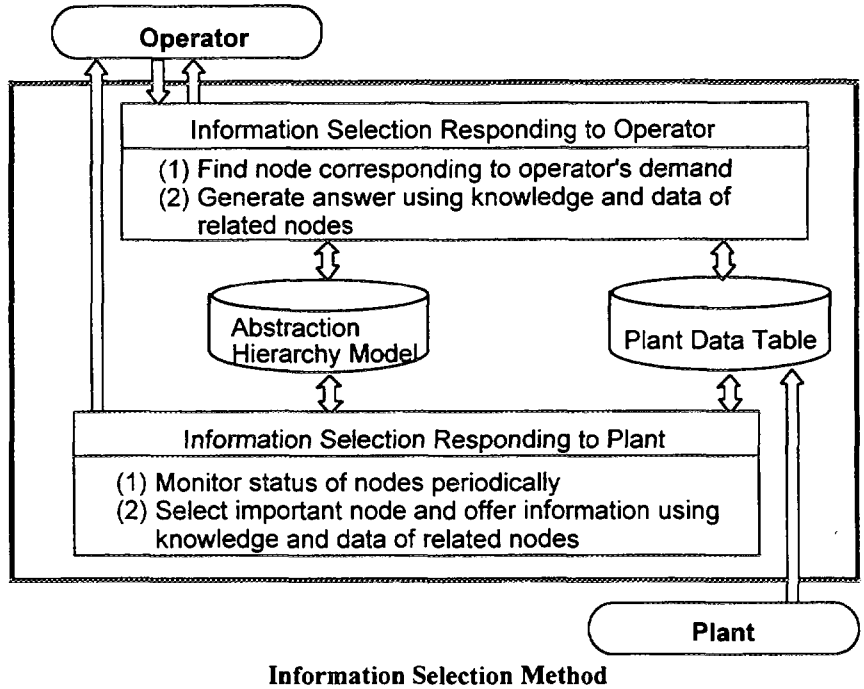


Abstraction Hierarchy Model

In the abstraction hierarchy, by paying attention to a function node on a certain level, the purpose or "why" of the function is represented in the upper level. The implementation or "how" of the function is represented in the lower level. When a function becomes abnormal, information on the influence of the anomaly is retrieved from the upper level nodes. On the other hand information on the anomaly cause is obtained from the lower level nodes. Therefore the information on influences and causes can be automatically retrieved by referring to the upper and lower level nodes if the knowledge and data on node status are prepared in each node. Another merit of the abstraction hierarchy model is that plant data, such as alarms, are managed and can be offered to operators hierarchically.

3.1.2 Information Selection Method

Plant information is selected by two parts using the abstraction hierarchy model and a plant data table as shown in Figure 6. One selects information responding to the operator's demand. The other selects information responding to plant status change such as anomaly occurrence.
The information selection responding to the operator's demand is activated when the operator's demand is input. The node is searched corresponding to the demand. Then an answer is



Information Selection Method

generated using the knowledge and data stored in the node. The related nodes, in upper and lower levels, are referred to if required according to the kind of demand. When the demand requires related information for a system, for example, related nodes in upper and lower levels are referred to and information on status, influence and cause are selected.

The information selection in response to plant status change is activated periodically. Status of nodes are monitored using the judgement condition in the abstraction hierarchy model. Based on the monitoring results, the nodes for which the judgement condition is satisfied are obtained. From the nodes, one node is selected to offer information automatically. Plant information, such as the system diagram and generated alarms, is selected using the knowledge and data in the related nodes including connected nodes in upper and lower levels.

3.2 EVALUATION TEST

3.2.1 Prototype System

The prototype system was evaluated using a real time simulator of a boiling water reactor (BWR). The prototype system and test situation are shown in Figure 7. The prototype system is composed of a process computer with touch sensitive CRT, a workstation, and speech input and output devices. A microphone headset and a touch sensitive CRT are used for input devices. Input from these devices are both transformed into words in natural language (Japanese) and analyzed as a sentence to realize an arbitrary input mode combination. Output from the system is offered by a loudspeaker and the CRT.

An example CRT display is shown in Figure 8. The displayed information includes a system diagram, a trend graph and generated alarms, etc. In the input monitoring region, speech input and touch input from operator are displayed in Japanese words. In the output monitoring region an answer for the operator is displayed.

3.2.2 Result

The results of a system evaluation are shown for a case of an abnormal transient initiated by loss of feedwater. An example dialog between the operator and the system is summarized in Table II.

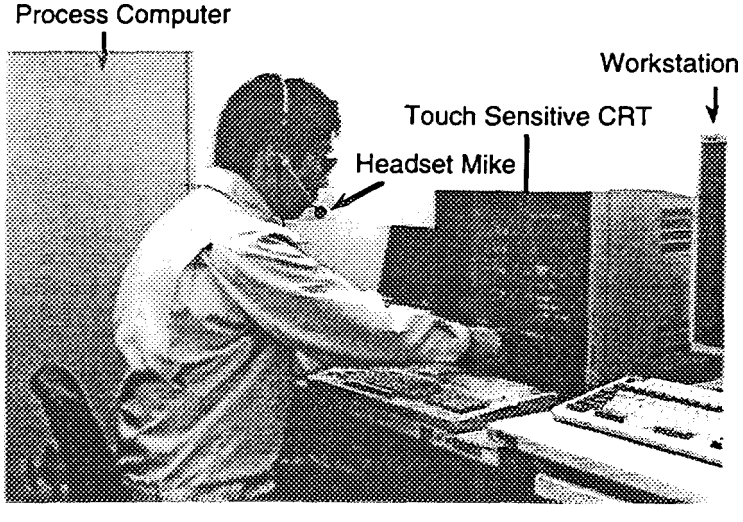


Figure 7: Prototype System

When loss of feedwater occurs, the feedwater flow rate decreases to zero and the reactor water level decreases. According to the reactor water level decrease, reactor scram occurs due to plant interlock. The reactor water level further decreases. Then reactor core isolation cooling system (RCIC) and high pressure core spray system (HPCS) begin coolant injection and closure of the main steam isolation valves (MSIVs) occurs. The system detects these plant status changes and selects and offers related information automatically. The system output shown in Table II is a part of the speech output. Besides this system diagram, a trend graph and generated alarms, etc., are displayed on the CRT as Figure 8. Related messages are output from a loudspeaker. As for alarms, related alarms are selected referring to the related nodes including connected nodes in upper and lower levels. The system displays alarms after arranging them for each function.

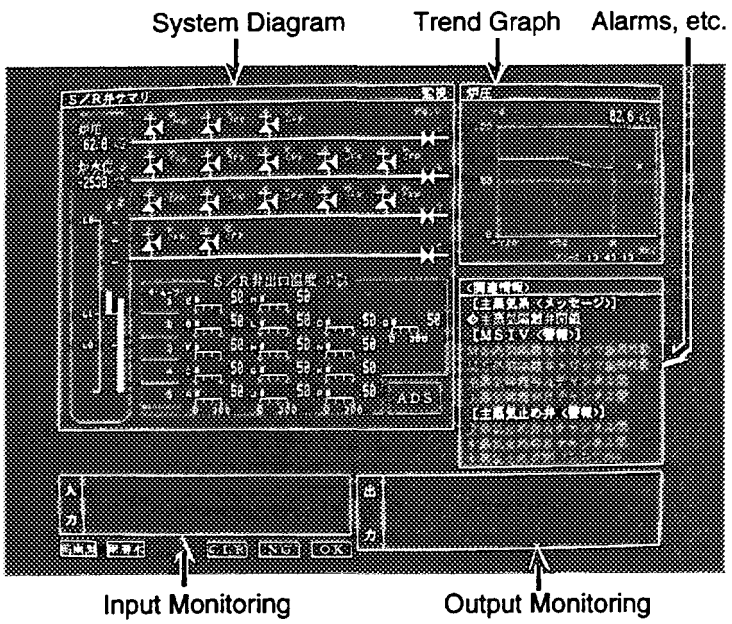


Figure 8: Example of CRT Display

Table 2: Dialog Between Operator and System (Originally in Japanese)

Operator Input	Speech Output from System
———	Loss of feedwater occurs.
———	Reactor water level is less than L3 set point.
———	Reactor scram occurs.
———	Reactor water level is less than L2 set point.
———	RCIC starts up.
———	HPCS starts up.
———	MSIV closure occurs.
:	:
Show alarms on main steam system.	Alarms relating to main steam system are displayed.
Display alarms on MSIV.	Alarms relating to MSIV are displayed.
:	:

The operator inputs demands to confirm information required for deciding and performing the anomaly mitigating operations. In the table the operator inputs two demands. First the demand "Show alarms on main steam system." is input. In response to this alarms related to main steam system and related components, such as MSIV, are selected referring to the main steam system node and lower component level nodes. The next demand is "Display alarms on MSIV." In answer the alarms only on MSIV are shown. Activated alarms are presented responding to operator's demand as shown in Figure 9. Displayed alarms are selected from the node corresponding to the demand and the lower level nodes connected.

From the test results, it is confirmed that related information is automatically selected in response to the plant status change, such as component failure and cooling system activation, in real time. The contents of the offered information are confirmed to be adequate based on reference to emergency operation guidelines of the plant. In the method, information not only on status of the plant function, but also on the influences and causes is offered to operators, which is useful for anomaly mitigating operations. Automatically offered information in response to plant status change is advantageous because the operator might not select and change the CRT displays to identify the plant status changes. Another merit of the model is that it manages alarms in functional hierarchy and the operator can confirm the activated alarms hierarchically. This means the operator can confirm the generated alarms to the desired extent. He can selectively monitor all the alarms relating to the main steam system or the alarms only for MSIV.

4. MAN-MACHINE SYSTEM APPLYING TWO METHOD

A new type man-machine system offering alarm and other plant information will be realized by using the above mentioned two methods. The composition of the man-machine system is shown in Figure 10. In the system the information to the operator is offered through the information offering method. Namely the information responding to the plant status change and information responding to operator's demand is offered after selection and arrangement by information offering method. As for alarm information, important alarms selected by the alarm selection method are stored in the data base on selected alarms. The information offering part refers to the selected alarm data and offers alarm information considering the importance of alarms. Only selected important alarms are displayed or selected alarms are displayed by using different colors than unimportant alarms. This alarm presentation method requires further research.

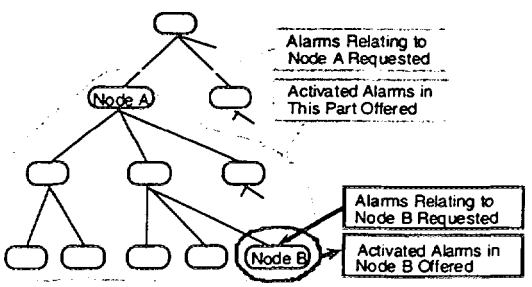


Figure 9: Offered Alarms Responding to Operator's Demand

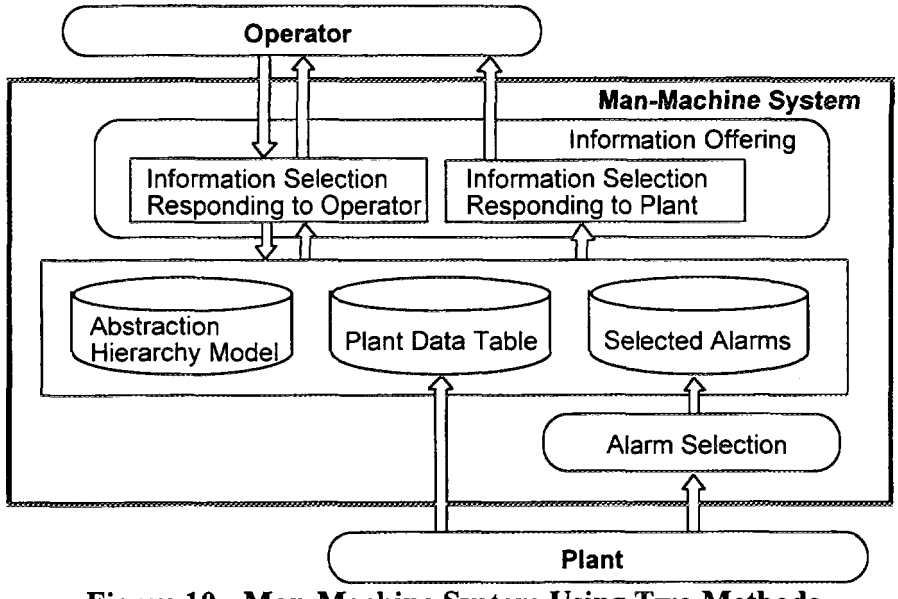


Figure 10: Man-Machine System Using Two Methods

With the man-machine system, alarms are automatically presented with other related information, such as system diagrams and trend graphs, according to the plant status change. The initial event is also presented automatically. This supports operators in their recognition of plant statuses immediately after the transient occurs when the plant status changes rapidly according to anomaly and plant interlock actuation. In the long term after the transient occurs, all information on activated alarms becomes important to confirm statuses of components and to decide repair or re-startup procedures. Responding to this occasion, alarms are hierarchically presented according to the operators' demands.

5. CONCLUSIONS

Two methods for alarm handling were developed to minimize the potential for human errors in nuclear power plants. One is to select important alarms according to the plant status. The other is to offer plant information including alarms in response to plant status changes and operators' demands. The feasibility of two methods was confirmed by using prototype systems.

The new man-machine system concept was proposed applying these two methods. With the system, alarm information as well as other plant information will be effectively offered to operators. The system should be useful to support operators in their recognition of plant statuses under transient conditions in nuclear power plants.

REFERENCES

[1] Førdestrømmen, N. T., et al., "CASH: an Advanced Computerized Alarm System," Proc. ANS Topical Meeting on Computer-Based Human Support Systems: Technology, Methods, and Future, Philadelphia, USA, June 25-29, 1995, p. 329 (1995).

[2] Bye, A., et al., "COAST, a System for Advanced Alarm Handling and Interactive Alarm Analysis," ibid., p. 168 (1995).

[3] Feher, M.P. and Davey, E.C., "Annunciation Improvements - Assessment Approaches and Lessons Learned," ibid., p. 143 (1995).

[4] Ohga, Y. et al., "Evaluation Test of Alarm Handling System in Kashiwazaki/Kariwa-4 Plant," ibid., p. 305 (1995).

[5] Ohga, Y. et al., "Evaluation Test of Event Identification Methods Using Neural Network at Kashiwazaki Kariwa Nuclear Power Station Unit No. 4," J. Nucl. Sci. Technol, 33, 5, 439 (1996).

[6] Ohga, Y. and Seki, H., "Abnormal Event Identification in Nuclear Power Plants Using a Neural Network and Knowledge Processing," , Nucl. Technol, 101, 159 (1993).

[7] Ohga, Y. and Seki, H., "An Information Offering System for Operation Support Based on Plant Functional Structure," J. Nucl. Sci. Technol., 32, 8, 727 (1995).

[8] Rusmussen, J., " Information Processing and Human-Machine Interaction - An Approach to Cognitive Engineering, Elsevier Science Publ., New York (1986).

XA9744363

ALARM PROCESSING - WAYS TO THE FUTURE

Dominique Pirus
EDF - Septen Service Études et Projets Thermiques et Nucléires
12-14, Avenue Dutriévoz - 69628
Villeurbanne Cedex, France

ABSTRACT

After a brief presentation of the main characteristics an efficient alarm system should have, a presentation of the N4 alarm processing and presentation is described in terms of reduction in alarm occurrence, alarm handling and operator presentation.

The EDF experiments on the future alarm processing expected for the next generation of the French nuclear plants are then presented. This alarm system will manage the alarms functionally in order to present to the operators the real consequences on the whole plant of a dedicated alarm and try to imbed deeply the alarm presentation within the operating formats and the procedures.

1. GENERAL DESIGN PHILOSOPHY AND REQUIREMENTS FOR AN OPTIMAL ALARM SYSTEM

1.1 Current Situation Analysis

Current alarm systems usually suffer of different lacks. They often generate too many alarms during transients, and produce information overflow to the operators.

The operators are able to perform their main cognitive tasks; state identification (detection, diagnosis), action planning (prognosis), and action implementation during small disturbances where only a few alarms are generated, but as the amount of alarm increase, as their tasks grow until to be difficult to be managed in real time.

In order to reduce this amount of information, they have to recreate the information generation by use of information from process parameters to deduce and determine what is really going on in the plant and try, thereby, to eliminate irrelevant alarms.

This task is complicated by the fact there is no optimisation of the alarm generation according to the process situations.

The important obstacle for an efficient alarm generation design, is the complexity of the different situations to take into account for alarm filtering and, some time, a kind of fear from the designers to inhibit. When an alarm is inhibited, the information is hidden to the operators, it is more secured for the designers to keep the annunciation on and expect that the operators will be able to manage them.

These observations indicate that the alarm systems are non-optimal, or more general, that the overall process information system may be non-optimal.

1.2 General Requirements

An alarm system that only contains alarm information and disconnected to the other operation means can never become an ideal alarm system because it is not adapted to the operator mental model to solve problems.

The operators use as inputs both process parameters and alarms. If the alarm system and the process information system are either integrated or at least coherent, the operators will be in a non-optimal situation to perform their tasks.

In order to try to find solutions to these problems, it is necessary to develop a complete process surveillance & control system of which the alarm system is a part. This integrated information and control system should be designed in a manner where the operators are never exposed to information overflow, even in case of the worst plant disturbances, and where the operators are always aware about the real state of the whole plant.

As a such kind of information system must contain only the necessary information the operator needs to perform his tasks. It should be dynamic, i.e., the content will in general vary from one process situation to an other.

One solution to improve the information presentation is to present all relevant alarm and process information integrated into the same display:

- the operator tasks workload necessary to extract and to manage together the relevant process and alarm information is therefore minimised, and
- the operator dialogues, (i.e., the number of display retrievals, use of keyboard, trackerball, etc.,) is optimised.

All information that could be needed by an operator must be available to the operator through the displays.

The system do not have to suppress definitively any information, it only filter parts of the information from the operating displays and must allow the operators to be able to make the decomposition of any internal logic.

The major difficulty in designing a such alarm and process information system is to optimise it for all process situations with respect to the limitations of the operator's mental capabilities. Two other ways can be followed, for a new design, in order to increase the operator's mental capabilities, either by increasing the operator's available time for these instances, or by introducing more automation.

2. N4 ALARM PROCESSING PRESENTATION

2.1 General Organisation of the Main Control Room

The N4 control room comprises:

- Four identical computerised workstations (called KIC system).
- Each workstation includes three graphic CRT's for control and information on the plant unit, four CRT's for alarm presentation and storage, and dialogue devices (three touch-sensitive CRT's, two functional keyboards, one alphanumeric keyboard, and a tracking ball).
- A wall-mounted mimic panel for an overall view of the plant unit.
- The state of main actuators, systems, and key parameters are presented to give an overview to the shift and management members entering the control room. The mimic panel is also used to prevent each control room operator from being isolated on his workstation, giving him the opportunity in verbal information exchange (in particular during shift turnover).
- A conventional auxiliary panel, used only in case of KIC failure.

2.2 Description of the Alarm Treatment

Alarm management and processing is a particularly rich in functionalities. The major characteristics of the alarm processing system are:

- strict-classification used to draw the operator's attention to important alarms,
- classification, with respect to their importance,
- classification of alarm, with respect to their origin,
- on-line diagnosis of the causes of alarms and indication of corrective actions to undertake.

The major aim was to reduce the occurrence of an non relevant alarm and present to the operators, in real time, which alarm is the most important to manage in any situation of the plants.

This has been achieved by using several level of validation and ways of processing:

- the first level, signal validation, allows to guarantee that the alarm is really relevant and that its generation is error free,
- the second level, functional validation, allows to inhibit the "normal alarms" or the ones which can be hidden by an other one,
- the third one, situation validation, allows to manage the accuracy and the severity of the alarms, according to the situation of the plant.

2.2.1 Signal Validation

The signal validation allows to guarantee that the alarm is really relevant and that its generation is error free. This is possible because all the component of the plant, and of course all the power supplies of the sensors which generate alarms, are monitored by the plant computer. In case of malfunctioning of the item which generates the alarm, the alarm signal is automatically inhibited because it is impossible to determine if there is a real failure on the process or if the alarm is only an irrelevant alarm, due to the signal malfunction.

A such kind of processing allows to avoid a great amount of alarms, mainly in case of loss of electrical power supplies, and by the way, to show only relevant alarms to the operators.

2.2.2 Functional Validation

The functional validation allows to inhibit the "normal alarms" or the ones which can be hidden by an other one.

Some examples can be chosen to explain what we call "normal alarms". When a pump is stopped manually, it is absolutely normal that the pressure and the flow decrease to zero and in many times, in current alarm systems, alarms are generated because the designer wanted to secure the circuit of the loss of circulation. These such kind of alarms are inhibited on N4. Of course, if the pump fails and is not stopped manually by the operator, we have to determine which alarm is the most relevant from a functional point of view (for example, it is preferable to present the initial cause of the pump failure rather than the loss of flow).

2.2.3 Situation Validation

The plant situations are used to validate alarms. They are used to reduce the number of alarms displayed to the operator, so as to enable him, as much as possible, to analyse only those alarms which are really significant with respect to the current plant situation. An alarm can be validated by several plant situations and can have a different importance in each of these situation. An alarm not validated by a plant situation is not displayed to the operator. An alarm validated by a plant situation is displayed to the operator with the gravity defined with respect to the operating situation.

2.3 Alarm Classification

The N4 alarms are separated in four different categories, depending of the available time to act after the occurrence of the default. The available time depends itself of the location of the actions (e.g., main control room, turbine hall, ...).

For example for an action needed in the main control room:

- between 5 to 15 minutes, the colour will be red,

- after 15 minutes, the colour will be yellow,
- between 0 to 5 minutes, we suppose that the operators will not have sufficient time to act, the action is automated and a white alarm is sending as report,
- immediately, it is an automatic plant protection and the colour is green.

For the red and yellow alarm a sub-classification exists, the gravity classification:

- red or yellow level 3 signify that if nothing is done, we will have, at least, material failure,
- red or yellow level 2 signify that if nothing is done, we will have, at least, plant protection, e.g. reactor trip,
- red or yellow level 1 signify that if nothing is done, we will have, at least, safeguard protection, e.g. safety injection initiation.

The gravity classification is dynamic and depends of the plant situation. For example, one alarm can be classified red in one situation (e.g. hot shutdown), yellow in an other (e.g., incidental situation), and does not exist at all in a third one (e.g.; cold shut down).

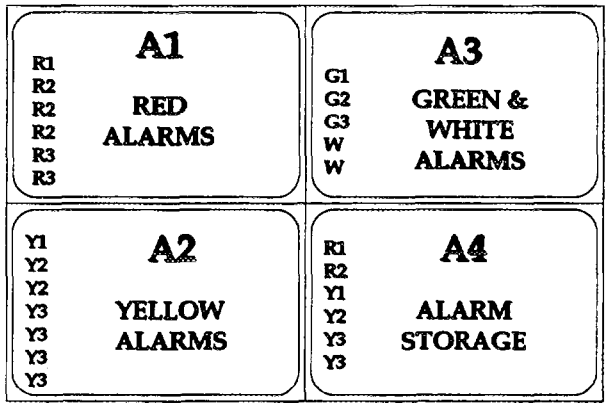
Only for alarm screens are sufficient to present the alarms to the operators:

- one for red alarm apparition,
- one for yellow alarm apparition,
- one for green and white alarm apparition,
- the last one is used for store the ancient red and yellow alarms, already treated by the operators, and for which the default is always on. It allows to clear the alarm apparition screens and discriminate easily the new one from the others.

The basic presentation of the alarms on the screen is not by chronology but by gravity. The first alarm of the list is always the most serious alarm of the plant in the current situation.

Of course, it possible for the operators, in real time, to obtain other presentations lists of the alarms on one operating screen:

- by chronology,
- by category,
- extract the alarm of one dedicated system of the plant,
- the list of the inhibited alarms,
- the list of the modified alarm by the last situation modification.



2.4 Alarm Dialogue

In the main control room, four operator workstations are provided. Two operator workstations are devoted to the 2 main operators, in charge of the control and monitoring of the plant. The 2 other are for the supervisor and for the safety engineer. As these persons need only to monitor the plant, all the operating dialogues are locked on their workstations (e.g. plant control or alarm acknowledgement). Of course in case of failure of one of the workstations of the two main operators, operating controls can be unlocked on the supervision workstations.

The two operating workstations allows the same possibilities the alarms management, but it is possible to specialise them on operator request.

There are three families of alarms:

- primary alarms, which interest mainly the primary operator,
- secondary alarms, which interest mainly the secondary operator,
- general alarms, which interest the both operators.

It is possible on a workstation to visualise any kind of the three families and the visualised ones, to have, or not the possibility to manage them.

The alone obligation for the operators is to visualise and manage at least all the three families on the two workstations together.

This has been an important result of the evaluation phases made on simulator to allow flexibility in term of dialogue and management for the two operators.

The operators are able to decide themselves to acknowledge and/or to store and/or to manage all the visualised alarms with the less level of rigidity of the dialogues as possible (e.g., call an alarm sheet without acknowledgement, or store an alarm without asking the alarm sheet,...). That was an important demand of the operators within the evaluation tests to be able to do what they would like because there is not one model of operator and there is no two similar situations.

2.5 Alarm Presentation

For any dedicated causes of failures, there is an alarm and all alarms have their own alarm sheet. This allows to present on the alarm sheet, the most precise procedure to follow for each case of event.

When there is redundant or identical files, there is one alarm (and one alarm sheet) for each file, and in case of a same fault on all the different files, one synthesis alarm for the all the files is generated and all elementary alarms are inhibited by the synthesis alarm.

Each alarm sheet presents:

- the elaboration of the alarm,
- the causes of the failure,
- the risks, and
- the procedure to follow.

Furthermore, the alarm sheet presents all the information and component needed by the associated procedure to allow a quick and appropriate response of the operators. Of course, if the operator need more information, links are provided to the other operational displays.

When the required actions are only "apply the procedure XXXX", at that time the alarm sheet is not presented and the operator have direct access to the procedure.

3. FUTURE EVOLUTION OF THE ALARM PROCESSING FOR THE NEXT DESIGN

The main features of the N4 alarm system reside in the availability to suppress non effective alarms for the operation. The number of presented alarms is between five to ten time smaller than on the previous plants.

But, up to now, the alarms are always separated from the other operating means (as displays or procedures), and the alarm management is an tedious task for the operators, mainly in case of complex events.

An important effort of research is undertaken in EDF, for the design of the future plants, to try to deeply integrate alarms within all these operating means.

3.1 General Design Aspects

The alarm system and the plant information structure is totally redesigned in order to determine in real time basis the incidence of any occurrence of one or several alarms on plant and present to the operator:

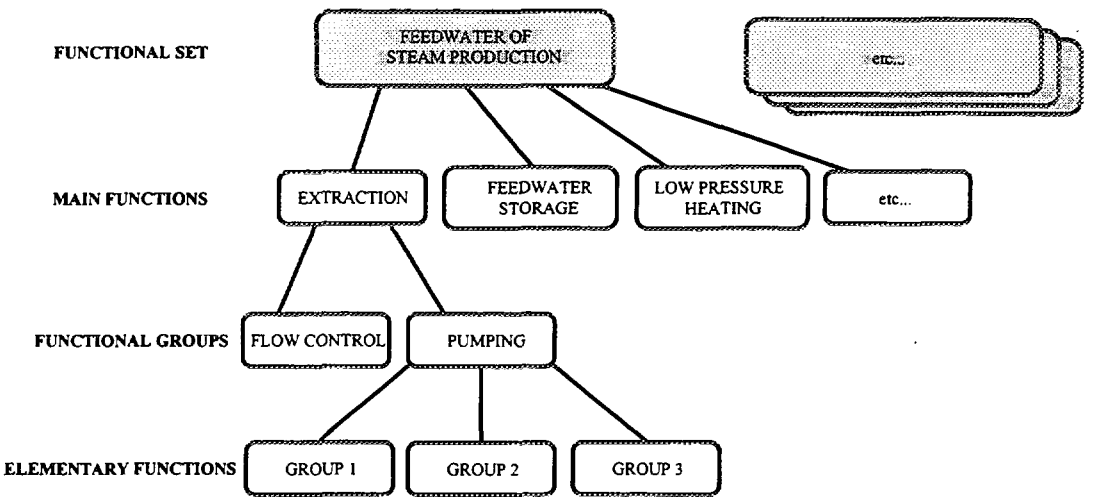
- the final consequence,

- the safety margins always available,
- the actions to perform.

The main requirement of the alarm system is that it should be the more consistent with the other operating means and should have the minimum impact on the management, by the operator, of all his means.

All the plant is functionally shared into 12 functional sets representing global operating functions (e.g. heat production, heat transfer.).

These functional sets are themselves split into main functions, themselves into sub-functions until elementary functions (as pumping group for example).



Functional Breakdown Philosophy

By this breakdown, we describe all the functions needed to achieve, in all circumstances, the operation and monitoring of the global functional sets.

All the functional relations have to be described in order to determine, for any situation, the needed elementary functions necessary to achieve the goals of the upper functional group. This allows to calculate the impact, on the upper functional group, of an event on an elementary functional group.

A such kind of technical description is needed for any functions, at all the different levels.

All the alarms relevant to an elementary function is analysed to determine his own level of severity in regard on the availability of this elementary function. Only three level of severity are sufficient:

- level 1, red colour, for total lost of the function,

- level 2, yellow colour, for severe failure but the function is always is service but degraded,
- level 3, white colour, for minor problems.

A special functional processing has been designed in order to determine, in real time basis, the incidence of elementary alarm on the upper functional levels.

The alarms are presented on lists, according to their severity classification for the whole plant, but not only. They are also presented in the operating displays, at each functional level, near the functions or components, by symbols according to the three levels of severity of the event on the dedicated function or component.

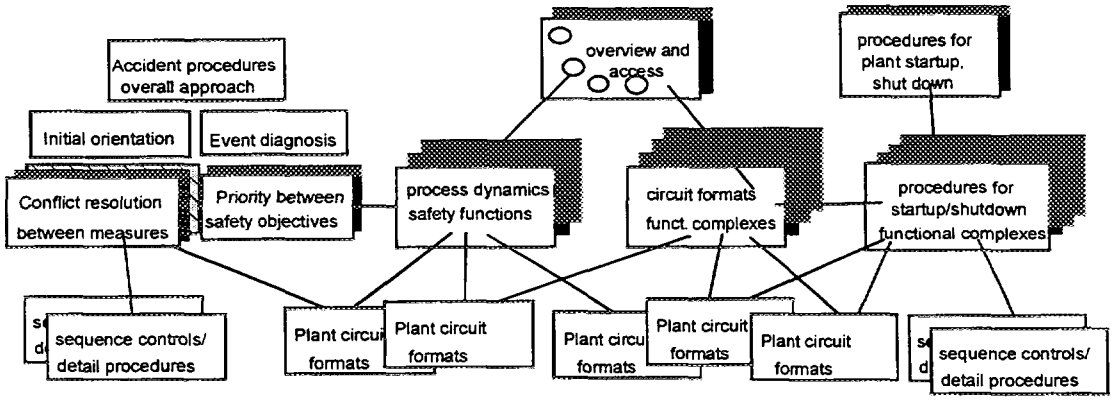
3.2 Displays Structure

One display presents all the information relative to the whole plant in an optimal way and is named the overview display.

The overview display is intended to be permanently on screen because it gives the global state of the plant and have a fixed display layout for keeping the spatial allocation of the information.

This allows to present to the operators, on the overview display the real incidence, for the whole plant, in terms of plant availability and safety incidence, of any elementary or combination of alarms.

A set of displays presenting supportive and complementary information to the overview display are needed and classified in two different classes, one mainly circuit oriented, the other safety function oriented. By definition, the overview display is intended to be sufficient for the operator to monitor all the plant, in all situations and also during time-critical conditions and determine the severity of any alarm and combination of them. The other displays are used to understand more in detail the origins and causes of occurring events, and for diagnosis.
All the displays are functionally designed.



Displays and Information Structure

By selection of a function representation on screen, the operators are able to obtain:

- a dedicated list of alarms relevant to the function,
- an access to the alarm sheets or procedures,
- an access to the sub-levels of functions in order to analyse the origins and send appropriate actions,
- an access to the upper-levels of functions in order to analyse the consequences on the whole plant.

XA9744364

DEVELOPMENT OF THE NEWLY ADVANCED ALARM SYSTEM FOR APWR PLANT

Manabu Shimada, Yoshihiro Yamamoto, Mamoru Tani and Shuichi Kobashi
Kansai Electric Power Co.,
Osaka, Japan

ABSTRACT

We have been developing AMCB (Advanced Main Control Board) for APWR consisting of a large overview display and an operator console. We have adopted the alarm prioritizing functions, which are already in use in the existing Japanese PWR plants, for easier identification of the high priority alarms. Moreover, we have developed an alarm system with a large overview display, which presents alarms on the plant process flow diagram. This enhances the location aids and pattern recognition in the alarm identification process. This time, we made further improvement and studies for better and various functions combining a large overview display with a CRT display. We determined the alarm system specification as follows, taking account of flexible alarm recognition processes.

(1) The high priority alarms can be identified upon the LOD (large overview display). On the display, the alarms are described on the plant flow diagram, and the alarm status is shown on the fixed position of process or equipment symbols.

(2) Other alarms are identified on large overview display and on CRTs using a hierarchical process.

(3) The alarm messages are divided into 4 different groups according to the plant systems, thus enabling to undertake the countermeasure operations, using only the CRT.

Moreover, we integrated a computerized ARPs (Alarm Response Procedures) into the alarm system.

1. INTRODUCTION

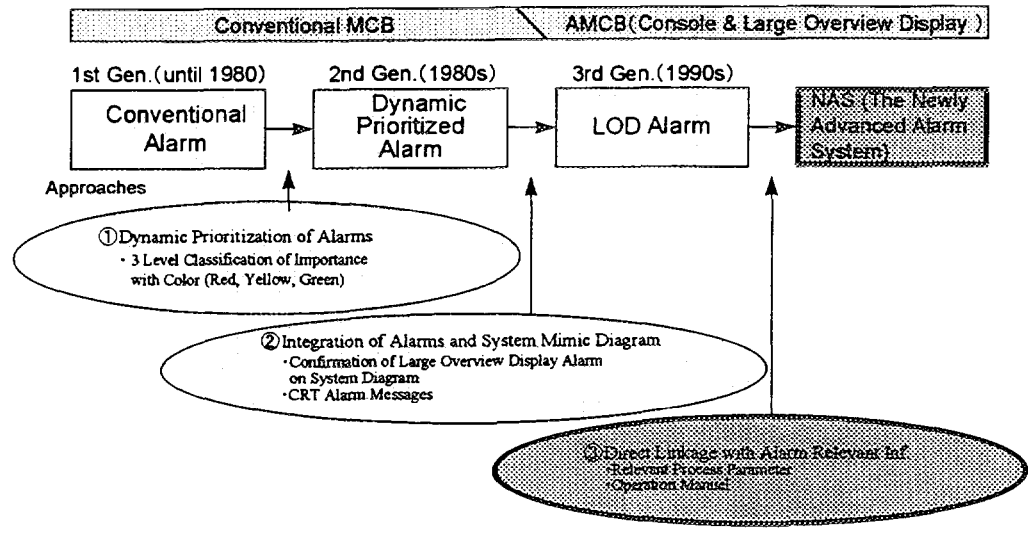
Compared with the conventional alarm display system with the hardware alarm tiles and the textual alarm messages on CRTs, the alarm display system with a software operation panel gives a substantially larger flexibility of designing. Consequently, many types of alarm system have been so far developed and proposed. We must deliberate to set the most optimum specifications for our purpose.

In this context, in developing the alarm system, adding to the possible approach by the improvement of the conventional systems, we have to pursue the optimization of software alarm specifications to the inherent requirements of the alarm functions. Also, we may have to take into consideration preservation of the traditional design philosophy and the skill of operators.

Bearing that in mind, we have developed NAS (the Newly Advanced Alarm System) for the APWR power plant. The development has been made in a close collaboration between the Japanese PWR utilities and the MITSUBISHI Group.

2. HISTORY OF DEVELOPMENT

The evolution of the alarm system of the PWR plants in Japan is shown in Figure 1.



Evolution of the Alarm System

2.1 Conventional Alarm System

The alarm system of the conventional MCB consisted mainly of the hardware alarm tiles. Its principal technology reposed on the alarm grouping and the rules of the alarm tiles arrangement in order to take advantage of so-called location aid and pattern recognition.

2.2 Dynamic Prioritized Alarm System

Although high availability of the plants has been maintained in Japan with the conventional alarm system, the accident of the TMI-2 revealed that too many alarm activating at the same time have the operators overburdened with alarm recognition. As a result, the system needed improvement.

The main purpose of the development was to avoid that any important alarm should be overlooked, and the alarm prioritizing technology was the main view point of the alarm system. In consideration that it was necessary to keep the number of the alarms within a range where operators can recognize all the high priority alarms, the developed system was based upon the following rules:

(a) Prioritization of alarms with multi-setpoint relationship

When an alarm with higher setpoint level is activated, alarm messages at lower levels are no longer considered.

(b) Prioritization by cause-and-consequence relationship between alarms

When "Charging Pump Trip" alarm is activated, Charging pump outflow is decreased. In this case, the cause alarm "Charging Pump Trip" is set as a high priority alarm and the consequence alarm "Charging Pump Outflow Low" is set as a low priority alarm.

(c) Prioritization according to the operation mode

An alarm related to the process parameters and an equipment of the system not in use is not considered as a highest priority alarm.

While the Reactor is in trip, "Control Rod at Reactor Bottom" alarm is set as a low priority alarm.

With those prioritization logic processing's, the alarms are categorized into the 3 priority levels; the highest priority is attributed to red, then yellow, and the lowest is to green. This clarified the high priority (red) alarms to which the operators must response. At the issue of the evaluation operation, the operators recognized the improvement, particularly in the higher detection rate of secondary failure.

2.3 Alarm System of the AMCB Using Large Overview Display

We have already developed AMCB for APWR. In this development, we established an alarm system with a hierarchical alarm recognition process, mentioned as follows:

(a) Recognition of alarm activation on the large overview display

(b) Identification of detailed textual alarm messages on CRTs of the console

Taking account of that the conventional alarm system relies largely upon the pattern recognition effect of the alarm tiles arrangement, we have aimed to enable an more instinctive and direct identification of the location of the alarm, making use of the integrated display of the plant system diagram and the alarms.

At the same time, the alarm system displays alarms categorized according to the priority level on a CRT. Categorization is carried out likewise mentioned above (2).

The validation test proved that the alarm system applied to AMCB enables higher recognition capacity of the alarms than the existing alarm systems. The questionnaire to the operators, however, revealed that there remain still several problems to be resolved.

3. PROCESS OF DEVELOPMENT

The present development has been carried out with the purpose of bringing solution to the alarm problems of AMCB. In developing the new system, we set the basic design principle based on the search of the solutions to the problems, extraction of the improvement items from the present alarm system specification, operator needs, and analysis of the requirements to the alarm system. Furthermore, we have conducted static and dynamic validation test before setting the final specifications of NAS.

4. EXTRACTION OF THE IMPROVEMENT ITEMS

4.1 Analysis of the Improvement Items for the Alarm System of AMCB

The following problems have been extracted throughout the validation tests.

(a) Alarms on the large overview display enable easier recognition of the defective part location, but it is difficult to identify specific alarm context.

(b) It is difficult to find the detailed corresponding alarm on the CRT to a group alarm on the large overview display. Therefore, it is required that the precise alarm message on the CRT is identified smoothly after recognition of the group alarm on the large overview display is required.

(c) Some reinforcements of operation support function after alarm recognition are required.

4.2 Inquiry to the Operators on their Needs and its Analysis

Prior to undertaking the new development, we have conducted inquiries to the operators on their needs in regard to the alarms. As a result, we have ascertained, as it had been pointed out before, continuous display of the alarm tiles and the maintenance of pattern recognition effect with the display position. Also, we have made sure of their needs for further decrease in number of alarms and in display of ARPs at alarm activation.

5. REQUIREMENTS

Admitting that the basic function of alarm is to alert the operators that some event has occurred, we have to put into place a more complete system which can play adequate roles in accordance with the process of operators actions at alarm activation along with each of the following phases:

1. Detect of anomalies and alert the operation crew
2. Inform about the priority and the situation
3. Guide the operation response
4. Confirmation of recovery

In this process, easy detection of anomalies is important not only for the primary failure but also for secondary failures. In developing this system, we have conducted thorough studies in order to meet the above requirement to provide the most adequate information for each process. Also, we have endeavored to have the improvement items and the needs of the operators reflected.

6. BASIC DESIGN PRINCIPLE

6.1 Detection of Anomalies

(a) Recognition of alarm

We have adopted the alarm display system taking full advantage of a large overview display, intending to make easier the recognition of alarm location and to alert the whole operation crew to the alarm. For this purpose, display of the alarms is integrated with the plant process flow diagram on the large overview display. The alarms which are not categorized to the alarms on the diagram are grouped otherwise.

(b) Detection of secondary failure

We have intended to make easier the detection of secondary failures even when many alarms are being raised. In order to make it easier, we have the following ways of detection:

- Direct detection: automatic checking of the inter-lock actuation
- Indirect support: reduction of the operators' burden in the alarm recognition by reducing the number of the alarms with the alarm prioritization

Direct Detection of Secondary Failure

We have focused upon the serious failures which may affect the safety and the operation of the plant and upon those for which we can precisely define the extent of support. In this meaning, we have set our target on the misfunction and malfunction of the equipment related to the reactor protection system and engineering safety features.

We decided to display together, for facilitating a secondary failure detection ,with a "OK" or "NG" status information on the screen being checked the integrity of the alarm related interlock actuation by the computer. We have added new alarm items, such as "Malfunction of Control Rods at the Reactor Trip".

Indirect Support

We have reinforced the alarm prioritization in order to reduce the number of alarms that require some countermeasures. At the same time, the alarms are categorized into some groups with the view to reduce the burden of alarm recognition. However, since a complicated alarm prioritization logic may lead to increase the cognitive burden, we are

adopting only those which are simple and comprehensible and give a single and clear reply.

In order to reduce the human error probability, we have set target to provide less than 10 alarms in each group in view of easier search of information from the alarm list on a CRT.

6.2 Identification of the situation

For the purpose of easier identification of the situation at alarm activation, we have integrated the alarm related information. Also, for the request of further detailed information, we made the most adequate allocation of the CRT displays corresponding to each alarm item.

(a) Provision of complementary information

As complementary information related to the alarm, we decided to add the process values of the alarm parameters and their trends to the alarm all the time.

(b) Request for related CRT screens

With a view to allowing a smoother shift to the precise plant status recognition at alarm activation, related screens can be called with a one-push request on alarm messages. Operators can get CRT displays both for process status recognition and interlock and system status recognition by touching the related area of the alarm message on the display.

(c) Some reinforcements of operation support function after alarm recognition are required.

6.3 Countermeasures

We have provided easy access to ARPs in order to ensure the appropriate countermeasures to the activated alarm. By touching the alarm name on the screen, operators can request corresponding operation procedures. It makes sure, completing the memory of the operators, that no part of the necessary measures should be neglected and that the operation should be conducted perfectly in conformity with the operation procedures.

In addition to the request for ARPs corresponding to alarms, we have provided also functions to proceed to one-push request for the emergency operation procedures which may be required next when the accident countermeasures would have to be faced in place of the alarm response. Such support information can be afforded as a part of integrated manual, covering all along the countermeasure process even if the failure should develop into an accident.

6.4 Confirmation of Reset

In order to proceed to confirmation of reset after successful completion of the corresponding countermeasures, we have provided specially a reset alarm display.

7. ALARM DISPLAY SYSTEM

In accordance with the above-mentioned design principle, we have established the alarm display system described below.

(a) Alarms on the large overview display

- With a view to taking an efficient advantage of the large overview display, alarms are shown, making use of its great features of continuous display and of location aided information.

- Integrated display of the plant flow diagram and the alarms, for easier instinctive recognition of alarm location and plant status.

- Display of all the alarms by hierarchical classification according to their priority.

  a. Important alarms are shown individually with a partly adjustable display for easier recognition.

  b. The other alarms are displayed by group alarms, of which the precise identification can be made on a CRT in a hierarchical process.

- Visual confirmation of the alarms according to their priority.

  a. Important alarms are located on the upper part of the display, with the most important ones on the top. Size of the characters is optimized in consideration of their readability. First Out (F.O.) alarm is indicated on the top of the display in large characters.

  b. The alarms other than F.O. are displayed in admissibly small characters, considering that the volume of the displayed information and the size of the characters are in relation of trade-off and that the operators are expected to comprehend its content, thanks to the fixed location display.

(b) CRT alarms available at the operation console

- For the purpose of easier alarm recognition and their management, the alarms are categorized into 4 groups according to plant system and their priority, i.e., 2 groups of the primary system, each group of turbine system and electric system.

- With the dynamic suppression of alarms and the unification of the alarm messages, the number of alarms is reduced in a range where the operators can recognize them easily (about 10 alarms for each group).

(c) Combination of the large overview display and CRTs

- For the purpose of operating the displays together in the most appropriate way, the entries and the paths are designed in a flexible way so that they can be used in a way as it may be judged good by the operators depending upon the situation.

(d) Provision of ARPs

- For the purpose of making sure that the appropriate countermeasures should be taken further to the alarm, we integrated the alarm response procedures into the computer software. We took into consideration easy revision management of the procedures (prevention of double management of the data base) and maintenance of the conformity of the procedures. In this meaning, we adopted the basic principle of direct procedures display and of unified data base management.

(e) Coding of the alarm sounds

- We have set coding of the alarm sounds with their frequency and the length of their repetition period, according to the systems concerned and the category of the alarms such as F.O.

8. DISPLAY METHOD OF ALARM

Optimization of the alarm colors must be made in such a way to prevent that the alarm should be overlooked. For this reason, it is evident that highly eye-catching colors which are distinctly discernible from each other must be chosen. Also we must avoid the colors which would cause visual fatigue of the operators who keep watching for a long time.

For these reasons, we have chosen gray back-ground taking account of harmony with the conventional alarm colors and operators' familiarity with some colors used for a long time. The selected three colors are as follows:

(a) Alarms which require operators' response: red
(b) Alarms which require operators' confirmation due to the interlock system actuation etc. to the alarm: yellow
(c) The other alarms prioritized by the preceding alarms ((a) and (b)): green

The new alarm system CRT screen is shown in Figure 2.

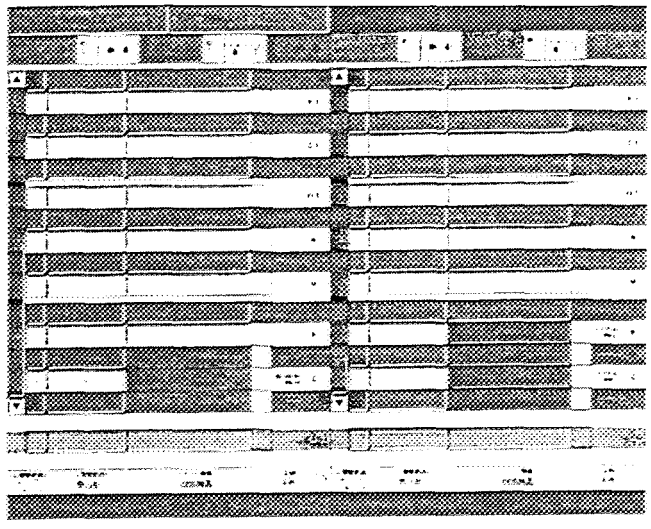


Figure 2: Display Format of New Advanced Alarm System

9. STATIC VALIDATION AND REFLECTED ITEMS

Based upon the specifications established at the design room level, a mock-up was made for the operators' evaluation.

10. PROTOTYPE SYSTEM FOR VALIDATION OF THE FUNCTIONS

We have built a prototype system in order to validate NAS throughout dynamic simulated operation. The characteristics of the prototype are described hereunder. The prototype system consisted of a large overview display, CRTs and AMCB, necessary for NAS. It was coupled with a full scope simulator which simulated a Japanese standard 4 loop plant.

Validation installations built for the above purpose are described in Figure 3.

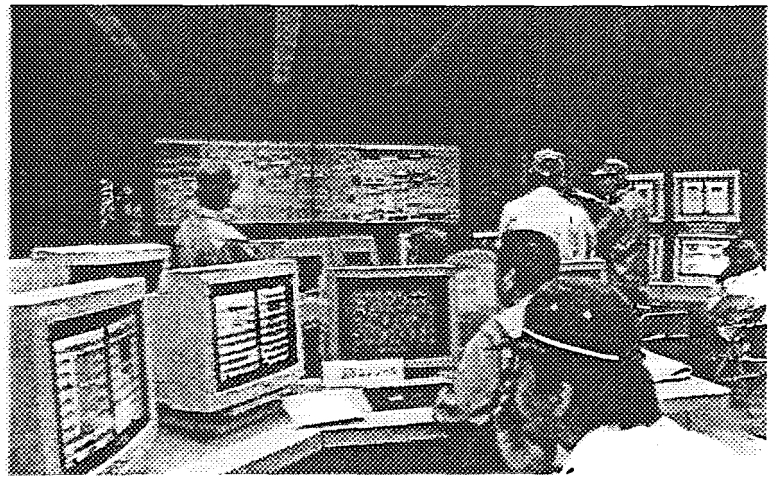


Figure 3: Prototype System for Validation Test

11. DYNAMIC VALIDATION TEST AND THE IMPROVED ITEMS

11.1 Validation Method

Since the newly developed system leads to substantial improvements of alarm recognition process and of the monitoring operation sequence such as the procedures to shift to the monitoring operation, wide range evaluation works, inclusive of the operators' subjective evaluation and quantitative evaluation of the operability with NAS, have been required. For this purpose, we have conducted the following validations.

(a) Validation of the user's acceptance

We have made a questionnaire to the operators in order to verify if they had felt that NAS was easily operable and if the basic specifications had been considered acceptable by them subjectively.

(b) Validation of the system performances

In order to verify if the newly developed alarm system fulfills the expected improvements as compared with the conventional systems in performing the tasks of recognition, confirmation and treatment, we have conducted the following variation works and confirmed that the designed performances are attained quantitatively and that the intended improvements are proven.

- Number of alarms transmitted and the suppression rate
- Request sequence of the related information

(c) Validation of the operators' performances

In order to verify if operators performances in carrying out the necessary measures are improved further to the improved performances of the alarm system itself, inclusive of the higher secondary failure detection rate, we have conducted validation on the following items.

- Detection time of secondary failure
- Utilization rate of the alarms
- Work load reduction rate(NASA-TLX method)

11.2 Results of the Validation Test

Dynamic operation validation with simulator confirmed the improvement effects as compared with the conventional alarm system. On the other hand, with regard to the subjects on which the operators made valuable comments, we have established improvement scheme which shall be integrated in the final specifications of NAS.

(a) The user's acceptance

The results of the questionnaire are shown in TABLE I. It was confirmed that NAS had been accepted by the users.

Table 1: Results of User Questionnaire

Alarm Confirmation Process	Improvement Items	Rate of "Effective/Rather Effective"
Detection Recognition	Large Overview Display	Alarm Detection on LOD 100%
	Simplification of Confirmation Process through Group Alarm (Large Overview Display)/Individual Alarm (CRT)	Total Plant View 75% Grouping in accordance with Importance 70% Alarm Detection from Alarm CRT 100%
Confirmation	CRT	
	Facilitation of Secondary Malfunction Detection	Secondary Malfunction Detection with 'OK Monitor' 95%
	Facilitation of Transition to Monitoring/Operation	Operation CRT Request 100%
Corrective Action	CRT	ARPs Request 100% (Single ANN)
	Display Format	Improvement of Visibility 66% (Positive Display, Half-tone)

(b) The system performances

- Number of alarm activation and prioritization rate

We confirmed that the number of alarm activations was within 1 page for every group, mostly under 10 activations.

Also, we are now sure that an adequate unification of the alarms will allow to further decrease the number of alarms.

As a conclusion, the objectives of our design are achieved.

The prioritization rate has been improved compared with that of the conventional system further to the enlarged application range of the alarm prioritization logic. Number of activated alarm is described in Figure 4.

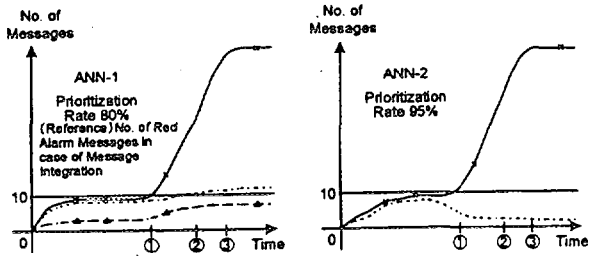


Figure 4: Number of Alarm and Suppression Rate

- Request sequence

Validation of the real information response time during the operation allowed to confirm that the shift to the monitoring operation from the alarm is made smoothly. High efficiency was proved through analysis of the request sequence based upon the operation log and the evaluation by the operators answering to our questionnaire. Variation results are shown in TABLE II and TABLE III.

Table 2: Related Information Request Function Utilization Rate

Malfunction	Alarm	Rate of design base request sequence
1. B.O	Charging pump auto start-up failure	70%
2. Reactor Trip	Two rods stuck at the Reactor trip	80%
3. PSS failure	PSS failure	50%
4. RCP failure	RCP stand pipe water level high	70%

Table 3: Alarm Response Procedures Utilization Rate

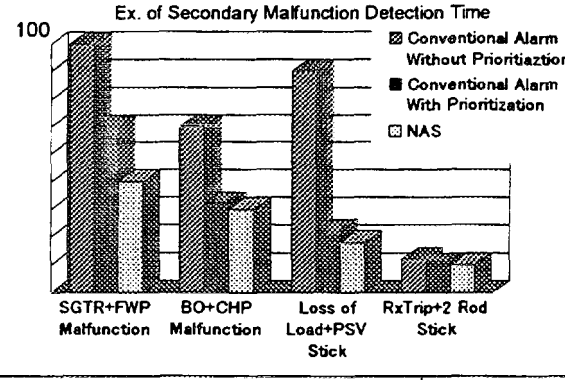
malfunction	Operator	Shift-supervisor
Single alarm event	100%	100%
Multiple alarm event	29%	53%

(c) Operators' performances

- Detection of secondary failure

During the dynamic validation, in addition to the basic event such as SGTR and BO etc., we have simulated secondary failures such as defective isolation of the feed water, etc. and we measured detection time by the operators. As a result, we confirmed a shorter detection time compared with the conventional system. It proves that we can expect to carry out very rapidly and surely the necessary operations. Validation results are shown in TABLE IV.

TABLE 4: Detection Time of Secondary Failure



a. Secondary Malfunction Detection Time	Approx.20% Reduction
b. Secondary Malfunction Detection Time Variation	Approx.20% Reduction
c. Alarm Usage Rate	Multiplied 1.7-fold

- Work load reduction rate (by NASA-TLX method)

  By means of the NASA-TLX method, we tried to evaluate the work load and to determine, by relative comparison with the conventional alarm system, reduction rate of the work load. As a result, we confirmed that the total work load had been lower. Validation results are shown in TABLE V.

Table 5: Reduction Rate of Operator's Workload

	Conventional Alarm System	New Advanced Alarm System
WWL	63.7	47.0
WWL Reduction	26% Reduction	

WWL: Weighted Work Load

12. CONCLUSION

We introduced in this paper the history of the development and application of the alarm system in Japanese PWR plant, and the development of NAS together with the validation results as the results of our latest development.

Since the alarm system performs important functions for the security and stable operation of the plant, we continue to integrate the results of our development into the commercial plants and to pursue improvement.

VALIDATION OF THE COMPUTERIZED ANNUNCIATION MESSAGE LIST SYSTEM (CAMLS)

M.P. Feher, E.C. Davey, and L.R. Lupton
AECL, Chalk River Laboratories
Chalk River, ON

ABSTRACT

The Computerized Annunciation Message List System is a computerized annunciation system for the control rooms of nuclear generating stations. CAMLS will alert operators to changes in plant conditions that may impact on safety and production and help staff to effectively respond. CAMLS is designed to:

- *provide a clear and concise overview of the current problems or faults in the plant,*
- *provide an overview of the current state of the plant in terms of automatic process and equipment actions,*
- *provide support for specific operational tasks, through either pre-configured or operator-configured annunciation displays, including:*
  - *rapid and efficient upset response,*
  - *plant stabilization,*
  - *problem diagnosis,*
  - *recovery action planning and implementation, and*
  - *rapid recovery from trip and return to power operation.*

To achieve this, several information processing, presentation, and interaction concepts were developed including:

- *Alarm Processing Concepts/Features*
  - *definition of plant state (operating regions)*
  - *prioritization based on plant state*
  - *alarm conditioning based on plant state*
  - *reduced volume through improved utilization of information*
  - *new types of alarms*
- *Alarm Presentation Concepts/Features*
  - *separation of faults (problems) and status messages into separate displays*
  - *ordering faults by order of priority*
  - *colouring messages by priority*
  - *retaining fault messages until fully acknowledged and returned to normal*
  - *backshading unacknowledged alarms (new and return-to-normal)*
- *Alarm Interaction Concepts/Features*
  - *single key acknowledge/reset*

- *single tone on initial alarm occurrence*
- *auto acknowledge for status messages*

The result is that CAMLS:

- *prioritizes relevant alarm data according to the consequence to the plant and the urgency for an operator response,*
- *adjusts the alarm presentation and priority with variations in the operating state of the plant,*
- *significantly reduces irrelevant alarm messages without losing key information,*
- *improves operator accuracy and speed of diagnosis and planning by providing organized information, and*
- *prevents distraction from important operational activities through less intrusive and demanding operator interactions.*

CAMLS has two distinct components–two central overview displays and a desktop inquiry system (annunciation interrogation workstation, AIW).

These new design concepts for CANDU annunciation have been developed, prototyped, and evaluated. As part of a CANDU Owners' Group (COG) R&D project, CAMLS has been assessed for operational performance over several upset scenarios in full scope simulators for two different operating CANDU stations. A formal validation process was used to arrive at statistically valid statements of comparative system performance between the current CANDU annunciation systems and CAMLS. The evaluation clearly establishes that CAMLS improves operator performance for most operationally significant tasks involving annunciation compared to existing CANDU annunciation systems. The implications of these improvements on safety margins, production costs, and human performance are significant. This paper will summarize these activities and report on validation findings.

1. INTRODUCTION AND BACKGROUND

The Computerized Annunciation Message List System is a computerized annunciation system for the control rooms of nuclear generating stations. CAMLS will alert operators to changes in plant conditions that may impact on safety and production and help staff to effectively respond. CAMLS is designed to:

- provide a clear and concise overview of the current problems or faults in the plant,
- provide an overview of the current state of the plant in terms of automatic process and equipment actions,
- provide support for specific operational tasks, through either pre-configured or operator-configured annunciation displays, including
  - rapid and efficient upset response,
  - plant stabilization,

- problem diagnosis,
- recovery action planning and implementation, and
- rapid recovery from trip and return to power operation.

To achieve this, several information processing, presentation, and interaction concepts were developed including:

- Alarm Processing Concepts/Features
  - definition of plant state (operating regions)
  - prioritization based on plant state
  - alarm conditioning based on plant state
  - reduced volume through improved utilization of information
  - new types of alarms
- Alarm Presentation Concepts/Features
  - separation of faults (problems) and status messages into separate displays
  - ordering faults by order of priority
  - colouring messages by priority
  - retaining fault messages until fully acknowledged and returned to normal
  - backshading unacknowledged alarms (new and return-to-normal)
- Alarm Interaction Concepts/Features
  - single key acknowledge/reset
  - single tone on initial alarm occurrence
  - auto acknowledge for status messages

This paper summarizes the formal evaluation of the COG CANDU annunciation message list system (CAMLS). The evaluation clearly establishes that CAMLS improves operator performance for most operationally significant tasks involving annunciation compared to existing CANDU annunciation systems. The implications of these improvements on safety margins, production costs, and human performance are significant.

2. SCOPE OF THE EVALUATION

Validation can be applied at many levels of detail and at various times during the development, design, and implementation cycle. This validation effort represents a comparative test of the system performance with certain changes to annunciation message lists. Although the tests were performed on a CANDU 6, specifically Point Lepreau GS in New Brunswick, and the Darlington CANDU (4 x ~900MW units CANDU station) it is anticipated that the results are equally applicable to any other CANDU or almost any other nuclear power plant in the world.

The validation activities from 1994 through 1996 included three experiments. All experiments were a validation of the effectiveness of different components of the CAMLS annunciation system compared with similar components in the CANDU design for host station. Experiment 1 focused on the validation of the CAMLS' central annunciation at the Point Lepreau station in 1994/95. Experiment 2 focused on the validation of the Annunciation Interrogation Workstation

(AIW) at the Point Lepreau station in 1994/95. Experiment 3 focused on the validation of the CAMLS central annunciation at the Darlington station in 1995/96.

2.1 Objectives Of The Validation

The overall objectives of the COG CAMLS validation program for both the 1994/95 and 1995/96 fiscal years were to:

- perform validation and evaluation trials of various elements/concepts of the new annunciation strategy,
- incorporate feedback from the validation and evaluation trials to make further improvements in CANDU alarm annunciation,
- investigate and provide recommendations on the integration of the various annunciation facilities into existing station environments,
- establish benefits and risks of a specific configuration prior to implementation of design changes, and
- reduce the regulatory risk of a retrofit to existing stations.

The specific objectives of the different experiments were:

- Experiment 1 - Central Alarm Message Screens at Point Lepreau
  - assess CAMLS effectiveness in supporting upset operations associated different complexities of upset events,
- Experiment 2 - Annunciation Interrogation Workstation at Point Lepreau
  - assess the CAMLS AIW effectiveness in supporting specific operator tasks associated with upsets as well as some normal operations,
- Experiment 3 - Central Alarm Message Screens at Darlington
  - assess CAMLS effectiveness in supporting normal and abnormal operations associated with station startup and outage management, thereby ensuring that CAMLS is effective over all significant regions of plant operations.
  - assess and identify issues associated with crew usage of CAMLS (e.g., potential changes to crew member roles, communication, operational practices to achieve maximum operational benefits from CAMLS use).

2.2 Types Of Assessment

Both year's validation efforts focused on comparing the existing station annunciation system with the complete CAMLS system concept across several scenarios and operating situations.

2.3 Degree Of Formality

The validation plans and reports included the definition of:

- performance hypotheses,

- design of scenarios to test the hypotheses and/or the selection of hypotheses to test that were compatible with the scenarios chosen,
- measures of performance consistent with the hypotheses,
- acceptance criteria for the measures selected,
- an experimental design that accounted for certain possible confounds, and
- a statistical analysis of the results leading to a degree of confidence in the acceptance or rejection of the hypotheses tested.

3. PERFORMANCE HYPOTHESES

3.1 Identification

A combination of the upset response strategies used at CANDU plants and a decision making model were used to identify possible performance hypotheses.

During the 1993/94 annunciation work, several evaluations were carried out and a number of subjectively based statements of performance enhancement were made by station-based reviewers of the work. These statements were identified and extracted as performance hypotheses to be tested in a more controlled and dynamic setting. In addition, several statements were made by the designers regarding potential performance benefits of the system, and these statements were also extracted and used as performance hypotheses to be tested. Finally, existing station utility staff and design organization staff were polled for input to the kinds of measures necessary to assess annunciation system design. These were then added to the set of hypotheses as appropriate.

In summary, we generated the hypotheses (for the most part) based on a map of operator activities in response to plant upsets.

3.2 Organization

We then provided a framework that organized the hypotheses, first, by the pre-trip and subsequently by stages of the upset response strategy:

Pre-trip
- response to changes in plant state consistent with operational goals,

Post-trip
- execution and confirmation of special safety system functions,
- stabilization of plant processes and systems,
- diagnosis of fault conditions,
- correction of fault conditions, and
- restoration of power production capability.

3.3 Hypotheses Identified

A summary of the hypotheses identified for the experiments is:

- Improved detection of
  - potential alarms conditions before they are alarmed (improved plant state prediction due to improved situation awareness)
  - alarms identifying improperly configured systems
  - alarms not related to a primary event or condition
  - automatic actions
- Improved diagnosis of
  - trip casual factors
  - root causes of upsets
  - current plant state
  - future state of the plant
  - abnormal plant process disturbances
  - safety concerns
  - production concerns
- Improved decision-making
  - for order of priority for response to alarms
  - for procedure selection
- Task specific improvements
  - Reduced access time to alarm comprehension and response information
  - Reduced access time to alarm information.
  - Improved access time to historical information
  - Improved transfer of information during shift change-over
  - less demanding and easier acknowledgment approach
  - reduced demands on user memory
  - improved access to alarm response procedures or alarm detail

The results sections of this paper include the specific hypotheses selected and tested for the various validation exercises.

4. MEASURES OF PERFORMANCE

In deriving measures of performance, Meister [1] outlines a process for the derivation of measures of performance. This process consist of identifying first, mission dimensions; second, selecting a subset of mission dimensions as performance criteria; third, deriving measures for each criteria and finally establishing standards. We have followed a similar outline in identifying dimensions, criteria, measures and standards.

First, we considered what dimensions most directly validated or tested the performance hypotheses previously identified. Some of the dimensions identified were time, errors, and accuracy. These dimensions have been chosen as the criteria because they best reflect overall system performance. The relevance and importance of each potential criterion was assessed by asking how success of or failure of a particular criterion affects system performance. For example, because the NPP is a complex system, reaction time is important for the safe and effective operation of the plant. Thus, reaction time is a important criterion. Since operators

have to perform a variety of tasks or functions, there may be multiple criteria. It is possible that one criterion suggests effective performance and yet another criterion may suggests the opposite. This is understandable since operators may favour performance associated with one criterion at the expense of another to suit the operational goals and situation. In this report, we use the term performance hypothesis as an equivalent to a criterion.

Second, we derived the measures based on the criteria identified. The level of the measures we have derived go in accordance with assessing system's effectiveness.

4.1 Measures Identified

The measures for the experiments were drawn from:

- Subjective - How do you rate the annunciation system's:
    1. ease of use or difficulty for acknowledgment?
    2. ability to keep you aware of the state of the plant?
    3. ability to keep you informed of important alarms independent of the primary upset?
    4. demand on your memory?
    5. ability to keep you informed of the state of the automatic actions during an upset?
    6. support for root cause diagnosis?
    7. ease of access to alarm response procedures?
    8. likelihood of making an error in selecting an alarm response procedure?

- Objective
    1. Early and continuing plant state awareness
    2. Identification of problems
    3. Awareness of plant state trend
    4. Awareness of plant safety concerns
    5. Awareness of plant production concerns

4.2 Methods of Collection

The set of data collection techniques considered for use, and ordered by desirability, included:

- Direct process parameter data from simulator data collection facility
- Direct physical action data from simulator data collection facility
- Post scenario debriefing of subjects
- Post scenario debriefing of subject matter experts
- During scenario questioning of subject matter experts
- Observation of objective issues by subject matter experts
- Observation of objective issues by the validation team.
- Observation of subjective issues by subject matter experts
- Observation of subjective issues by the validation team
- Post scenario debriefing of validation team (observers)

- Scenario interruption and debriefing of subjects
- During scenario recording of "talk aloud" verbal protocols of subjects
- During scenario recording of operator performance and later analysis of recordings post scenario

4.3 Data Collected

For all the experiments, the following types of data were collected:

- Subjective
  - Anchored Subjective Rating Scales
    - Subjects
    - Subject Matter Experts
  - Subject system-comparative questionnaire
- Objective
  - Scenario Specific Measures of Performance

5. PERFORMANCE ACCEPTANCE CRITERIA

The only performance criteria used for all experiments was a measure of effectiveness based on the degree of improvement over the existing designs.

6. EXPERIMENTAL DESIGN

6.1 Experimental Factors

There are three basic types of independent variables [2]:

- System characteristics
- User characteristics
- Environment characteristics

For the purpose of this validation effort we have identified, for the most part, independent variables concerning system characteristics. This is because the purpose is to evaluate the effectiveness of the new annunciation concepts developed in previous years. Independent variables concerning user and environmental characteristics will be considered as appropriate in this validation effort but the emphasis is on system characteristics variables.

Four experimental system factors and one environmental factor have been identified. In addition, each of the factors has a set of basic elements from which to create the factor levels. The factors and their elements are:

- Processing
  - Static Prioritization (Existing Design)
  - Perceive Importance Prioritization (Existing Design)
  - State Conditioning (Existing Design)

  - Minor Alarm Suppression (Existing Design)
  - Mode-based Prioritization (New Concept)
  - Consequence/response prioritization (New Concept)
  - Mode-based Relevance conditioning (New Concept)
  - State conditioning (New Concept)
  - Mode conditioning (New Concept)
  - Event conditioning (New Concept)
  - Coalescing (New Concept)
  - Expected-but-not occurred (New Concept)
- Central Presentation
  - Integrated Fault & Status (Existing Design)
  - Faults & Status by ~Time (Existing Design)
  - Coded Cryptic Text (Existing Design)
  - Colour by System (Existing Design)
  - New change by Flashing 1st char. (Existing Design)
  - Scrolling list of changes (Existing Design)
  - Separate Fault & Status (New Concept)
  - Faults by Priority (New Concept)
  - Status by Time (New Concept)
  - Full Message Text (New Concept)
  - Colour by Priority (New Concept)
  - New Change by shading (New Concept)
  - Active only faults & scrolling status (New Concept)
- Task Specific support
  - Printer (Existing Design)
  - OMs(Section 7) (Existing Design)
  - alarm summary pages (Existing Design)
  - annunciation interrogation workstation (New Concept)
- Interaction
  - Silence (Existing Design)
  - Acknowledge (Existing Design)
  - Reset (all acknowledged) (Existing Design)
  - Two tones horn (Existing Design)
  - Acknowledge Only (Faults) (New Concept)
  - Auto acknowledge of status alarms (New Concept)
  - Single horn tone (New Concept)
- Scenario (A description of the scenarios is included in Appendix E)
  - Loss of Feedwater to Boiler
  - Loss of Class IV Power

For the 1994/95 validation trials, the focus was the effects of system characteristics on subject performance in order to compare the performance of the CAMLS with the existing CANDU annunciation system. The use of scenarios as an independent variable was required to establish

whether the results may in fact be scenario dependent within the scope of scenarios used. As a result, the above points can be simplified in the following manner:

- the system characteristic identified was the type annunciation of system being used,
- the user characteristic was fixed as the licensed operator (senior power plant operator, SPPO, at PLGS and the authorized nuclear operator, ANO, at DNGS) and was the subject in the experiments, and
- the environment characteristic was the scenario used.

The selection of scenarios was based on the authors' experience of plant operations as well as feedback from training personnel from PLGS and Darlington.

For Experiments 1 and 2 at Point Lepreau, two upset scenarios were selected:

- Loss of class IV power (LCIV) due to failure of the system service transformer and a loss of condenser vacuum leading to turbine trip, and
- Loss of boiler feedwater (LOFW) due to the wrong level control valve being removed from service.

The first scenario, ROP was used for training subjects on the CAMLS system. The other two scenarios were used for experimental data collection. These scenarios were believed to represent different levels of complexity in terms of the amount of annunciated information, the number of actions required from the operators, and the seriousness of the transient.

For experiment 3 at Darlington, two simulator scenarios were used:

- Reactor trip and recovery - This involves a heat transport pump trip as the initiating cause for a reactor stepback. Several additional process disturbances and equipment failures have been inserted to provide means for testing the ability of the CAMLS system to make the operating crew aware of the plant configuration and state.

- Reactor startup from outage - This involves a change in heatsink state from shutdown cooling to boilers as the plant is prepared for return to power generation. The scenario involves a 15 minute period beginning just after criticality is reached and ending prior to the heatup of the heat transport and secondary process systems.

6.2 Experimental Levels and Treatments

The levels for each factor were created by the set of permutations and combinations of the individual elements associated with each factor. The total number of possible experimental conditions or treatments for a complete factorial design are too many for the available resources (i.e., the number of subjects needed, the time per subject available, and simulator time). We therefore broke down the validation effort into phases in order to make it more manageable. For phase I (the only currently planned phase) of experiments 1 and 3 (central message list display evaluation), we have selected four treatments from the set of possibilities as noted in Table 1.

Table 1: Experiments 1and 3 - Experimental Treatments

Treatment	Factors			
	Processing	Central Presentation	Interaction	Scenario
1.	New: none Old: Static Prioritization, Perceive Importance Prioritization, State Conditioning, Minor Alarm Suppression	New: none Old: Integrated Fault & Status, Faults & Status by ~Time, Coded Cryptic Text, Colour by System, New change by Flashing 1st char., Scrolling list of changes	New: none Old: Silence, Acknowledge, Reset(faults & status), Two tones horn	Loss of FW to Boiler
2.	New: Mode-based Prioritization, Consequence/response prioritization, State conditioning, Mode conditioning, Event conditioning, Coalescing, Expected-but-not occurred Old: none	New: Separate Fault & Status, Faults by Priority, Status by Time, Full Message Text, Colour by Priority, New Change by shading, Active only faults & scrolling status. Old: none	New: Acknowledge Only (Faults), Auto acknowledge of status alarms, Single horn tone. Old: none	Loss of FW to Boiler
3.	New: none Old: Static Prioritization, Perceive Importance Prioritization, State Conditioning, Minor Alarm Suppression	New: none Old: Integrated Fault & Status, Faults & Status by ~Time, Coded Cryptic Text, Colour by System, New change by Flashing 1st char., Scrolling list of changes	New: none Old: Silence, Acknowledge, Reset(faults & status), Two tones horn	Loss of Class IV Power
4.	New: Mode-based Prioritization, Consequence/response prioritization, Mode-based Relevance conditioning, State conditioning, Mode conditioning, Event conditioning, Coalescing, Expected-but-not occurred Old: none	New: Separate Fault & Status, Faults by Priority , Status by Time, Full Message Text, Colour by Priority, New Change by shading, Active only faults & scrolling status. Old: none	New: Acknowledge Only (Faults), Auto acknowledge of status alarms, Single horn tone. Old: none	Loss of Class IV Power

Where: Old = Existing C-6 Design, New = COG CAMLS Design

Table x: Experiments 2 - Experimental Treatments

Treatment	Factors	
	Task Specific Support	Scenario
1.	New: none Old: Printer, Alarm response procedures, alarm summary pages	Loss of FW to Boiler
2.	New: AIW Old: none	Loss of FW to Boiler
3.	New: none Old: Printer, Alarm response procedures, alarm summary pages	Loss of Class IV Power
4.	New: AIW Old: none	Loss of Class IV Power

Where: Old = Existing C-6 Design, New = COG CAMLS Design

6.3 Experimental Design

6.3.1 Experiments 1 and 3 - Central Alarm Message Screens at Point Lepreau and Darlington

The 2 annunciation systems (COG, Existing CANDU) which were investigated, and the 2 at each station, resulted in 2x2=4 treatments (factors-levels combination). Thus, the experiment was a two factorial (2x2) completely randomized design with repeated measures. Tables 2 and 3 describe the experimental designs used for each of experiments 1 and 3.

Table 2: Experiment 1 - Experimental Design

Annunciation System Design	Scenario Order	Subjects
Existing C-6 Design	LCIV - LOFW	1st half subjects of Group 1
Existing C-6 Design	LOFW- LCIV	2nd half subjects of Group 1
COG CAMLS Design	LCIV-LOFW	1st half subjects of Group 2
COG CAMLS Design	LOFW- LCIV	2nd half subjects of Group 2
Note: LCIV = Loss of Class IV scenario and LOFW = Loss of Feed Water Scenario		

Table 3: Experiment 3 - Experimental Design

Trial 1	Trial 2	Subjects
COG CAMLS Design/Heat Sink Pump Trip	Darlington Design/Heat Sink Transition	1st half subjects of Group 1
COG CAMLS Design// Heat Sink Transition	Darlington Design/Heat Sink Pump Trip	2nd half subjects of Group 1
Darlington Design/Heat Sink Pump Trip	COG CAMLS Design/ Heat Sink Transition	1st half subjects of Group 2
Darlington Design/Heat Sink Transition	COG CAMLS Design/Heat Sink Pump Trip	2nd half subjects of Group 2

6.4 Experiment 2 - Annunciation Interrogation Workstation at Point Lepreau

For Tasks 2 and 4 the following design was used:

The 2 operator support systems (AIW, Current paper-based approach) were investigated, and the LOFW scenario resulted in 2x1=2 treatments (factors-levels combination). Thus, the experiment was an one factorial (2x1) completely randomized design with repeated measures.

Each subject was tested under the LOFW scenario with both systems. Subjects were randomly assigned to two groups. The following table shows the experimental design used:

Table 3: Experimental Design for AIW Tasks 2 and 4

• **Resources Used for Task**	• **Subjects (6 in total)**
• Current paper-based approach	• Group 1 - 3 subjects
• AIW support	• Group 2 - 3 subjects

All other tasks used the following experimental design.

The 2 operator support systems (AIW, Current paper-based approach) were investigated, and the LOFW scenario resulted in 2x1=2 treatments (factors-levels combination). Thus, the experiment was an one factorial (2x1) completely randomized design with repeated measures.

Each subject was tested under the LOFW scenario with both systems. Subjects were randomly assigned to two groups. Subjects in group 1 used Current paper-based approach first and then they use the AIW. Subjects in Group 2 used AIW first and then they used the Current paper-based approach. This was done to minimize any learning effects carry over from using the same scenario. The following table show s the experimental design used:

Table 4: Experimental Design for AIW Tasks 1,3,5,6,7

Resources Used for Task	Subjects (6 in total)
Current paper-based approach	Group 1 - 3 subjects
AIW support	Group 1 - 3 subjects
AIW support	Group 2 - 3 subjects
Current paper-based approach	Group 2 - 3 subjects

7. EXPERIMENTAL PROCEDURE

7.1 Experiments 1 and 3 - Central Alarm Message Screens at Point Lepreau and Darlington

Each subjects session will include, in order, 10 minutes of training in the new system (COG CALMS Design), an experimental trial using the new system under one of the two scenarios (15 min.), a 5 min. simulator reset and data collection in parallel with collection of subjective measures from the subject, an experimental trial using the old system with the other scenario (15 min.), and another 5 min. simulator reset and data collection in parallel with collection of subjective measures from the subject. The entire session will take about 1 hour.

Operators were told at the beginning of each session, that they were to perform the role of SPPO. Also, that they will be supported by a Power Plant Operator (PPO), a Field Senior (FS-SPPO) and Shift Supervisor (SS). Subjects were drawn from the control room shift compliment, refresher training programs, personnel in-training for licensed positions, and from licensed station staff not on shift. The supporting roles were played by a member of the training staff and members of the validation team.

During each scenario, subjects were asked by the SS a series of questions about the plant's state, problems, state trend, safety concerns and production concerns. The interaction between subjects and SS was designed so as to be consistent with normal operational practices. The questions were scenario specific and the answers were recorded in the checklists. Answers provided that were not in the checklist were noted, but were not included in the data analyzed. For the LOFW scenario, the time taken for the diagnosis of the root cause of the upset was recorded. After each scenario, the subjects completed a series anchored rating scales. The subjects were asked to check anywhere along the scale and to use the behavioral descriptor as a guide. After each session, the operator was asked to fill a second questionnaire that provide direct comparative assessment of the support provided by CAMLS or the current CANDU 6 central annunciation system.. Half the subjects did Scenario 1 first and half did scenario 2 first. Each entire session for each subject took approximately 80 minutes. The subjects were split into two groups.

The checklist items, subjective scales, and the questionnaire were defined based on the performance hypotheses.

The schedule of activities for the Groups was as follows:

Group 1

- explanation of the experimental procedure and the supporting staff roles (10 min.),
- completion of questionnaire on operational experience (5. min.),
- an experimental trial using the CANDU 6 annunciation system with one scenario with simultaneous collection of objective performance measures (20 min.),
- completion of subject questionnaires (subjective measures) using anchored rating scales (5 min.),
- a second trial with the CANDU 6 annunciation system with the other scenario with simultaneous collection of objective performance measures (20 min.),
- completion of subject questionnaires (subjective measures) using anchored rating scales (5 min.),
- explanation of the COG CAMLS system using the ROP scenario as an example (5 min.),
- replay of the second scenario with the COG CAMLS system (5 min.), and
- completion of the comparative performance questionnaire by each subject (5 min.).

Group 2

- explanation of the experimental procedure and the supporting staff roles (10 min.),
- completion of questionnaire on operational experience (5. min.),
- explanation of the COG CAMLS system using the ROP scenario as an example (5 min.),
- an experimental trial using the COG CAMLS system with one scenario with simultaneous collection of objective performance measures (20 min.),
- completion of subject questionnaires (subjective measures) using anchored rating scales (5 min.),
- a second trial with the COG CAMLS system with the other scenario with simultaneous collection of objective performance measures (20 min.),
- completion of subject questionnaires (subjective measures) using anchored rating scales (5 min.),
- replay of the second scenario with the CANDU 6 annunciation system (5 min.), and
- completion of the comparative performance questionnaire by each subject (5 min.).

7.2 Experiment 2 - Annunciation Interrogation Workstation at Point Lepreau

Operators were told to assume they are on shift in the control room and that the plant will experience an upset. They will be asked to perform a number of tasks associated with upset diagnosis and response recovery. The tasks performed represented a mix of tasks that could be performed by the senior power plant operator, assistant power plant operator, or shift supervisor. Finally, the operators were told that for some tasks they will be asked to use the normal control room resources. For other tasks they will be asked to use the Annunciation Interrogation Workstation. The subjects were split into two groups.

Tasks selected for testing were based on the following performance hypotheses:

- The AIW provides better support for the task of accessing an alarm response procedure than the use of paper-based operating manuals (Task 1).
- The AIW provides better support for the task of confirming the cause of a trip than an examination of paper-based annunciation logs (Task 2).
- The AIW provides better support for tasks where alarm reference or detail information needs to be recalled rather than an examination of operating manuals and reference flowsheets (Tasks 3 and 5).
- The AIW provides better support for the task of determining the cause of the upset than an examination of paper-based annunciation logs (Task 4).
- The AIW provides better support for the task of confirming shutdown system trip inhibit actions than an examination of paper-based annunciation logs (Task 6).
- The AIW provides good support for the task of examining the alarm state and history for a specific system (Task 7).

The schedule of activities for Group 1 was as follows:

Group 1

- explanation of experimental procedures and supporting staff roles (5 min.)
- completion of operational experience questionnaire (5 min.)
- evaluation of Tasks 1 to 6 using control room resources (20 minutes)
  - provide scenario starting context to subject
  - begin scenario
  - task 1 performed (find procedure) when CI 0601 5552 INVIA AUTO TRANSFER TROUBLE appears
  - observe plant stepback and trip
  - subject makes upset alert announcement as filler task
  - repeat Task 1 (find procedure) when CI 907 4118 CLG STM ATT SPRAYS FAIL appears
  - inform subject plant stabilizing as expected
  - task 2 performed (find cause of trip)
  - task 3 performed (find conditioning) when CI 1383 4112 SP DRNS TK-EMERG DRN I/S appears
  - task 4 performed (find cause of upset)
  - task 5 performed (find alarm setpoint) for CI 907 4118 CLG STM ATT SPRAYS FAIL
  - task 6 performed (confirm SDS inhibit actions)
- questionnaire to gather information on (10 minutes)
  - relative support of CR paper-based resources for each task
- training in AIW functions and practice (10 minutes)
- evaluation of Tasks 1 to 7 using AIW functions (20 minutes)
  - provide scenario starting context to subject
  - begin scenario
  - task 1 performed (find procedure) when CI 0601 5552 INVIA AUTO TRANSFER TROUBLE appears

- observe plant stepback and trip
- subject makes upset alert announcement as filler task
- repeat Task 1 (find procedure) when CI 907 4118 CLG STM ATT SPRAYS FAIL appears
- inform subject plant stabilizing as expected
- task 2 performed (find cause of trip)
- task 3 performed (find conditioning) when CI 1383 4112 SP DRNS TK-EMERG DRN I/S appears
- task 4 performed (find cause of upset)
- task 5 performed (find alarm setpoint) for CI 907 4118 CLG STM ATT SPRAYS FAIL
- task 6 performed (confirm SDS inhibit actions)
- task 7 performed (examine alarm state and history for a system)

• questionnaire to gather information on (10 minutes)
  - relative support of AIW resources for each task
  - a comparative assessment of the support provided for each task by the AIW versus current control room resources.
  - other tasks AIW could support
  - other functions AIW should include
  - modifications to AIW functions to support task strategies better

Group 2

Group 2 subjects used the same basic experimental procedure except that the AIW was used first and the current control room resources were used second and training was adjusted accordingly.

8. DATA ANALYSIS

Since this is a comparative evaluation, we are interested in testing whether the observed difference between the means of the two systems is statistically meaningful. The implication of this is that one system can be statistically better than the other. We used a t-test for testing the difference between two population means, assuming independent samples and unequal variances.

It should also be noted that the nature of experimentation in the nuclear industry is that the subject population is small resulting in a small value for "n" in statistical calculations. This has to be weighed with the fact that large percentages of the total population itself were included in the trials. To take this into consideration, confidence intervals were considered down to 80% for some measures and are noted in the results.

8.1 Experiment 1 - Central Alarm Message Screens at Point Lepreau

Table 5 summarizes the statistical results of the data analysis for the central annunciation systems presented below with respect to the various hypotheses tested.

Each of the following sections provide a summary of the data collected for each of the measures and categories of data.

8.1.1 Objective Results

8.1.1.1 Checklist Data

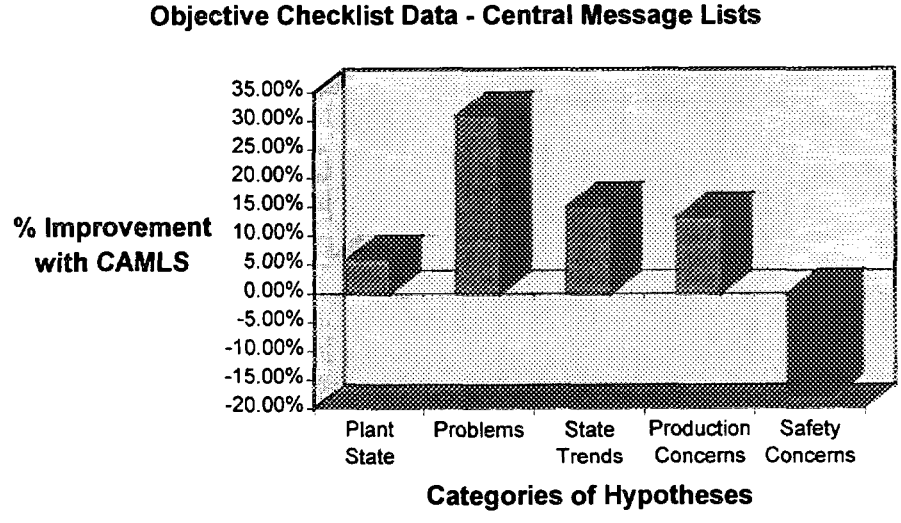


Figure 3: Central Annunciation Validation - Objective Checklist Results

8.1.2 Subjective Results

8.1.2.1 Anchored Rating Scales

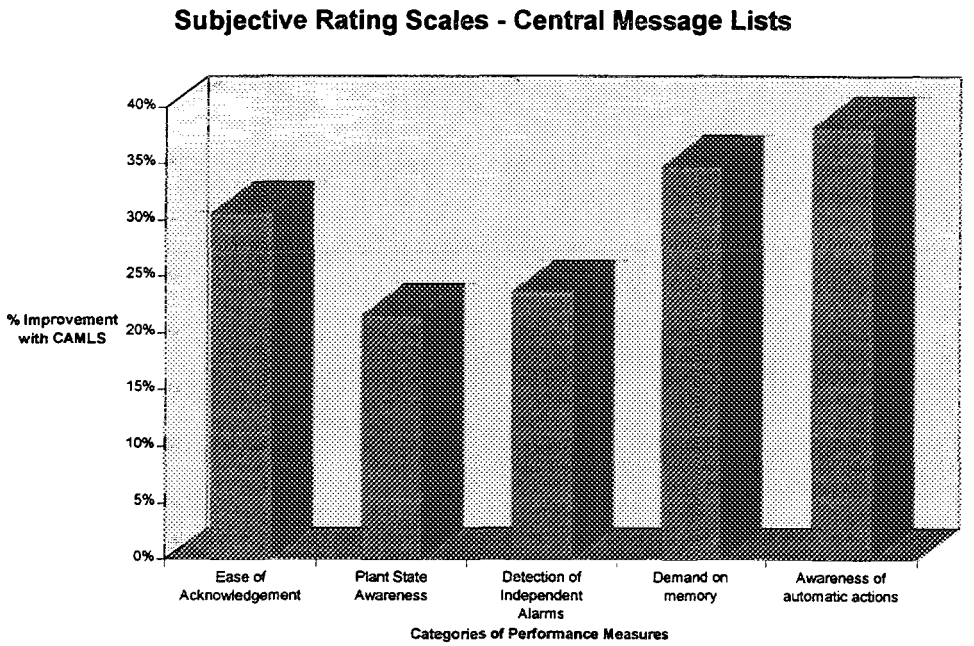


Figure 1: Central Annunciation Validation - Subjective Rating Scale Results

8.1.2.2 Questionnaire

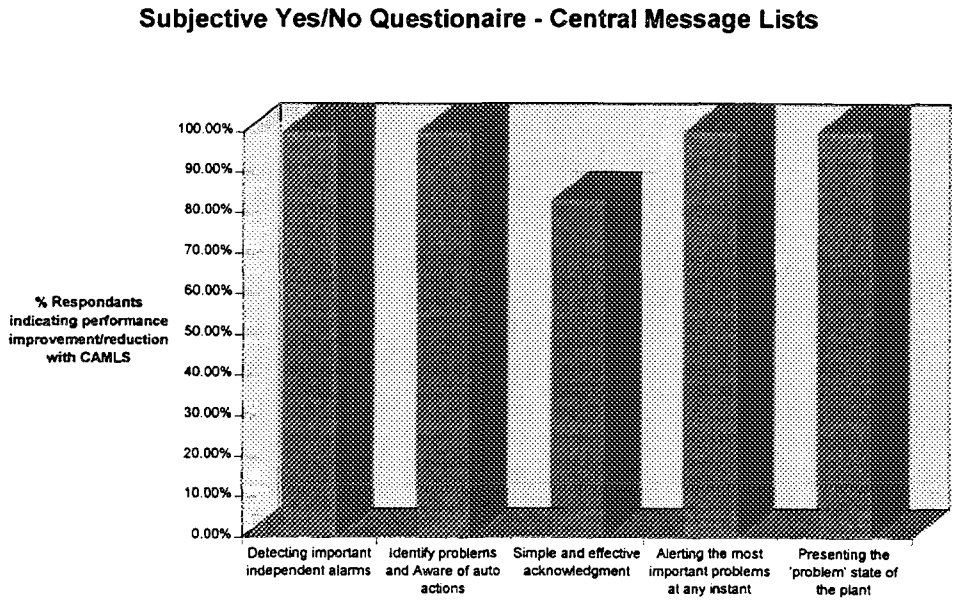


Figure 2: Central Annunciation Validation - Subjective Questionnaire Results

8.2 Experiment 2 - Annunciation Interrogation Workstation at Point Lepreau

Table 6 summarizes the statistical results of the data analysis for the annunciation interrogation workstation with respect to the various hypotheses tested.

8.2.1 Objective Results

8.2.1.1 Timing Data

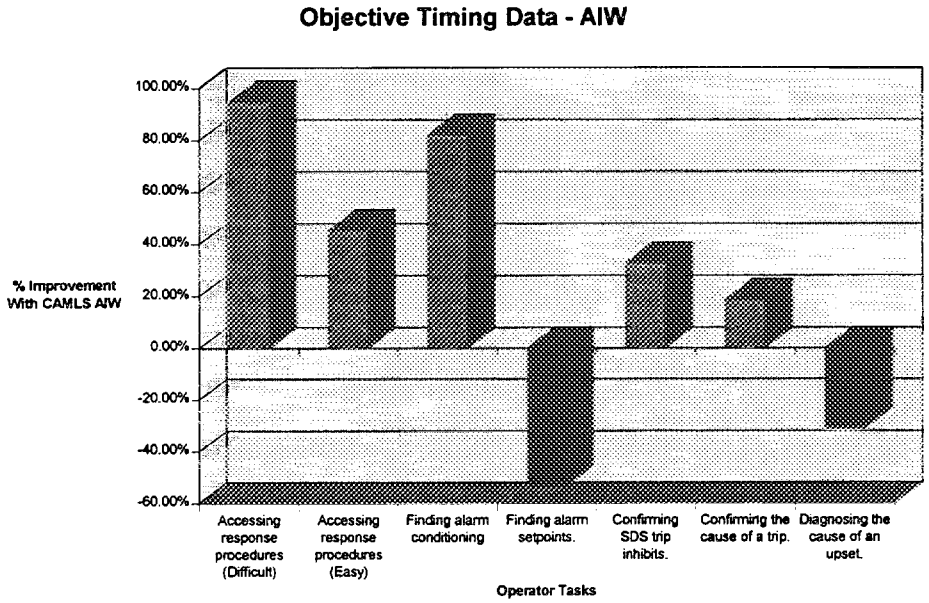


Figure 6: AIW Validation - Objective Timing Results

We expected that with the AIW finding the setpoint for a contact input alarm would be faster that the current approach. This is because this information can be found in the alarm response procedure display. Since the AIW provided faster access to alarm response procedures then the subjects should had also found the setpoint for a contact input alarm faster. However, due to the lack of training they did not know where to look for that information in the alarm response procedure display.

8.2.2 Subjective Results

8.2.2.1 Anchored Rating Scales

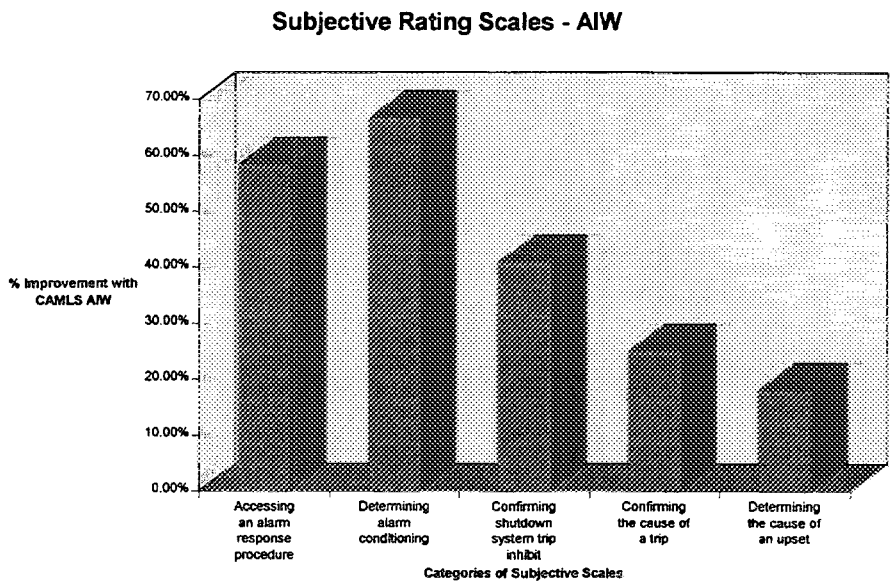


Figure 4: AIW Validation - Subjective Rating Scale Results

8.2.2.2 Questionnaire

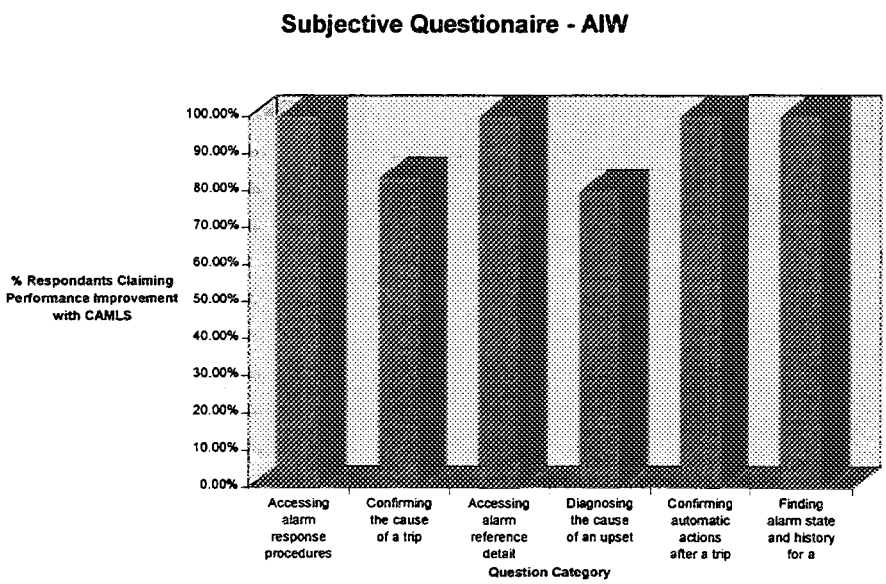


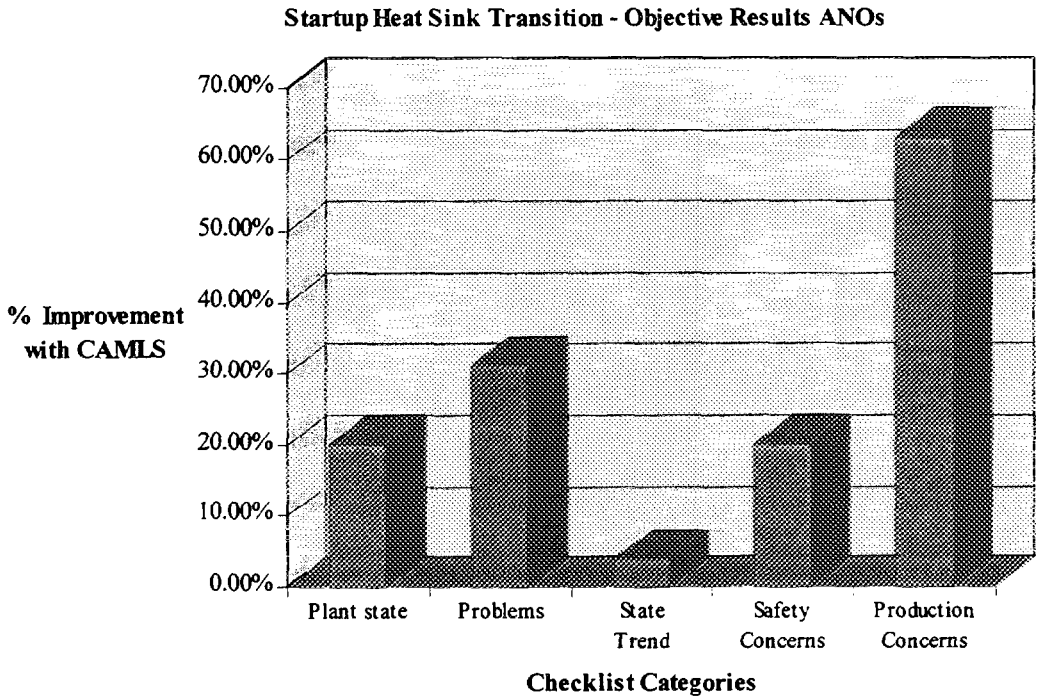
Figure 5: AIW Validation - Subjective Questionnaire Results

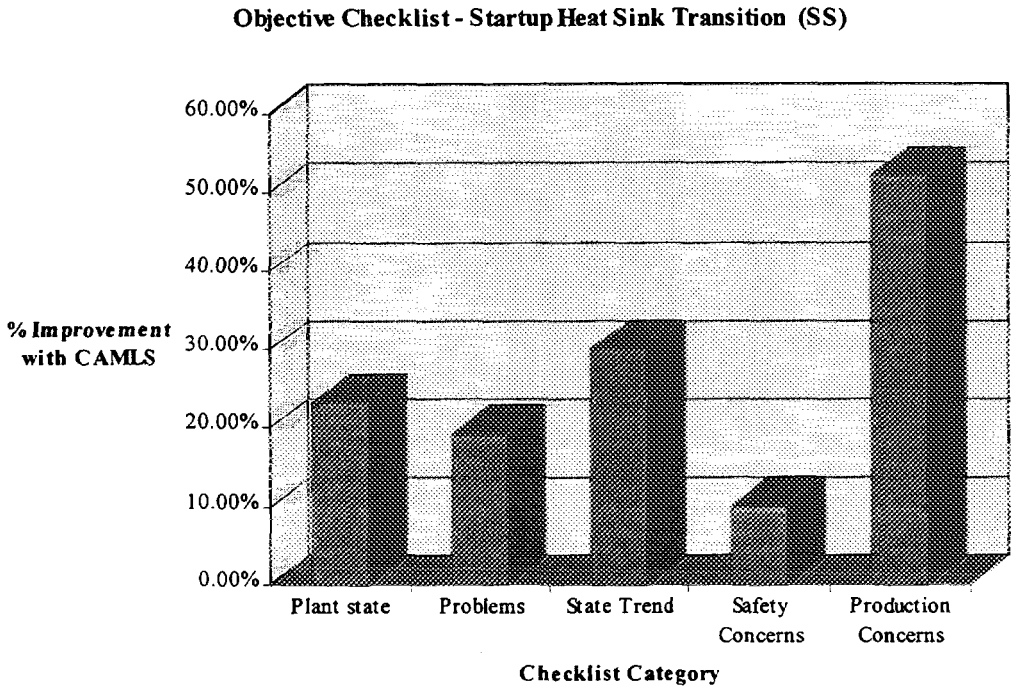
8.3 Experiment 3 - Central Message Lists at Darlington

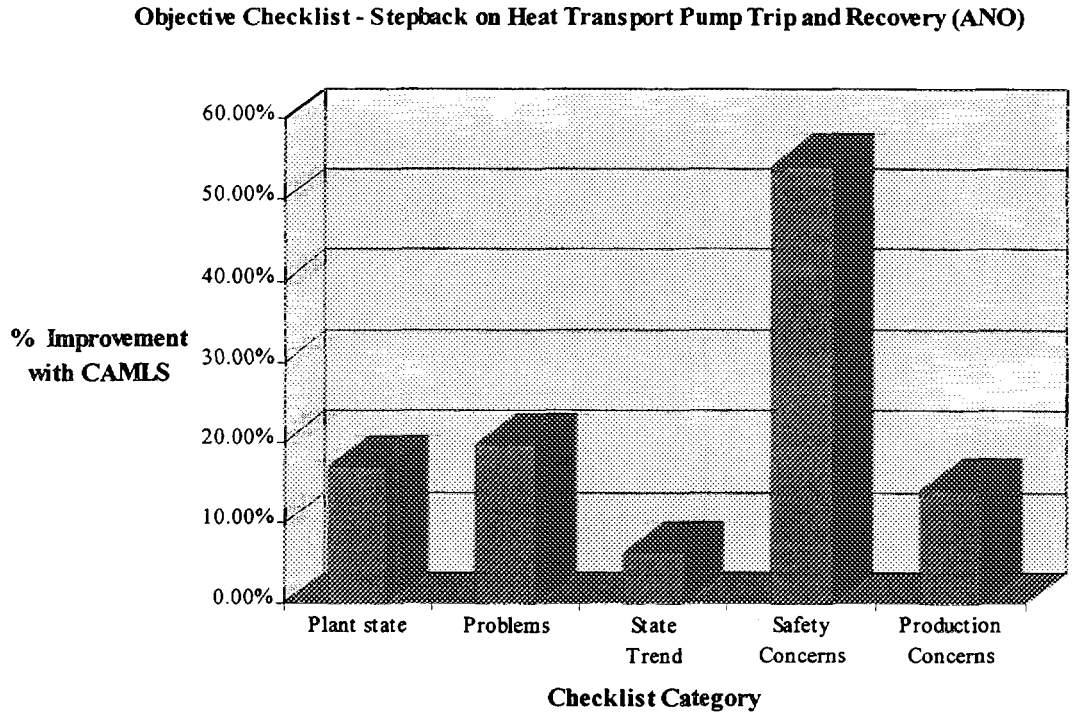
Table 7 summarizes the statistical results of the data analysis for the annunciation interrogation workstation with respect to the various hypotheses tested.

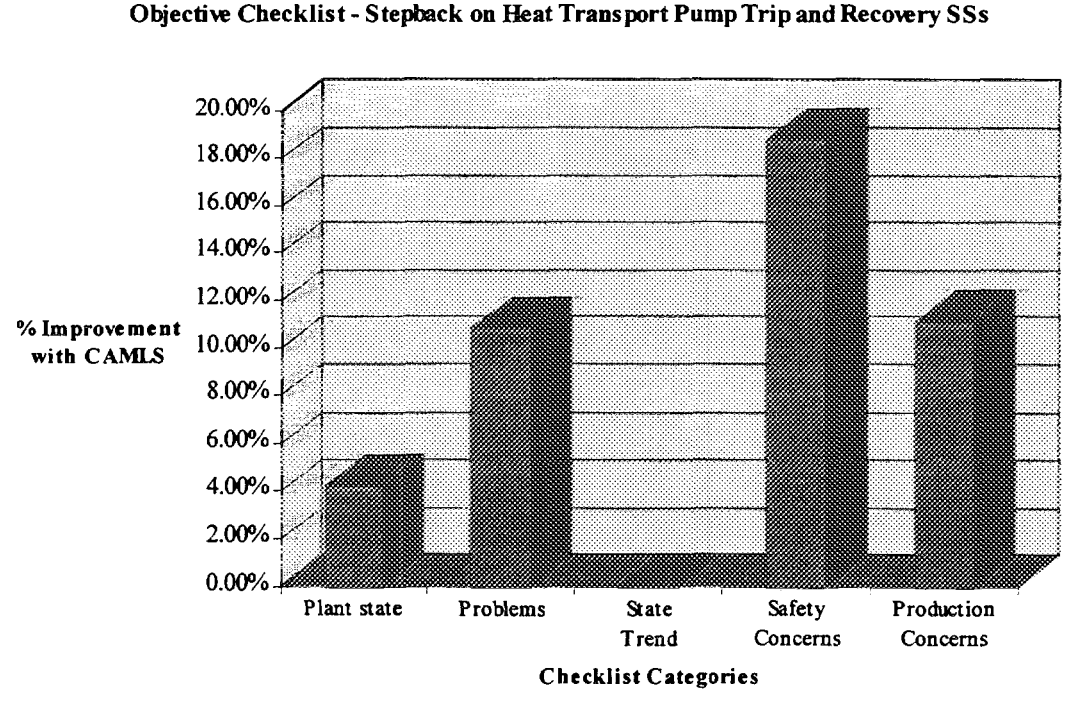
8.3.1 Objective Results

8.3.1.1 Checklist Data



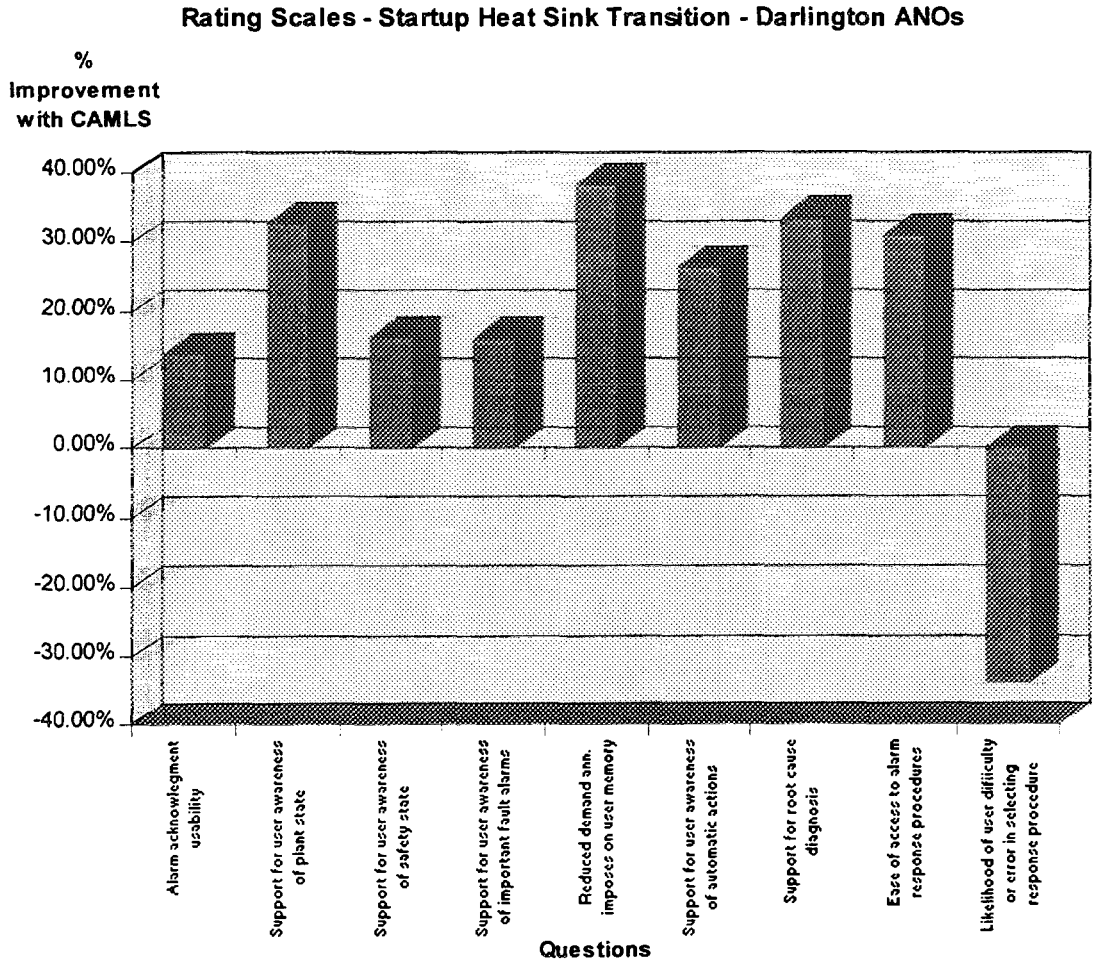


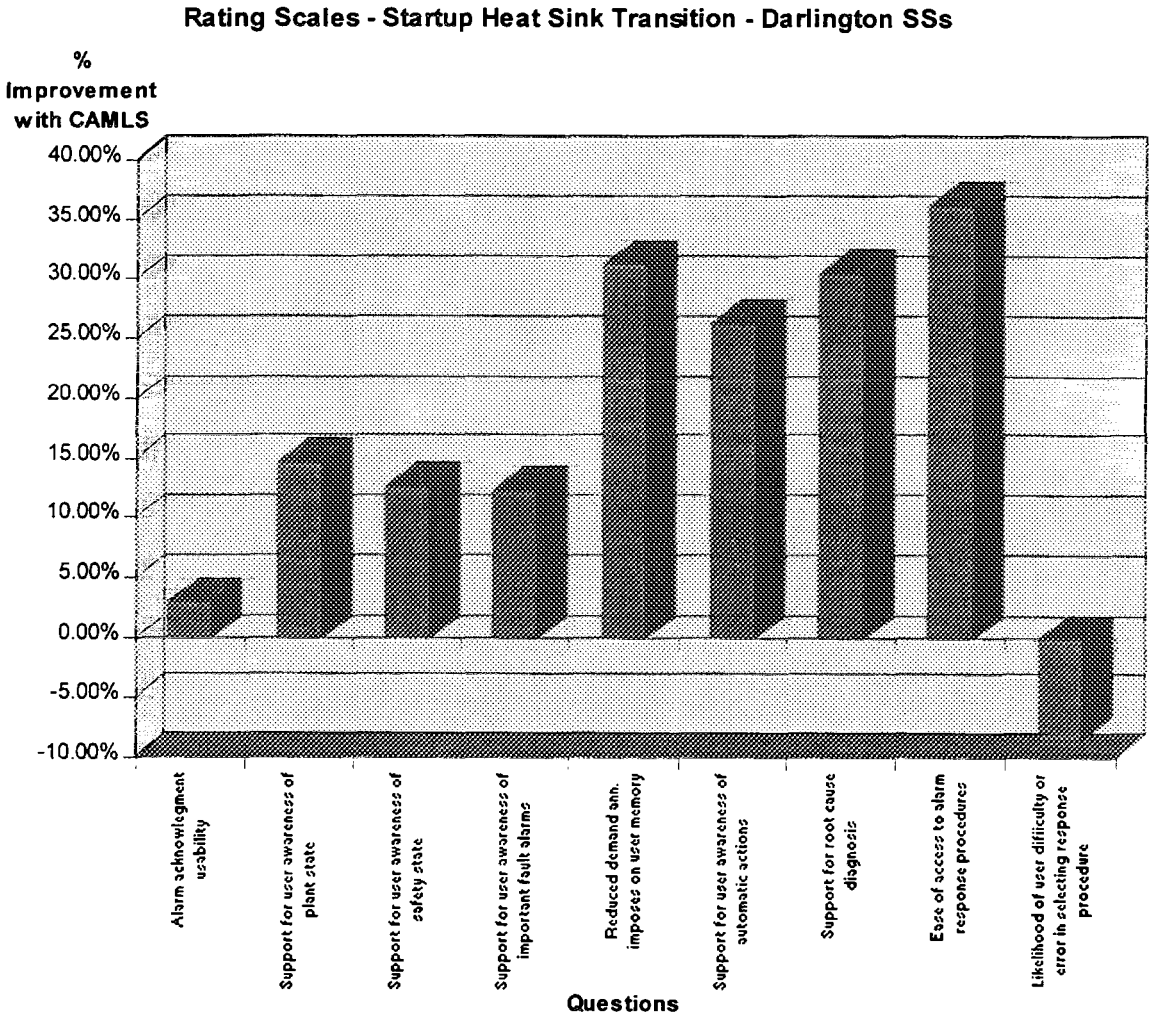




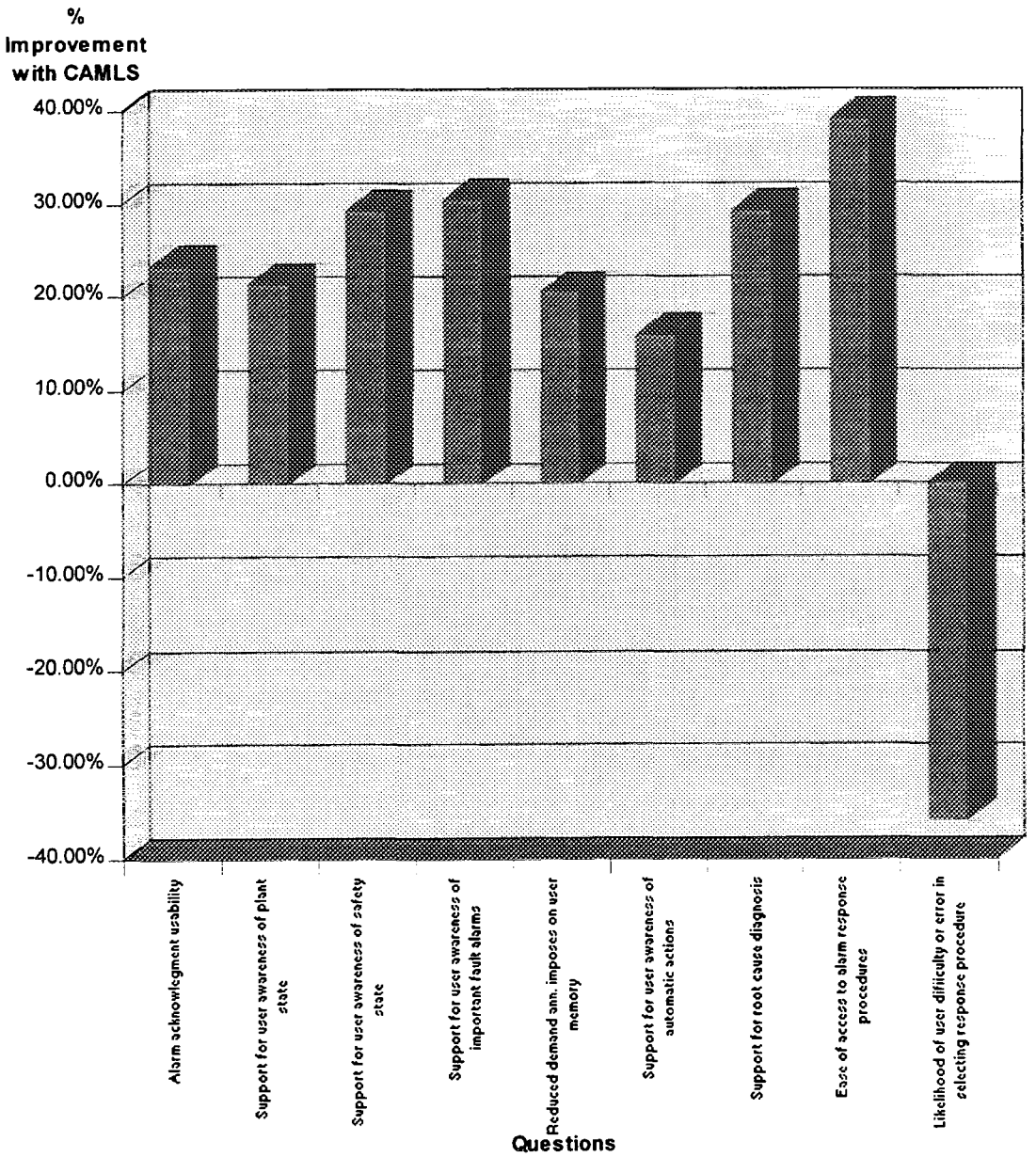
8.3.2 Subjective Results

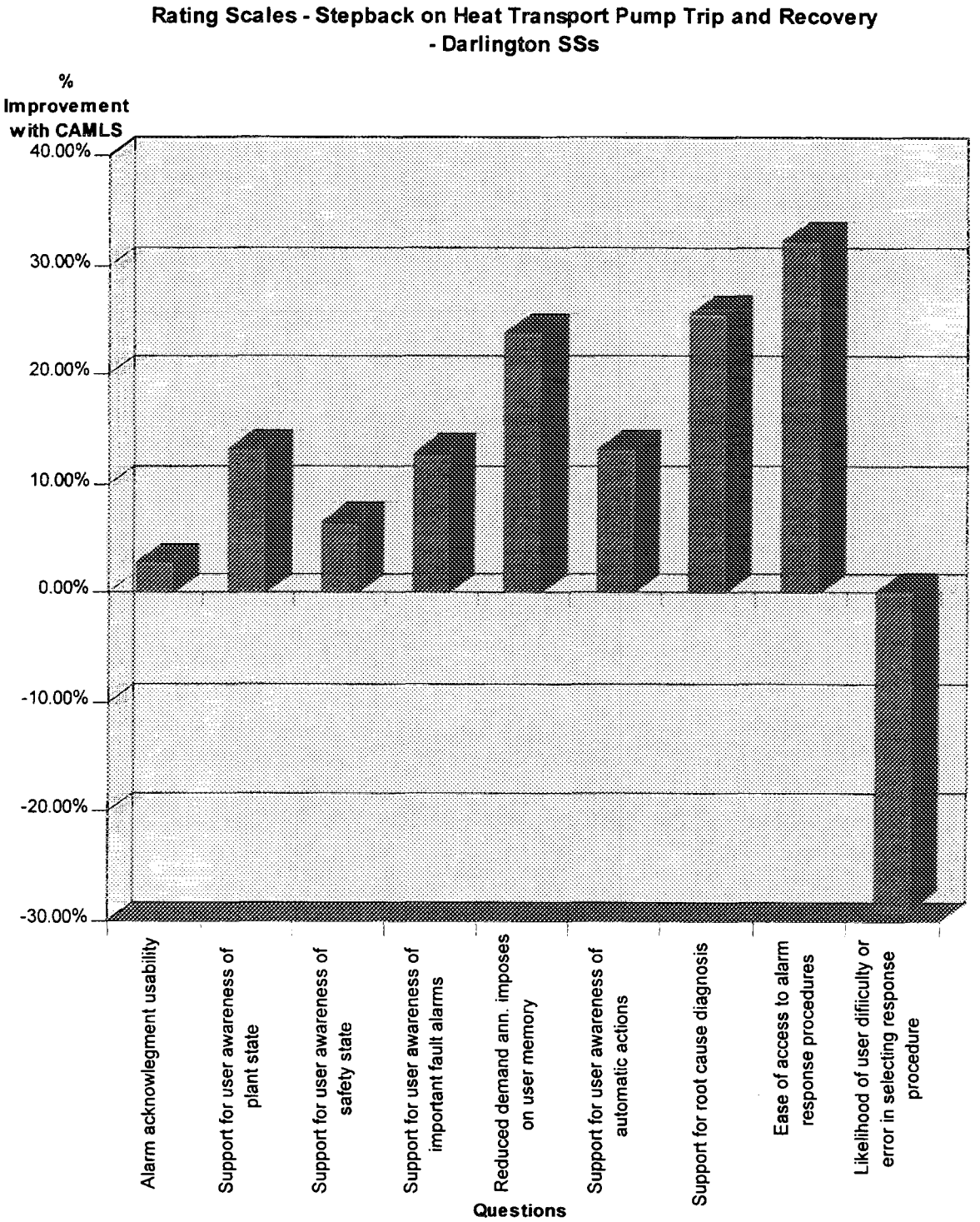
8.3.2.1 Anchored Rating Scales


Rating Scales - Startup Heat Sink Transition - Darlington ANOs
% Improvement with CAMLS
40.00%
30.00%
20.00%
10.00%
0.00%
-10.00%
-20.00%
-30.00%
-40.00%
Alarm acknowlegment usability
Support for user awareness of plant state
Support for user awareness of safety state
Support for user awareness of important fault alarms
Reduced demand ann. imposes on user memory
Support for user awareness of automatic actions
Support for root cause diagnosis
Ease of access to alarm response procedures
Likelihood of user difficulty or error in selecting response procedure
Questions


Rating Scales - Startup Heat Sink Transition - Darlington SSs
% Improvement with CAMLS
40.00%
35.00%
30.00%
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
-5.00%
-10.00%
Alarm acknowledgment usability
Support for user awareness of plant state
Support for user awareness of safety state
Support for user awareness of important fault alarms
Reduced demand sm. imposes on user memory
Support for user awareness of automatic actions
Support for root cause diagnosis
Ease of access to alarm response procedures
Likelihood of user difficulty or error in selecting response procedure
Questions

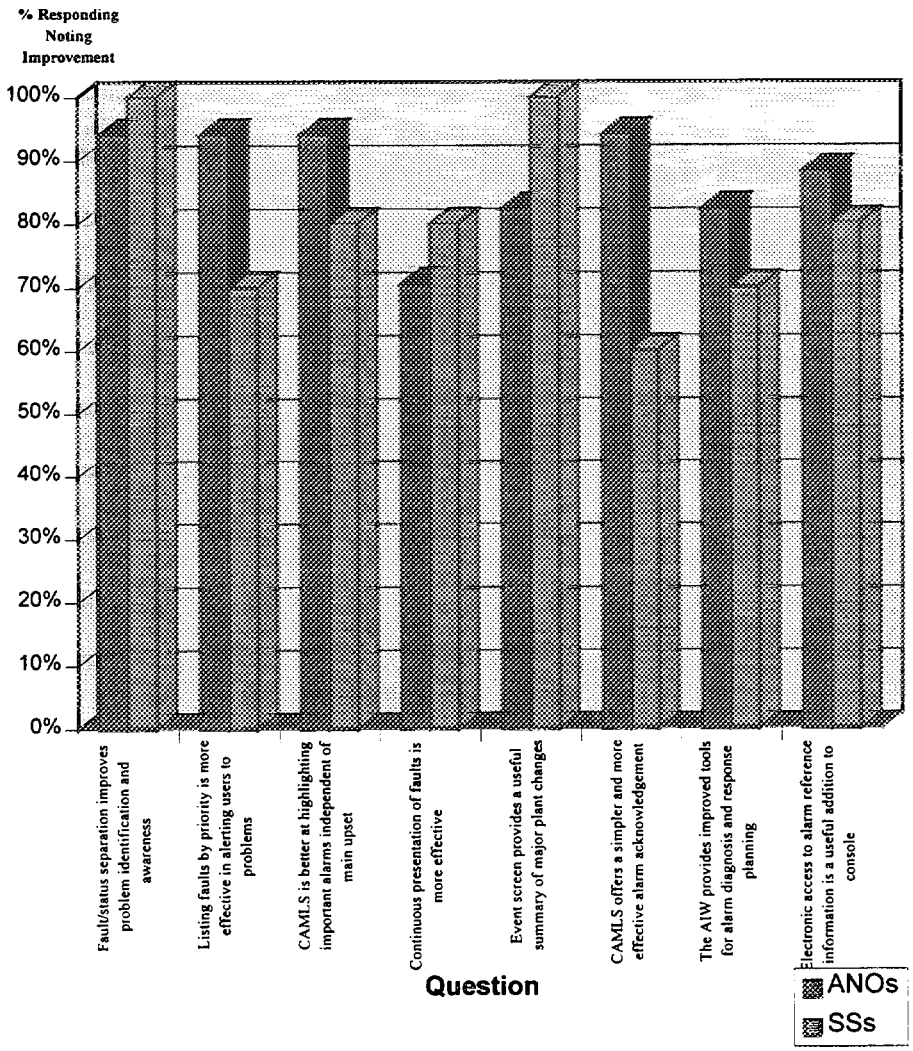
Rating Scales
- Stepback on Heat Transport Pump Trip and Recovery - Darlington ANOs





8.3.2.2 Questionnaire

Experiment 3 - Darlington Comparative Questionaire



9. INTERPRETATION OF THE DATA

9.1 Experiment 1 - Central Alarm Message Screens at Point Lepreau and Darlington

Based on these results, we can say with confidence that the COG Central Annunciation Message List System has demonstrated that compared to the existing CANDU central message lists plus the window tiles, the COG system improves:

- the probability that significant alarms are detected,
- the probability of detecting significant problems,
- the probability of detecting alarms secondary or independent of the primary or initial upset,
- awareness of plant state,

- the performance of operators by reducing the demand on operators' short term memory and the resulting mental workload,
- awareness of automatic actions in the plant, and
- the availability of operators for important activities by reducing distracting and unnecessary interaction with the annunciation system.

The degradation's in performance can be attributed to the elimination of the hard-wired safety-based window alarms from the simulator during trials with CAMLS. Although this was required to accurately measure the impact of the use of CAMLS, it is not intended nor desired to eliminate such alarm systems from the design at this point in time.

The first three points noted above have direct safety and economic implications. They can be said to point to an increase in the margins to safety of a CANDU plant and a decrease in the probability of plant trips and equipment damage thereby resulting in an economic saving. The last four points indicate an improvement in human performance in the system. At this point the link between improved human performance in these areas and improved safety and economics is tenuous within the context of this evaluation. However, research in the international aviation industry clearly points to a strong link between these types of measures and the eventual measures of safety and cost effectiveness.

CAMLS achieves this by:

- prioritizing relevant alarm data according to the consequence to the plant and the urgency for an operator response,
- adjusting the alarm presentation and priority with variations in the operating state of the plant,
- significantly reducing irrelevant alarm messages without losing key information,
- providing operationally organized information, and
- preventing unnecessary operator distraction from important operational activities.

9.2 Experiment 2 - Annunciation Interrogation Workstation at Point Lepreau

Based on these results, we can say with confidence that the COG Annunciation Interrogation System has demonstrated that compared to the existing CANDU 6 support for annunciation related tasks, the COG system improves operator performance by:

- directly supporting tasks for which there was no previous explicit support, and
- clearly has the potential to better support procedural and information search tasks given appropriate training and experience with the tool including
  - trip cause identification,
  - upset cause identification,
  - confirmation of automatic responses,
  - confirmation of successful safety system trip including trip inhibits,
  - access to alarm response procedures, and
  - access to alarm conditioning, setpoint, and other related information.

It is clear that many of the benefits of the AIW are independent of the benefits of the improvements to the central annunciation system design.

10. CONCLUSIONS AND RECOMMENDATIONS

New design concepts for CANDU annunciation have been developed, prototyped, and evaluated. As part of a COG R&D project, a CANDU Annunciation Message List System (CAMLS) has been assessed for operational performance over two upset scenarios. A formal validation process was used to arrive at statistically valid statements of comparative system performance between the current CANDU annunciation system and the COG developed CAMLS. The evaluation clearly establishes that CAMLS improves operator performance for most operationally significant tasks involving annunciation compared to existing CANDU annunciation systems. The implications of these improvements on safety margins, production costs, and human performance are significant.

REFERENCES

1. Meister, D., Advances in Human Factors/Ergonomics: Human Factors Testing and Evaluation, Elsevier, New York, New York.

2. Electric Power Research Institute, Computer-Generated Display System Guidelines, Volume 2: Developing an Evaluation Plan, Interim Report, EPRI NP-3701, 1984.

OTHER SOURCE MATERIAL USED

BOWERS, C., BRAUN, C. and KLINE, P., "Communication and Team Situational Awareness", Proceeding of the Center for Applied Human Factors in Aviation conference on Situational Awareness in Complex Systems, Orlando, Florida (1993).

ENDSLEY, M.R., "Situation Awareness in Dynamic Human Decision Making: Measurement", Proceeding of the Center for Applied Human Factors in Aviation conference on Situational Awareness in Complex Systems, Orlando, Florida (1993).

HOLMSTROEM, C., ENDESTAD, T., FOLLESOE, K., FOERDESTROEMMEN, N., HAUGSET, K. and VOLDEN, F., "Evaluation Programmer of the Integrated Surveillance and Control System ISACS - An Advanced Control Room Prototype", Proceedings of the American Nuclear Society Winter Meeting, San Francisco, California (1993).

International Electrotechnical Commission, Design for Control Rooms of Nuclear Power Plants. Report, IEC 694, 1989.

OHTSUKA, T., YOSHIMURA, S., KAWANO, R., FUJIIE, M., UJITA, H. and KUBOTA, R., "Nuclear Power Plant Operator Performance Analysis Using Training Simulators:

Operator Performance Under Abnormal Plant Conditions", Journal of Nuclear Science and Technology, Volume 31, pages 1184 to 1193 (1984).

REGAL, D.M., ROGERS, W.H. and BOUCEK, G.P., "Situational Awareness in the Commercial Flight Deck: Definition, Measurement and Enhancement", Proceedings of the Human Factors Society xxst Meeting, Anahiem, California (1988).

STUBLER, W. F., ROTH, E. M., and MUMAW, R.J., Evaluation Issues for Computer-Based Control Rooms. Westinghouse Science and Technology Center, Pittsburgh, Pennsylvania.

STUBLER, W. F., ROTH, E. M., and MUMAW, R.J., Integrating Verification and Validation with the Design of Complex Man-Machine Systems, Westinghouse Science and Technology Center, Pittsburgh, Pennsylvania.

ACKNOWLEDGEMENTS

The support and assistance of many people were essential to the successful performance of this simulator-based experimental program. The authors would like to acknowledge the key contributions made by the following people:

- CAMLS development and experimental team (K. Guo, G. Tosello, M. Thompson, R. Basso, D. Hickey, D. Elder, D. Riveras)
- D. Scott-Gillard, G. Cleghorn, T. Long, R. Arpin, D. Charette and E. Morin of Darlington NGS for assistance in planning and carrying out experiments in the Darlington simulator,
- B. Patterson, H. Storey, H. Thompson, F. McCallum, T. Myles, M. MacLean of Point Lepreau GS for assistance in planning and carrying out experiments in the Darlington simulator,
- M. Chignell of University of Toronto for advice and guidance in experimental design,
- Operations staff at Point Lepreau and Darlington GS who volunteered to be subjects for the experimental testing, and
- Management staff at Point Lepreau and Darlington GS who willingly provided station resources to support the experimental program.

Table 5: Summary of Statistical Significance of Results For Experiment 1, Central Annunciation, at Point Lepreau

HYPOTHESIS	SUBJECTIVE DATA		OBJECTIVE DATA	
The CAMLS central alarm screens provide:	**LCIV Scenario**	**LOFW Scenario**	**LCIV Scenario**	**LOFW Scenario**
Improved detection of problems to be resolved	No Test Performed	No Test Performed	Yes (85% CI)	Yes (95% CI)
Improved detection of the state of the plant	Yes (85% CI)	Yes (95% CI)	Yes (75% CI)	Not Statistically Better or Worse
Improved detection of the important alarms independent of the primary upset	Yes (85% CI)	Yes (95% CI)	Yes (90% CI)	yes (85% CI)
Improved detection of automatic actions	Yes (90% CI)	Yes (95% CI)	No Test Performed	No Test Performed
Improved diagnosis of the trip casual factors	No Test Performed	No Test Performed	No Test Performed	Not Statistically Better or Worse
Improved diagnosis of the root causes of upsets	No Test Performed	Yes (95% CI)	No Test Performed	Not Statistically Better or Worse
Improved diagnosis of the future state of the plant	No Test Performed	No Test Performed	Yes (95% CI)	Not Statistically Better or Worse
Reduced demand on memory	Yes (90% CI)	Yes (95% CI)	No Test Performed	No Test Performed
Reduced Distraction due to improved acknowledgment system	Yes (85% CI)	Yes (90% CI)	No Test Performed	No Test Performed
The COG message list system is better at presenting the operator with important alarms that are independent of the main upset	Yes 100% Agree		No Test Performed	No Test Performed
The separation of alarms into two groups faults and status improves the identification of problems to be address and better maintain an awareness of the automatic actions in the plant.	Yes 100% Agree		No Test Performed	No Test Performed
The COG message list system offers a more simple and effective acknowledgment approach.	Yes 83% Agree		No Test Performed	No Test Performed
The COG message list system approach of presenting faults in order of priority is more effective in alerting users to the most important problems at any instant.	Yes 100% Agree		No Test Performed	No Test Performed
The continuous presentation of active fault alarms is not as effective as the existing annunciation system.	No 100% Agree (No Means CAMLS is better.)		No Test Performed	No Test Performed
Note: "CI"- confidence interval				

Table 6: Summary of Statistical Significance of Results For Experiment 2, AIW Evaluation, at Point Lepreau

Hypotheses	Subjective	Objective
The AIW provides better support for the task of accessing an alarm response procedure than the use of paper-based operating manuals (Task 1).	Yes (95% CI)	Yes (95% CI)
The AIW provides better support for the task of confirming the cause of a trip than an examination of paper-based annunciation logs (Task 2).	Yes (95% CI)	Not Statistically Better or Worse
The AIW provides better support for tasks where alarm reference or detail information needs to be recalled rather than an examination of operating manuals and reference flowsheets (Tasks 3 and 5).	Yes - Tasks 3 (95% CI) Task 5- Not Statistically Better or Worse	Yes - Tasks 3 (95% CI) No - Tasks 5 (90% CI)
The AIW provides better support for the task of determining the cause of the upset than an examination of paper-based annunciation logs (Task 4).	Yes (85% CI)	Not Statistically Better or Worse
The AIW provides better support for the task of confirming shutdown system trip inhibit actions than an examination of paper-based annunciation logs (Task 6).	Yes (95% CI)	Yes (95% CI)
The AIW provides good support for the task of examining the alarm state and history for a specific system (Task 7).	Yes (85% CI)	No Test Performed
The AIW provides better support for the task of accessing an alarm response procedure in comparison to the use current paper-based operating manuals.	Yes 100% Agree	No Test Performed
The annunciation interrogation workstation (AIW) provides better support for the task of confirming the cause of a trip, by examining an annunciation log, in comparison to the use of a printed annunciation log.	Yes 83% Agree	No Test Performed
The AIW provides better support for tasks where alarm reference or detail information needs to be recalled in comparison to the use paper-based manuals and flowsheets.	Yes 100% Agree	No Test Performed
The AIW provides better support for the task of confirming the cause of an upset, by examining an annunciation log, in comparison to the use of a printed annunciation log.	Yes 80% Agree	No Test Performed
The AIW provides better support for the task of confirming automatic actions following a trip, by examining an annunciation log, in comparison to the use of a printed annunciation log.	Yes 100% Agree	No Test Performed
The AIW provides good support for the task of examining the state and history of alarms associated with a specific system.	Yes 100% Agree	No Test Performed
Note: "CI"- confidence interval		

Table 7a: Summary of Statistical Significance of Results For Experiment 3 at Darlington

	Scenario:	Stepback on Pump Trip and Recovery					
	Assessment Measures	**Objective**		**Subjective-Rating Scales**		**Subjective - Comparative**	
	Subject	ANOs	SSs	ANO	SSs	ANOs	SSs
No.	**Hypotheses Tested**						
o1	Improved awareness of plant state	Yes Sig. CI 95%	Yes Not Significant	s2	s2	c1	c1
o2	Improved awareness of problems to be addressed	Yes Sig. CI 95%	Yes Sig. CI 95%	s4	s4	c2, c3	c2, c3
o3	Improved awareness of plant state trends	Yes Sig. CI 75%	No Difference	Not Assessed	Not Assessed	Not Assessed	Not Assessed
o4	Improved awareness of safety concerns	Yes Sig. CI 95%	Yes Sig. CI 95%	s3	s3	Not Assessed	Not Assessed
o5	Improved awareness of production concerns	Yes Sig. CI 90%	Yes Sig. CI 90%	Not Assessed	Not Assessed	Not Assessed	Not Assessed
s1	Provides an alarm acknowledgement system that is easier to use.	No Test Performed	No Test Performed	Yes Sig. CI 90%	Yes Not Significant	c6	c6
s2	Provides users a better awareness of the overall state of the plant.	o1	1	Yes Sig. CI 95%	Yes Sig. CI 95%	c1	c7
s3	Provides users a better awareness of the safety state of the plant.	o4	o4	Yes Sig. CI 95%	Yes Not Significant	Not Assessed	Not Assessed
s4	Keeps users better informed of important fault alarms.	o2	o2	Yes Sig. CI 95%	Yes Sig. CI 90%	c2	c2
s5	Reduces the demand on users memory (e.g., need to remember active alarms or OM references).	No Test Performed	No Test Performed	Yes Sig. CI 90%	Yes Sig. CI 95%	Not Assessed	Not Assessed

s6	Provides users a better awareness of the state of automatic actions during an upset	No Test Performed	No Test Performed	Yes Sig CI 90%	Yes Sig CI 90%	Not Assessed	Not Assessed
s7	Provides users better support for root cause diagnosis.	No Test Performed	No Test Performed	Yes Sig CI 95%	Yes Sig CI 95%	c7	c7
s8	Provides users with easier access to alarm response procedures via the AIW.	No Test Performed	No Test Performed	Yes Sig CI 95%	Yes Sig CI 95%	c8	c8
s9	Reduces the likelihood users will have difficulty or make an errors in selecting the alarm response procedures via the AIW.	No Test Performed	No Test Performed	No Sig CI 95%	No Sig CI 95%	Not Assessed	Not Assessed
c1	Fault/status separation improves problem identification and plant status awareness.	o1,o2	o1,o2	s2	s2	Yes 100% Agree	Yes 100% Agree
c2	Listing of faults by priority is more effective in alerting users to problems.	o2	o2	s4	s4	Yes 100% Agree	No 25% Agree
c3	Highlights better important alarms independent of the main upset.	o2	o2	s4	s4	Yes 100% Agree	Yes 75% Agree
c4	Continuous presentation of active fault alarms is more effective.	Not Assessed	Not Assessed	Not Assessed	Not Assessed	Yes 63% Agree	Inconclusive 50% Agree
c5	Event screen provides a useful summary of major plant changes	Not Assessed	Not Assessed	Not Assessed	Not Assessed	Yes 88% Agree	Yes 100% Agree
c6	Offers a simpler and more effective alarm acknowledgement.	Not Assessed	Not Assessed	s1	s1	Yes 88% Agree	Inconclusive 50% Agree
c7	AIW provides improved tools for alarm diagnosis and response planning	Not Assessed	Not Assessed	s7	s7	Yes 88% Agree	Inconclusive 50% Agree
c8	AIW electronic access to alarm reference information is a useful addition to the console.	Not Assessed	Not Assessed	s8	s8	Yes 88% Agree	Yes 75% Agree

Table 7b: Summary of Statistical Significance of Results For Experiment 3 at Darlington

	Scenario:	Startup Heat Sink Transition					
	Assessment Measures	**Objective**		**Subjective - Rating Scales**		**Subjective - Comparative**	
	Subject	ANOs	SSs	ANO	SSs	ANOs	SSs
No.	**Hypotheses Tested**						
o1	Improved awareness of plant state	Yes Sig. 95% CI	Yes Sig. 85% CI	See s2	See s2	See c1	See c1
o2	Improved awareness of problems to be addressed	Yes Sig. 90% CI	Yes Sig. 90% CI	See s4	See s4	See c2, c3	See c2, c3
o3	Improved awareness of plant state trends	Yes Not Significant	Yes Sig. 85% CI	Not Assessed	Not Assessed	Not Assessed	Not Assessed
o4	Improved awareness of safety concerns	Yes Sig. 85% CI	Yes Sig. 80% CI	See s3	See s3	Not Assessed	Not Assessed
o5	Improved awareness of production concerns	Yes Sig. 95% CI	Yes Sig. 95% CI	Not Assessed	Not Assessed	Not Assessed	Not Assessed
s1	Provides an alarm acknowledgement system that is easier to use.	No Test Performed	No Test Performed	Yes Sig. CI 95%	Yes Not Significant	See c6	See c6
s2	Provides users a better awareness of the overall state of the plant.	See o1	See o1	Yes Sig. CI 95%	Yes Sig. CI 90%	See c1	See c7
s3	Provides users a better awareness of the safety state of the plant.	See o4	See o4	Yes Sig. CI 90%	Yes Sig. CI 90%	Not Assessed	Not Assessed
s4	Keeps users better informed of important fault alarms.	See o2	See o2	Yes Sig. CI 95%	Yes Sig. CI 90%	See c2	See c2
s5	Reduces the demand on users memory (e.g., need to remember active alarms or OM references).	No Test Performed	No Test Performed	Yes Sig. CI 95%	Yes Sig. CI 95%	Not Assessed	Not Assessed

s6	Provides users a better awareness of the state of automatic actions during an upset	No Test Performed	No Test Performed	Yes Sig. CI 95%	Yes Sig. CI 95%	Not Assessed	Not Assessed
s7	Provides users better support for root cause diagnosis.	No Test Performed	No Test Performed	Yes Sig. CI 95%	Yes Sig. CI 95%	See c7	See c7
s8	Provides users with easier access to alarm response procedures via the AIW.	No Test Performed	No Test Performed	Yes Sig. CI 95%	Yes Sig. CI 95%	See c8	See c8
s9	Reduces the likelihood users will have difficulty or make an errors in selecting the alarm response procedures via the AIW.	No Test Performed	No Test Performed	No Sig. CI 95%	No Not Significant	Not Assessed	Not Assessed
c1	Fault/status separation improves problem identification and plant status awareness.	See o1,o2	See o1,o2	See s2	See s2	Yes 89% Agree	Yes 100% Agree
c2	Listing of faults by priority is more effective in alerting users to problems.	See o2	See o2	See s4	See s4	Yes 89% Agree	Yes 100% Agree
c3	Highlights better important alarms independent of the main upset.	See o2	See o2	See s4	See s4	Yes 89% Agree	Yes 83% Agree
c4	Continuous presentation of active fault alarms is more effective.	Not Assessed	Not Assessed	Not Assessed	Not Assessed	Yes 89% Agree	Yes 100% Agree
c5	Event screen provides a useful summary of major plant changes	Not Assessed	Not Assessed	Not Assessed	Not Assessed	Yes 78% Agree	Yes 100% Agree
c6	Offers a simpler and more effective alarm acknowledgement.	Not Assessed	Not Assessed	See s1	See s1	Yes 100% Agree	Yes 67% Agree
c7	AIW provides improved tools for alarm diagnosis and response planning	Not Assessed	Not Assessed	See s7	See s7	Yes 78% Agree	Yes 83% Agree
c8	AIW electronic access to alarm reference information is a useful addition to the console.	Not Assessed	Not Assessed	See s8	See s8	Yes 89% Agree	Yes 83% Agree

SIMULATOR TESTING OF THE WESTINGHOUSE AWARE ALARM MANAGEMENT SYSTEM

J.P. Carrera, J.R. Easter, E.M. Roth
Westinghouse Electric Corp.
Pittsburgh, Pennsylvania
United States of America

ABSTRACT

Over the last year, Westinghouse engineers and operators from the Beznau nuclear power station (KKB), owned by the Nordostschweizerische Kraftwerke AG of Baden, Switzerland, have been installing and testing the Westinghouse AWARE Alarm Management System in Beznau/SNUPPS operator training simulator, owned and operated by the Westinghouse Electric Corp., in Waltz Mill, PA., USA. The testing has focused primarily on validating the trigger logic data base and on familiarizing the utility's training department with the operation of the system in a real-time environment. Some of the tests have included plant process scenarios in which the computerized Emergency Procedures were available and used through the COMPRO (COMputerized PROcedures) System in conjunction with the AWARE System.

While the results to date are qualitative from the perspective of system performance and improvement in message presentation, the tests have generally confirmed the expectations of the design. There is a large reduction in the number of messages that the control room staff must deal with during major process abnormalities, yet at times of relative minor disturbances, some additional messages are available which add clarification, e.g., "Pump Trouble" messages. The "flow" of an abnormality as it progresses from one part of the plant's processes to another is quite visible. Timing of the messages and the lack of message avalanching is proving to give the operators additional time to respond to messages. Generally, the anxiety level to "do something" immediately upon a reactor trip appears to be reduced.

1. THE AWARE SYSTEM

The AWARE Alarm Management System, based on many of the ideas described by Jens Rasmussen [8] and others in the Cognitive Systems Engineering literature, is being installed in the Beznau units as part of a large, distributed UNIX based computer network. In this network application, the run-time portion of the AWARE System is implemented on redundant SUN Microsystems SPARC 2 workstations and servers.

The AWARE System is composed of three major elements. These are the Overview Panel, a Support Panel of workstation VDU displays, and an off-line data base maintenance utility. The servers drive an Overview Panel composed of 254 alpha-numeric display devices, each capable of displaying an 80 character message, that present the abnormality messages. The System is comprised of 12 one meter square sections containing 21 alpha-numeric display devices. The messages which appear on these display devices flash between full and half intensity when the

message first becomes active. The flashing goes to continuous full intensity when the operator pushes the acknowledge button, just as is done with traditional annunciator systems. The messages are grouped into message sets or lists. Each list is capable of having one or more of its messages presented on the alpha-numeric display devices based upon each message's priority rank within the set of active messages in the list and the number of display devices assigned to that list. In other words, the message prioritization is used to make the messages compete for display space within a list. No attempt is made to prioritize alarms across the lists. The intention is that the operators will address the displayed messages as they come up, working through the push-down/pop-up stacks of messages as the priorities display them. In this way, all messages are expected to be addressed and each can be considered to be "important" by the operators when it is displayed. This contrasts with other computerized alarm systems that assign each alarm a fixed, predefined indication of urgency for operator action, with some alarms always coded as "high" urgency for action and other alarms always coded as "low" urgency. In the AWARE system operators do not have to consciously consider relative alarm priority. Whatever alarms appear in the display space at any given point in time are expected to be attended to and addressed.

The arrangement or layout of these display devices is enhanced by a fascia that provides labels or titles to the lists of messages. The back-bone of the display organization is plant process equipment purpose or function. An example of one of the twelve sections, this for the function of Reactor Coolant System Pressure, is shown in Figure 1. The entire Overview Panel can be seen in the video tape of a brief excerpt of the simulator tests, which we are showing during the presentation of this paper.

Messages which are active, but whose priority is too low to permit display on the alpha-numeric display devices on the Overview Panel are available, upon operator request, on the workstation VDU screens. The operators can query the System, at their own pace, with regard to Active messages, various parsings of the chronological list of active messages, the list of possible messages (whether or not they are currently active), message trigger logic and setpoints, access (through the trigger logic display) to detailed point (sensor) information residing in the data acquisition portion of the network, access through the messages (either active or inactive) to graphical process functional and physical displays, and the capability to access the message response procedure on the COMPRO System (this latter capability is available, though it has not, as yet, been activated for this application). The Support Panel is illustrated in Figure 2.

The third element is the off-line AWARE Database Maintenance Utility (ADMU), based upon the INGRES relational data base management software. The computerized data entry forms were built in INGRES using their 4GL interface language. The three elements of the AWARE System are more thoroughly described in References [1] through [5].

The software was engineered and constructed using the methods of Structured Analysis/Structured Design as described by DeMarco [6]. Computer Aided Software Engineering (CASE) tools such as TEAMwork [7] were used to ensure adequate structure, configuration control, and documentation for the Quality Assurance program. Software verification testing has been performed as a stand-alone element, integration testing during the Factory Acceptance Tests (FAT), the Site Acceptance

Tests (SAT) of the total network, and validation testing of the intended functionality during these simulator tests.

2. SITE INSTALLATION

In the Beznau application, the message trigger logic data base is composed of logic and message wording for approximately 4500 abnormality and status messages. This is compared to the approximately 1000 annunciator tiles that currently provide the same function to the control room operators. The additional messages come from essentially two sources: 1.) the elimination of "group" alarms, e.g., Pump Trouble as a single message for multiple problems such as vibration, bearing temperature, lubrication, power, etc., and 2.) including in message and logic data base the list of items in the Alarm Response Procedures that the operator is asked to investigate to determine the possible cause of the alarm, e.g., Tank Level LOW, check if pump is running, valve is open, etc. Also, the capability to add "higher level" messages has caused the addition of messages such as "Let-down line now ISOLATED". At this point in this application, we have only begun to scratch the surface of providing higher level messages such as this that could be useful to the control room staff.

Currently, the hardware and software are installed in one of the two units at the Beznau site. Installation will be completed on the second unit during the fall outage which begins in about two weeks. The AWARE System is operational and is running on the first unit but the Overview Panel display devices have not been turned on since the fascia have not been installed and the Swiss regulatory authority has not completed their review. Site personnel are using this time to refine the setpoints and to complete the installation of the last set of sensors to the system.

In early September, utility management and training personnel spent a week on the simulator developing the details of their control room operational philosophy (who does what, when) and determining the corresponding alternations needed in their training program in order to take full advantage of the System. The remainder of this year will be used to construct their training program modifications and to resolve any outstanding issues with the Swiss regulatory authority. Formal control room crew classroom and simulator training with respect to the AWARE System is expected to begin in early 1997, with the System becoming fully utilized in both control rooms in 1998.

3. THE TESTS

Over the last ten to twelve months, nine fully licensed utility control room operators and picket engineers (shift technical advisors) have periodically participated in simulated events and plant evolutions of all types on the full scope training simulator with the AWARE System in operation. Simultaneously, Westinghouse design engineers improved and refined the message and trigger logic data base using the ADMU. The focus of the tests was to validate the trigger logic data base and to familiarize the utility's operators and training personnel in the operation and attributes of the System. A formal test procedure was written prior to the formal test periods, a test log was maintained, and a test report has been written.

4. CONCLUSIONS

The tests to date have focused mainly on verifying the validity of the trigger logic data base and learning about its behavior during plant transients. However, there is evidence that the operators believe that the AWARE System is a significant improvement over their existing annunciator tile system.

As the video shows, there are seldom more than 5 to 10 messages active on the Overview Panel at any time. Quantitative comparisons of the number of messages vs. the number of lit annunciator tiles for given abnormalities is the subject of future investigations. It is, however, quite apparent at this stage in the testing that significant and effective message reduction has been achieved. While the total number of potential alarms is much larger (4500 as opposed to 1000 in a typical conventional control room), the number of alarms an operator sees at any given point in time is smaller and more informative. The effectiveness of this achievement is substantiated by the operators periodically exclaiming "now we can do something, it's clear what needs to be done".

To the extent possible, the data base is constructed so as to provide a dark board when nothing is abnormal. This is achieved for steady-state operations and for well understood transients, such as reactor trip. As a result, in a normal reactor trip situation, when there are no additional equipment malfunctions, with few exceptions, the only alarm the operator sees for the first 20 to 25 minutes (the time required for the processes to stabilize after the trip transient) is the "first-out" causal message. The messages that are simply reflecting the trip transient are cut-out, leaving only the messages about any abnormality to the trip as active messages. This, along with the effective organization and presentation of the messages, seems to have resulted in reducing the operators' post-trip tension and anxiety that they have experienced during reactor trips in the past. Operators tell us that knowing that the checks for abnormality are performed by the AWARE System and any resulting abnormality is immediately signaled gives them the confidence and patience to observe and evaluate the transient's progress without feeling that they MUST do something. Over time this anxiety reduction should help the operators to become more effective when addressing process transients or equipment abnormalities.

The utility has recognized the value of the AWARE System in providing a coherent and meaningful picture of plant state, both pre- and post-trip. They are currently grappling with how to adjust their control room operational philosophy and associated training to capitalize on System as a source of information to affirm and complement the information derived from working through the emergency operating procedures and from other resources in the control room.

Also, the organization of the presentation of the messages on the Overview Panel should be a valuable assistance in operator training. One operator (from another utility) upon first seeing the "functional" process layout on the Overview Panel exclaimed, "I wish I had this when I took my reactor operator's exam!".

Finally, the robustness of the logic parser, in terms of the speed of execution and the number and types of functions that it will process, has provided the capability to vastly grow the data base in the future. The utility is very interested in providing "high level" messages, i.e., synthesized from

multiple input points or utilizing synthetic variables or both, on-line in the control room. These tests have demonstrated that the AWARE System has the capability to fulfill this desire. In addition, incorporating the AWARE System in a network environment permits it to utilize the results or output from any number of application programs that may be performing sophisticated and in-depth analyses of a plant's equipment and processes. The AWARE Database Maintenance Utility has shown that it provides the utility's operations department, i.e., the operators, with the means to grow the data base in a direction and to a size that meets their needs.

REFERENCES:

[1] WOODS,D.D., et al., Alarm Management System, U.S. Patent Number 4,816,208, United States Patent Office, Washington, D.C., 1986.

[2] LEVETT, M.J., RICHELLE, G., CARRERA, J.P., AWARE, An Advanced Alarm Management System - Recent Developments and Operational Experience, Institute of Nuclear Engineers (INE), Second International Conference on Control & Instrumentation in Nuclear Installations, Churchill College, University of Cambridge, U.K.

[3] EASTER, J.R., HAENTJENS, J., Advanced Alarm Management System, Proceedings of the International Atomic Energy Agency, International Working Group on Nuclear Power Plant Control and Instrumentation, Espoo/Helsinki, Finland, June 1994.

[4] EASTER, J.R., HAENTJENS, J., Advanced Alarm Management System, Proceedings of TOPform '95 - FRANCE Avignon, April 1995.

[5] EASTER, J.R. and LOT, L., Back-Fitting a Fully Computerized Alarm System into an Operating Westinghouse PWR: A Progress Report, Proceedings of the IEEE 5th Conference on Human Factors and Power Plants, Monterey, Calif. U.S.A., June 1992.

[6] DeMarco, T., Structured Analysis and System Specification, Yourdon Press, Englewood Cliffs, N.J., 1979.

[7] INGRES, INGRES, The Intelligent Data Base, INGRES Corp, Alameda, Ca., 1991.

[8] RASMUSSEN, J., Information Processing and Human-Machine Interaction, An Approach to Cognitive Engineering, North -Holland, New York, N.Y., 1986.

ALARM SYSTEM FOR ABWR MAIN CONTROL PANELS

Yuji Kobayashi, Koji Saito
TOSHIBA Corporation
Japan

ABSTRACT

TOSHIBA has developed integrated digital control and instrumentation system for ABWR, which is the third-generation man machine interface system for main control room that we call A-PODIA (Advanced PODIA). A-PODIA has been introduced the first actual ABWR plant in JAPAN. In A-PODIA, TOSHIBA has realized improvement of alarm system that all operator crews in the control room can recognize plant anomalies easily. The alarm system can recognize essential alarms for plant safety easily and understand annunciators with each integrated annunciators and their prioritized color easily by classifying alarms into plant-level essential annunciators, system- level integrated annunciators and equipment level individual annunciators with hierarchical structure. This paper describes conventional alarm system and the design philosophy, alarm system design and operation of "Alarm System for ABWR Main Control Panels".

1. INTRODUCTION

TOSHIBA has been developing the integrated digital control and instrumentation system of optical multiplexing and advanced man-machine interface (MMI) since 1980 soon after TMI incident. With intensive effort, TOSHIBA developed that we call PODIA system. (PODIA: Plant Operation by Displayed Information and Automation) In PODIA, separation of main panel and sub-panel, adoption of CRT display and partial automation for auxiliary system to support plant operation and reduce human errors are introduced. After the first PODIA was introduced in 1985, 6 PODIAs has been in operation and had excellent experiences of over 50 reactors years. With the experiences, TOSHIBA started next development since 1985 and has developed A-PODIA system for ABWR. Fig.1 and Fig.2 shows the development of TOSHIBA Main Control Room (MCR) design.

In A-PODIA, the following designs are newly introduced.

- Compact operator console that centralized monitoring and control function
- Large display panels that among all operator crew in the control room can recognize important information for plant safety easily in common and understand plant general status easily
- Enhanced automation by automation of control rod maneuvering
- Hierarchical Alarm System

The hierarchical alarm system is the basic structure of "Alarm System for ABWR Main Control Panels".

And the large display panels consists of essential alarm panel, large mimic panel and large monitor screen. The large mimic panel is located at middle part of the large display panels. And large monitor screen is located at right part of the large display panels. The large mimic panel has assigned plant essential parameters as fixed location and fixed content. And large monitor screen can display the same information that is displayed on CRTs. And first hit display has been located as fixed location and variable content at upper of the essential alarm panel. Compact operator console has 7 CRTs, 17 FDs (Flat Displays) of color LCD (liquid crystal display) type and emergency hardwired switches. Auxiliary console that has 31 FDs and about 100 hardwired switches is provided at lower part of the large display panels. The CRTs are touch sensitive and high resolution 20 inch CRT driven by process computer and the FDs are touch sensitive 10 inch FD driven system-level digital controller.

2. CONVENTIONAL ALARM SYSTEM

2.1 Alarm System in PODIA

PODIA consists of main console and two auxiliary panel. In PODIA, operator crews have been shared with the panels as follows.

- To monitor and control with Main console, operator crew in charge of reactor side has been located.
- To monitor and control with Auxiliary panel that we call ECCS panel, operator crew in charge of auxiliary side has been located.
- To monitor and control with Auxiliary panel that we call BOP panel, operator crew in charge of turbine and generator side has been located.

And alarm system consists of over 1000 hard-wired annunciators as fixed location and fixed content. These annunciators have been assigned at upper part of main console and two auxiliary panels.

The location of operator crews and annunciators in PODIA is as shown in Fig.3.

2.2 Evaluation of Conventional Alarm System

From the location of operator crews and annunciators, the alarm system in PODIA has got the following evaluation.

- Since annunciators have been located at the distributed panels of main console and two auxiliary panels, monitoring and confirmation of annunciators must be done by each operator crews in front of each panel when some transient or accident occurred. That means operator crews need to recognize plant general status at a look.

- Since alarm system consists of over 1000 hard-wired annunciators as fixed location and fixed content, supervisor must handle at a time amount of annunciators and plant status that is reported by operator crews. That means a supervisor needs to consider important information for plant from the report and transmit the proper direction according to priority.

- The annunciators have mixed arrangement of important alarm for plant safety and minor alarm with same-size tiles. That means operator crews and supervisor need to distinguish important alarm for plant safety from minor alarm at a look when amount of annunciators happened.

- To inform plant general status after some transient and accident occurred, among operator crews including supervisor verbal communication are necessary.

3. DESIGN PHILOSOPHY

TOSHIBA has improved the alarm system from the evaluation of conventional alarm system. It is important to provide effective information transmission between plant and operator. Alarm system in A-PODIA has designed on a basis of the following design philosophy.

- Reduction and optimization of hard annunciators
- Classification and systematization of important alarm for plant safety and minor alarm
- Assignment of important alarm and minor alarm with different location and tiles' size

According to the design philosophy, the design strategy of the alarm system is the hierarchical structure and accessibility and space factor. On a basis of the design strategy, the alarm system is going to aim at easier understandable priority for operator crews, and location and device type of annunciators in accordance with priority of monitoring.

3.1 Hierarchical Structure

There are vast amount of alarm information in nuclear power plant. This alarm information contains important alarm for plant safety and minor alarm and so on. TOSHIBA has introduced the concept of hierarchical structure to classify and systematize the alarm information so that operator crews can understand priority easily. And it is important to consider quantity and importance to reduce and optimize the alarm information. On a basis of the concept, the alarm information in plant has been classified to three levels, such as plant level, system level and equipment level.

Alarm information in plant is analyzed by the relation of quantity and importance in hierarchy as shown in Fig.4. Alarm information of plant level, higher level information, are more important and less quantity. Alarm information of equipment level, lower level information, are minor important and much quantity.

Quantity	Importance
Plant Level	Plant Level
System Level	System Level
Equipment Level	Equipment Level

Fig.4. Feature of Alarm Hierarchy

3.2 Accessibility and Space Factor

TOSHIBA has introduced the concept of accessibility and space factor to assign important alarm and minor alarm with different location and tiles' size so that alarm information can assign the location and device type of the alarm information in accordance with priority of information.

In consideration of accessibility and space factor in the control room, MMI device types for displaying the alarm information are categorized as follows so that alarm information shall be assigned in accordance with priority of monitoring. In principle, the device types are categorized to three types.

- Fixed location and fixed content
- It has the highest accessibility and lowest space factors. (Ex. Hard tiles)
- Variable location and Variable content
- It has the lowest accessibility and highest space factor. (Ex. CRT)
- Fixed location and variable content

And it is important in assigning alarm information to proper device type to consider quantity and important of the alarm information.

Therefore, alarm information of plant level, more important and less quantity, shall be assigned fixed location and fixed content in consideration of accessibility. And alarm information of equipment level, minor important and much quantity, shall be assigned variable location and variable content in consideration of space factor. And also alarm information of system level shall be assigned fixed location and both fixed and variable content in consideration of accessibility and space factor.

3.3 Display Device

Table.1 shows actual design of alarm information assignment to display device. In A-PODIA, MMI devices are hierarchically adopted in consideration of accessibility and space factor.

Level	Location/ Content	Display
Plant Level	Fixed Location Variable Content	Essential Alarm
System Level	Fixed Location Variable Content	System Alarm FD(Flat Display)
Equipment Level	Variable Location Variable Content	CRT

Table.1. Device Type in A-PODIA

4. ALARM SYSTEM DESIGN

4.1 Assignment of Annunciators

(1) Plant level annunciators

Alarm information conforming to the following has assigned plant level annunciators so that operator crews can recognize important alarm information for plant safety. And since the annunciators happening in normal operation during plant start up and shutdown is not abnormal, they are handled. These annunciators consist of about 60 hard annunciators.

- 4 major events, that is SCRAM, MSIV closure, Turbine Trip and Generator Trip
- The anomalies initiating SCRAM and MSIV closure or Initial of plant safety
- (Ex. High flux, High main steam line radioactivity and actuation of ECCS)
- The Anomalies of plant safety, that is anomalies requiring Shutdown, Cooling, Containment
- (Ex. High/Low S/C water level and a bit of leakage)

(2) System level annunciators

System level annunciators have coloring function that presents fatal failure, minor failure and actuation of mitigative function with three different failure grade so that operator crews can recognize system status easily. These annunciators consist of about 120 hard annunciators.

- Fatal failure representing loss or reduction of each system function is displayed by red color.
- Minor failure representing trouble of process and equipment in each system is displayed by yellow color.

- Actuation of mitigative function representing actuation of system or consequence of operation is displayed by green color.

(3) Equipment level annunciators

Equipment level annunciators has assigned detailed causes of failed system and/or equipment so that operators crews can recover the failures easily on a basis of the assignment of System level annunciators.

- The individual anomalies causing loss or reduction of each system function
- The annunciators are displayed by red color on CRTs/FDs.
- (Ex. Redundant failure of redundant structure)
- The individual anomalies causing trouble of process and equipment in each system
- The annunciators are displayed by yellow color on CRTs/FDs.
- (Ex. Single failure of redundant structure)
- The individual anomalies effected by actuation of system or consequence of operation are displayed by green color on CRTs/FDs.
- (Ex. Flow runback by reactor re-circulation control system)
- And the annunciators happening in normal operation during plant start up and shutdown has assigned actuation of mitigative function as consequence of operation.
- (Ex. Turbine Trip)

4.2 System Configuration

(1) Plant-level Essential Annunciators

Alarm information corresponding to the plant level annunciators have ranked as Plant-level Essential Annunciators. These annunciators have been located at Essential Alarm of left part of the large display panels as fixed location and fixed content so that all operator crew in the control room can recognize plant safety-related status rapidly and surely when some transient or accident occur.

(2) System-level Integrated Annunciators

Alarm information corresponding to the system level annunciators have ranked as System-level Integrated Annunciators. These annunciators have been located at System Alarm of upper part of the large display panels as fixed location and fixed content so that all operator crew in the control room can confirm easily whether system using after SCRAM has failed or not and level of anomalies of the systems in plant operation.

(3) Individual Annunciators

Alarm information corresponding to the equipment level annunciators have ranked as Individual Annunciators. These annunciators have been assigned to CRTs or FDs to display amount of annunciators so that operator crews can confirm detailed status of failed systems and/or equipment.

5. OPERATION

Alarm system for ABWR main control panels has adopted hierarchical structure so that operator crew can recognize annunciators easily when some transient or accident occurs. TOSHIBA has confirmed the operation from the location of operator crews and annunciators.

5.1 Standard Location in A-PODIA

The standard location of operator crews in A-PODIA is as shown in Fig.5.

In A-PODIA, operator crews have been located the panels as follows.

- To monitor and control with Main console, operator crews in charge of reactor side and turbine/generator side have been located.
- To monitor and control Auxiliary system at lower of the large display panels, operator crew in charge of auxiliary side has been located.

5.2. Confirmation Flow in A-PODIA

Alarm System in A-PODIA consists of Essential Annunciators, System-level Integrated Annunciators in hierarchy. This hierarchical alarm system have realized as top down monitoring procedure against plant transients and accidents. Therefore, all operator crews in the control room can recognize plant status with the following procedure.

(1) The case of some transient or accident occur.

Operator crews confirm plant status with large display panels when some transient or accident occur as shown in Fig.6.

- Confirmation of 4 major events that is one of the Essential Annunciators
- Confirmation of First Hit located at upper of the Essential Alarm
- Confirmation of plant status and safety system actuation at the Essential Alarm
- Confirmation of plant essential parameters at the Large Mimic
- Confirmation of trend of essential parameters at the Large Screen Monitor
- Confirmation of failed system with system-level integrated annunciators located at upper of the large display panels

And next operator crews shall confirm cause of system failure with CRTs located on themain console and FDs located at lower of the large display panels. The following procedure is confirmation flow of the annunciators with CRTs as shown in Fig.7.

- Select [ANN] hard-wired switch located beside the CRTs on the main console
- Display of system-level integrated annunciators menu screen
- Touched selection of failed system
- The failed system is displayed by flicker with three different colors on CRTs
- Display of the detailed status of failed system and/or equipment with individual annunciators for the system

(2) The case of single failure occurs.

Large monitor screen can display the annunciators with message type and in order of happening that are the same as individual annunciators on CRTs. Operator crews can confirm alarm information with large screen monitor when single failure occurs as shown in Fig.8.

- Confirmation of failed system with system-level integrated annunciators
- Confirmation of message annunciators displayed Large Screen Monitor

And next confirming flow of operator crews by CRTs is the same as the case of some transient or accident. However, operator crews are not necessary to see CRTs as they can confirm detailed causes of failed system and/or equipment with large monitor screen.

5.2 Evaluation

Alarm system in A-PODIA introduced hierarchical structure has been able to confirm the evaluation as follows.

- By introduction of Essential Alarm Panel and System-level Integrated Annunciators, all operator crews in the control room have been able to recognize the anomalies instantly against plant transient and accident and recognize in common important information for plant safety and system status.

- By application of CRTs/FDs, amount of annunciators have been able to display easily in compact Man Machine Interface and operator crews have been able to confirm detailed cases of failed system and/or equipment to recover.

- As all operator crew including supervisor in the control room have been able to recognizeplant status with large display panels, the communication to inform plant status is not necessary. Therefore, operator crews have been able to monitor and control rapidly and surely without delay.

6. CONCLUSION

With the development of ABWR Main Control Room, TOSHIBA had developed hierarchical alarm system, which consists of plant-level essential annunciators, system-level integrated annunciators and individual annunciators.

It is important for operator crews to get the efficient and integrated information. This system has achieved reduction and optimization of hard annunciators, classification and systematization of important alarm for plant safety and minor alarm and assignment of important alarm and minor alarm with different location and tiles' size. Therefore, this system has realized easier recognition of distinguished important information for plant safety, and easy understandable priority with each integrated annunciators and their prioritized color. Finally improvement and effectiveness of this alarm system has been confirmed through fullscope simulator and experience of actual ABWR plant in Japan.

REFERENCE

[1] M.Makino,et al, "Operational Experience of Human Friendly Control and Instrumentation System for BWR Nuclear Power Plants", presented at ANS Topical Mtg. on Anticipated and abnormal Transients in Nuclear Power Plants, Atlanta,(1987).

[2] K.Iwaki, "Control Room Design and Automation in the Advanced BWR (ABWR)", presented at IAEA Int'l Symposium on Balancing Automation and Human Action in Nuclear Power Plants, Munich(1990).

[3] R.A.Ross,et al, "Control Room Design and Automation in Advanced BWR (ABWR)", IEEE Power Meeting,(1990).

[4] H.Nishiyama,et al, "Integrated Automation System of Control Rod Maneuvering for ABWR in Japan", presented at EPRI Conference on Advanced Digital Computers, Controls, and Automation Technologies for Power Plants, San Diego.

[5] S.Kawakami,et al, "ABWR C&I System and its Simulator", presented at 1994 Simulation Council, Inc. Required, with permission, from Proceedings of the 1994 Simulation Multiconference sponsored by the Society for Computer Simulation, San Diego, California, USA, Apr. 10-14, 1994, pp. 7-12.

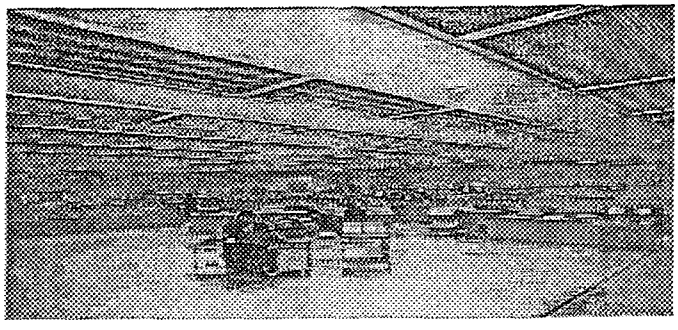


Fig.1-1 The First Generation MCR Design

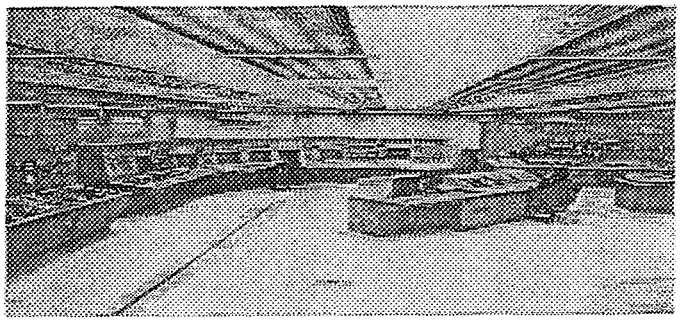


Fig.1-2 The Second Generation MCR Design
(PODIA)

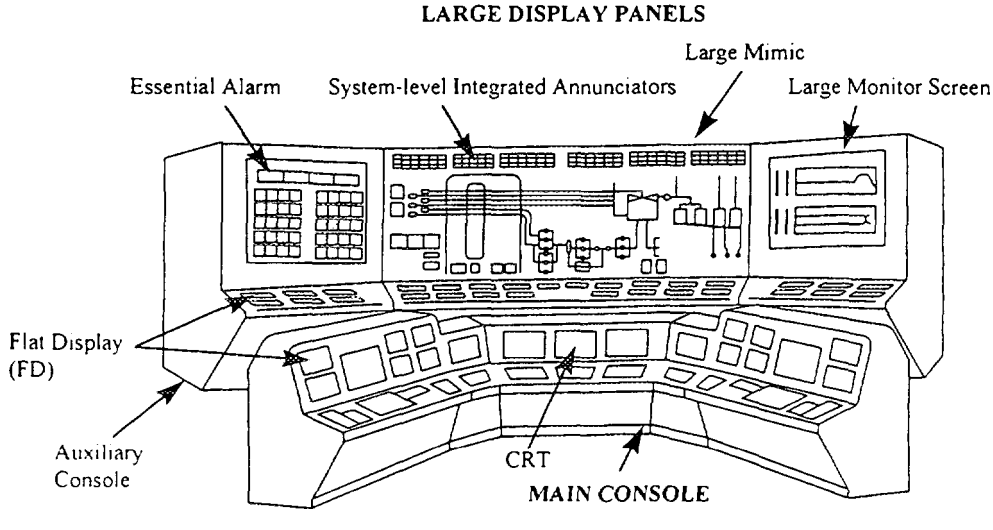
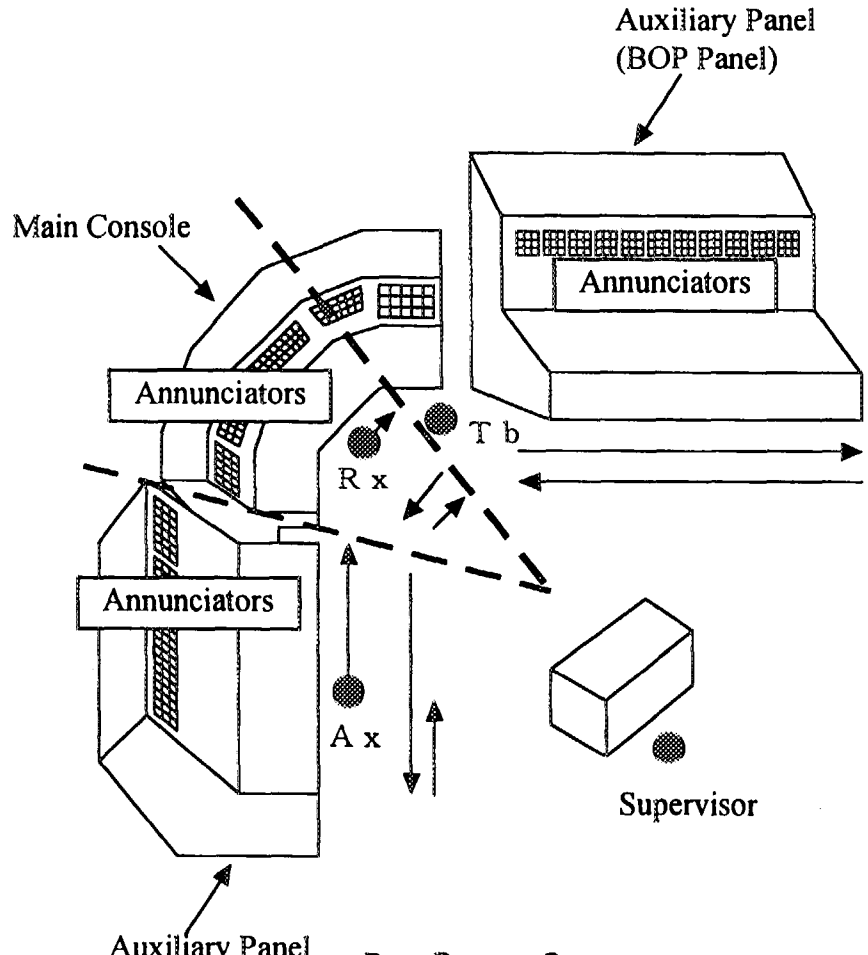
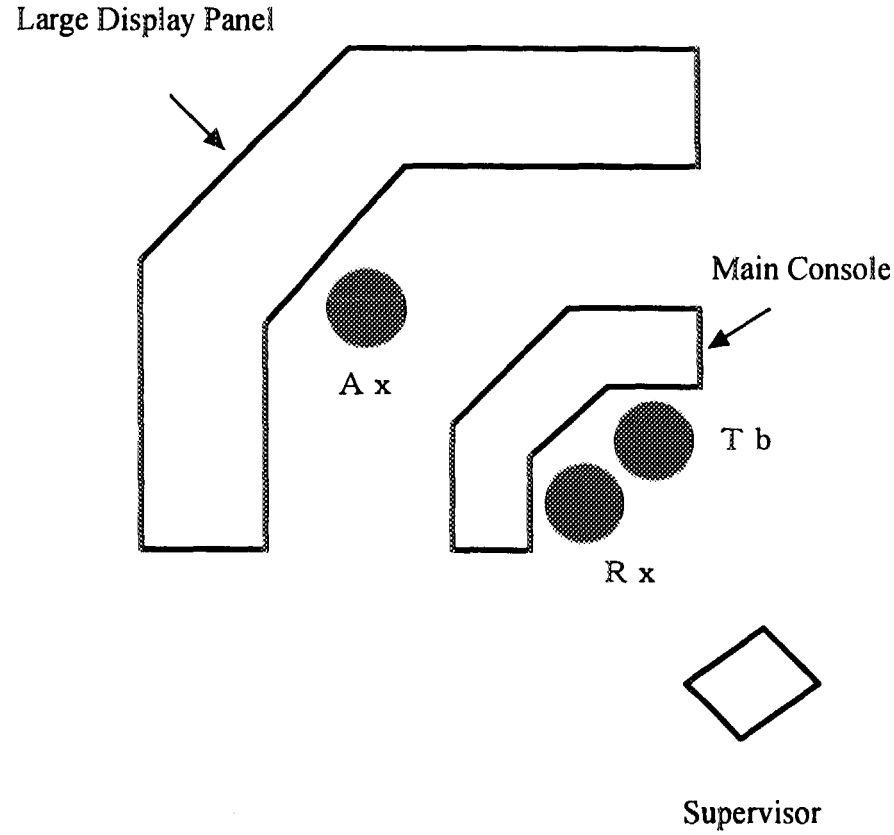


Fig 2 The Third Generation MCR Design
(A-PODIA)



Rx : Reactor Operator
Tb : Turbine Operator
Ax : Auxiliary Operator

Fig.3. Annunciators and Operator Crews in PODIA



Rx : Reactor Operator
Tb : Turbine Operator
Ax : Auxiliary Operator

Fig.5. Standard Location in A-PODIA

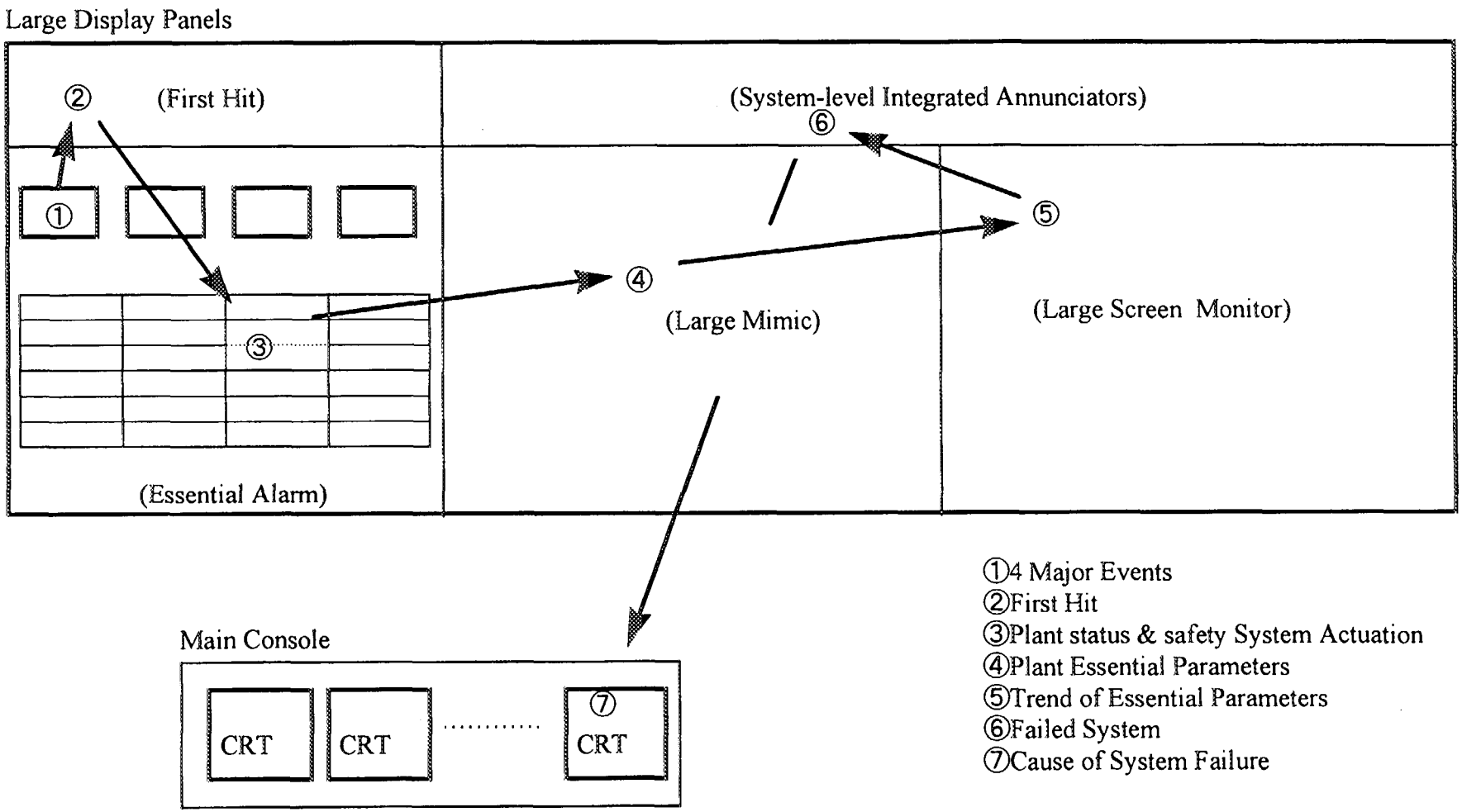


Fig.6. Confirmation Flow with the Large Display Panels in A-PODIA

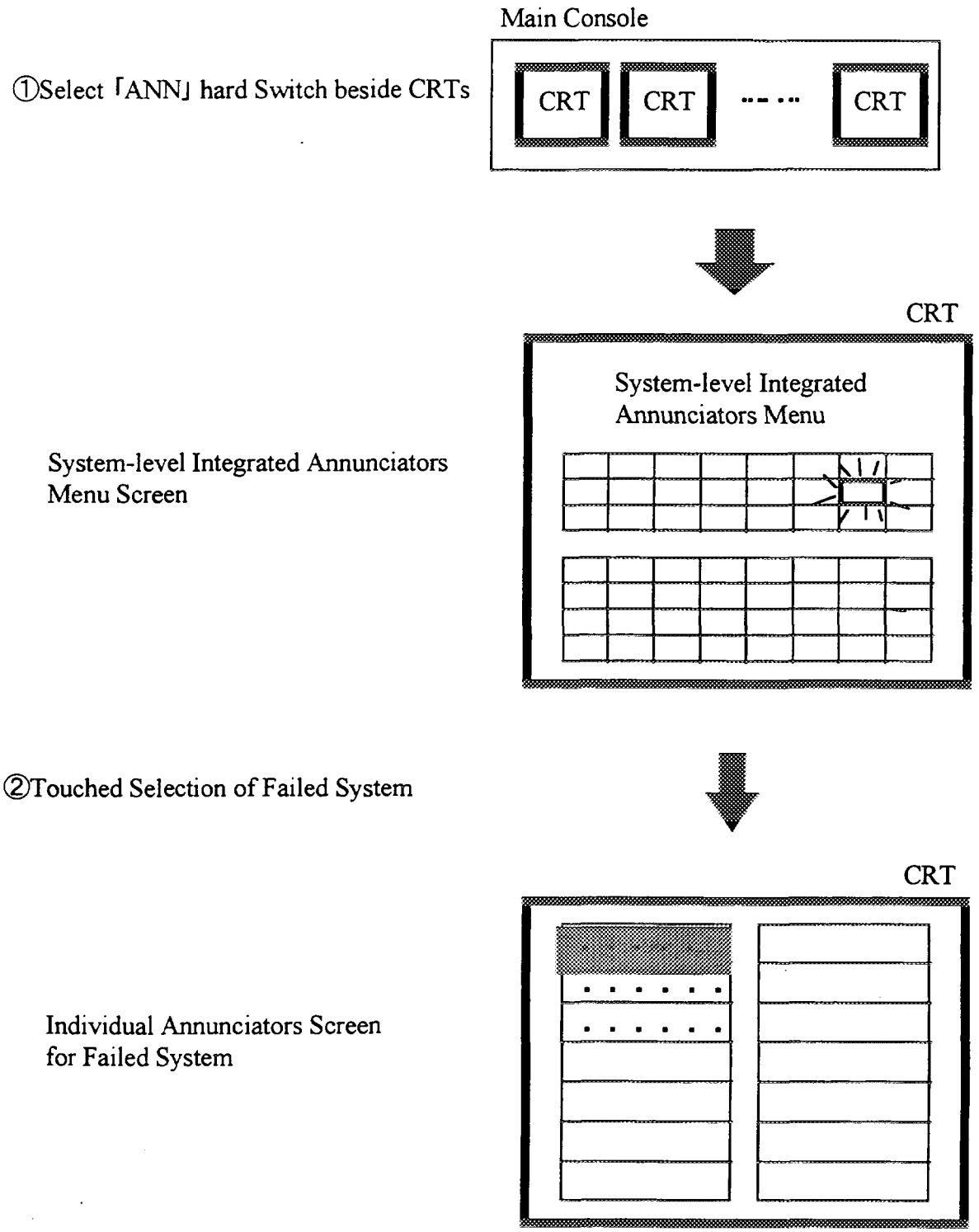


Fig.7. Confirmation Flow with the CRTs

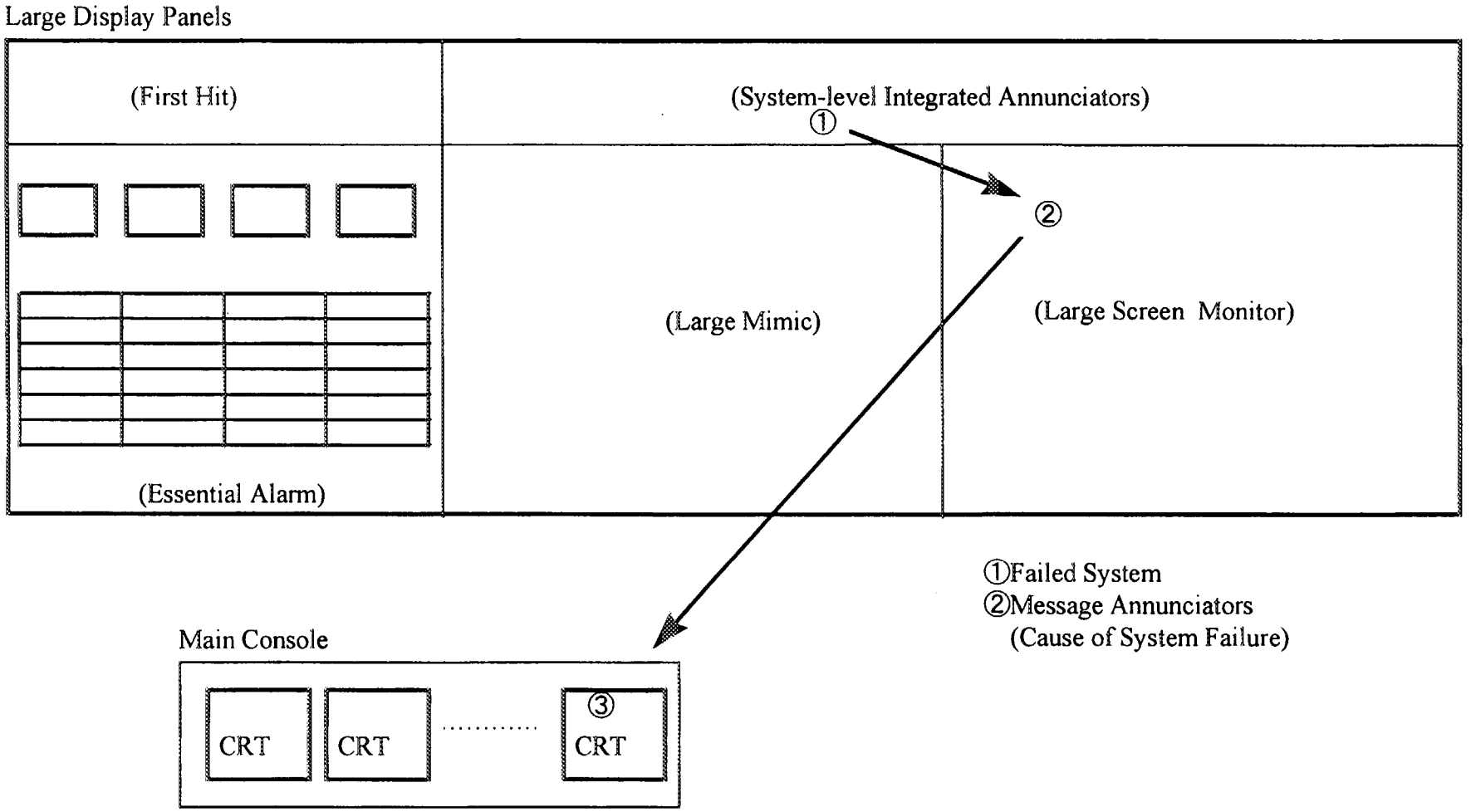


Fig.8. Confirmation Flow with the Large Monitor Screen in A-PODIA

REACTOR ALARM SYSTEM DEVELOPMENT AND APPLICATION ISSUES

J.E. Drexler, G.O. Oicese
INVAP S.E.
Argentina

ABSTRACT

The new hardware and software technologies, and the need in research reactors for assistance systems in operation and maintenance, have given an appropriated background to develop a computer based system named "Reactor Alarm System" (RAS).

RAS is a software package, user oriented, with emphasis on production, experiments and maintenance goals. It is designed to run on distributed systems conformed with microcomputers under QNX operating system.

RAS main features are: a) Alarm Panel Display, b) Alarm Page, c) Alarm Masking and Inhibition, d) Alarms Color and Attributes, e) Condition Classification and f) Arrangement Presentation.

RAS design allows it to be installed as a part of a computer based Supervision and Control System in new installations or to retrofit existing reactor instrumentation systems.

The analysis of human factors during development stage and successive user feedback from different applications, brought out several RAS improvements: a) Multiple-copy alarm summaries, b) Improved alarm handling, c) Extended dictionary, and d) Enhanced hardware availability.

It has proved successful in providing new capabilities for operators, and also has shown the continuous increase of user-demands, reflecting the expectations placed today on computer-based systems.

1. INTRODUCTION

During the 80's new hardware and software technology availability became a way to satisfy the increasing demand for assistance systems in the nuclear operation and maintenance areas. INVAP Nuclear Instrumentation and Control carried out the development, design and implementation of an advanced alarm system applied to research nuclear reactors. This system is named "Reactor Alarm System", abbreviated RAS.

One of the main goal of RAS is to provide the capability to manage the quantity, prioritization and presentation of real-time process alarm messages in the main plant locations (main control

room, secondary control room, maintenance centers, and supervision points). Ergonomic help to operation and maintenance goals have been emphasized.

RAS basic design principles aim to fulfill with:

- Display alarm information to enable the operator to understand the fault situation, avoiding information overload.
- Allow the operator to remove irrelevant information and ensure that the important information is presented in a simple and structured way.
- Enable the operator to distinguish clearly alarms for which corrective actions should be taken immediately, alarms which permit delay actions, and less important alarms which require the intervention of maintenance service.

The alarm system has:

- Processing Functions: to give the operator the most representative information of abnormal condition, and
- Presentation Functions: to permit the operator to identify easily an alarm and its importance.

The objective was to employ advanced digital technology to solve the problems associated with construction, operation and maintenance of nuclear reactor alarm systems.

2. DESIGN CRITERIA AND REQUIREMENTS

The RAS system was developed and its architecture selected according to the following design criteria:

- SIMPLICITY

  Low number of hardware components within the system, with low diversity of types; simple interconnection structure between system components due to its horizontal logic structure; low number of software components because of the use of equal platforms on each processor.

- RELIABILITY

  System low error rate due to structured development methodology, intensive verification and validation testing, highly reliable hardware components, redundant node / network design.

- MAINTENANCE

  Simple maintenance of hardware components, by board replacement; low diversity and low number of spare components; configuration management support.

- STANDARDIZATION

  Multiple source availability of all hardware components; use of market standard communication interfaces; use of highly proven and easily available hardware and software platforms.

- MODULARITY & FLEXIBILITY

  Simple implementation of changes to the interfaces of the system; quantitative increase possibility, e.g. addition of signals, new functional requirements, etc.; simplicity to add new software modules.

The key requirements for RAS design and development were:

- A fast processing of large number, multiple type of alarms.
- A simple and comprehensive selection of alarm trigger conditions.
- A fitted timing synchronization in presentation functions, immediately after alarm triggering.
- A monitor and panel based man-machine interface with straightforward graphic and table presentation.
- Multiple reporting points.

3. SYSTEM ARCHITECTURE

A physically distributed architecture was selected to implement the RAS.

The general architecture of the system has a clearly defined hierarchy of three processing levels:

- Supervision level
- Control process level
- Field level

and two communication levels:

- Supervision communication network level
- Control process communication network level

Each processing level is conformed by a set of units:

1) Supervision Unit (SU): These units, which run the man-machine interface, are used for reactor alarm presentation and historical data recording.

2) Control Unit (CU): These units are used to collect and centralize plant data from all field units, to execute all alarm detection algorithms, and to calculate the present plant alarm status. Control functions can also be implemented at this level.

3) Field Unit (FU): These units are in the boundary of the system and constitute the link to sensor devices. Input data from plant sensors is acquired, conditioned and processed here. The RAS interface with the Reactor Protection System signals is located at this level.

The two communication network levels are implemented with simple redundancy in order to increase the availability of the system.

The communication systems are based on communication networks of horizontal behavior, where all nodes connected to this network are enabled to communicate directly with each other. The horizontal structure of each communication network assigns the same communication priority to all nodes connected to them.

The real-time data-base system is functionally distributed among all control units in order to enable the transient operation of these units independently of the status operation of other units or the communication network.

Figure 1 shows the general architecture and levels above mentioned of the RAS.

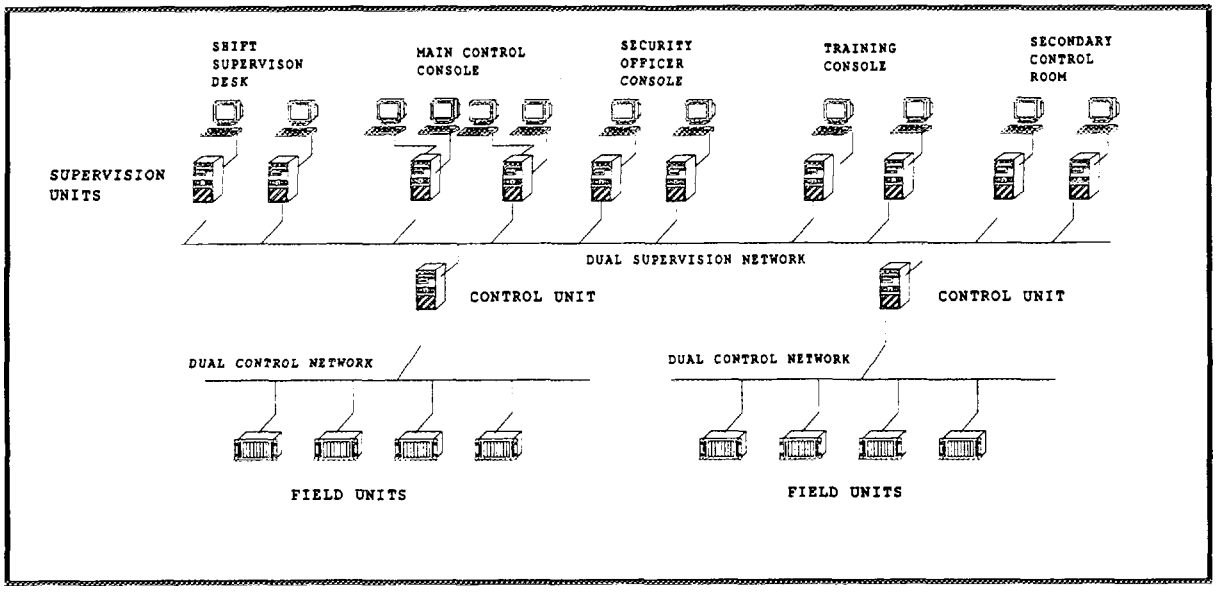


Figure 1: RAS Architecture

RAS system is able to carry out processing tasks and alarm presentation through the following devices:

- Video display Units through dedicated pages and mimics
- Printers
- Optical and acoustics annunciation
- Historic data base record

- Keyboards, touchscreens and trackballs input.

A modular design allows it to be installed both as a part of a computer based Supervision and Control System in new installations or to Retrofit existing Reactor Instrumentation System.

4. HUMAN FACTORS

Human engineering design concepts were taken into account during the development stage. The alarm consoles layout and equipment selection followed standard recommendations.

The analysis of human factors during RAS development, under successive user feedback, from different applications, brought out the following RAS improvements:

- Multiple-copy alarm summaries: Complete alarm plant status overview is provided to operators at more than one screen/console panel.
- Improved alarm handling: When several alarms are detected in a small time frame, the system provides easy means to cope with all information. It aids the operator to determine the importance of each alarm, the relation between them, the previous and subsequent events in time and an appropriate acknowledgment of each one.
- Extended Dictionary: An on-line data dictionary allows getting a detailed description about signals, alarms, events, equipment, parameters, limits and operational states.
- Enhanced hardware availability: RAS hardware and software component are based on current industrial standards products to ease maintenance and future upgrades.

5. FUNCTIONAL DESCRIPTION

5.1 Alarm Trigger Conditions

Alarms are generated from the following conditions:

1) Analog variables: All analog signal values are checked if they are going above or below one or more limits.

   The system limits defined are:

   - Absolute Very High
   - Absolute High
   - Absolute Low
   - Absolute Very Low
   - Rate of change

2) Digital variables: Digital variables are compared with its normal state. If a variable changes to its abnormal state an alarm is generated.

3) Inconsistent states: The system checks the inconsistency between signals which indicate directly or indirectly the same component or process state.

The above conditions are applied to real or virtual variables. Virtual variables are calculated by specific software modules.

5.2 Alarm Classification

Alarms are arranged in groups according to their relevance as follows:

- Safety alarms
- Safety related alarms
- Non-safety related alarms

This classification is denoted by coding the alarm message leading a character before the tag description. The convention for this coding is as follows:

"A": Safety alarms
"B": Safety related alarms
"C": Non-safety related alarms

The alarm display system has also the capability to classify and differentiate alarms according to the system they belong to, they are:

- Plant systems
- Reactor protection system
- Supervision and control system
-

Each alarm, besides its status identification character, has a system identification tag.

The reactor operator can select those alarm messages belonging to a particular system in order to obtain group classification.

Figure 2 shows the RAS Functional Description Block Diagram.

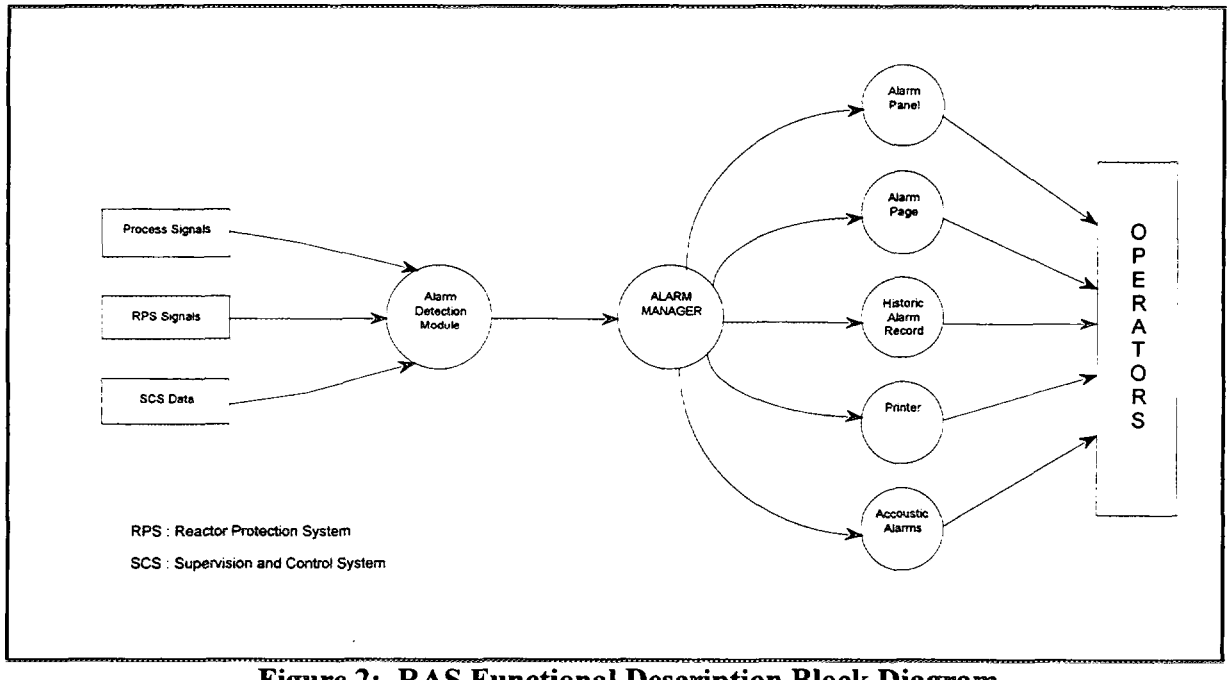


Figure 2: RAS Functional Description Block Diagram

6. RAS MAIN FEATURES

6.1 Alarm Panel

Alarm Panel graphic picture is conformed by a set of tiles. Each one shows a summary of current alarm state of a particular plant subsystem. In that way an top-down alarm presentation approach is used.

Figure 3 shows an example of alarm panel.

6.2 Alarm Page

When a specific tile is selected, the system shows a detailed alarm information about the related process. Alarm events are presented in chronological order, placing the latest alarm at the top of the page.

Alarm message description, associated tag, trigger time, normalization time, alarm state condition, and safety code are displayed for each alarm.

A typical alarm page is shown in figure 4.

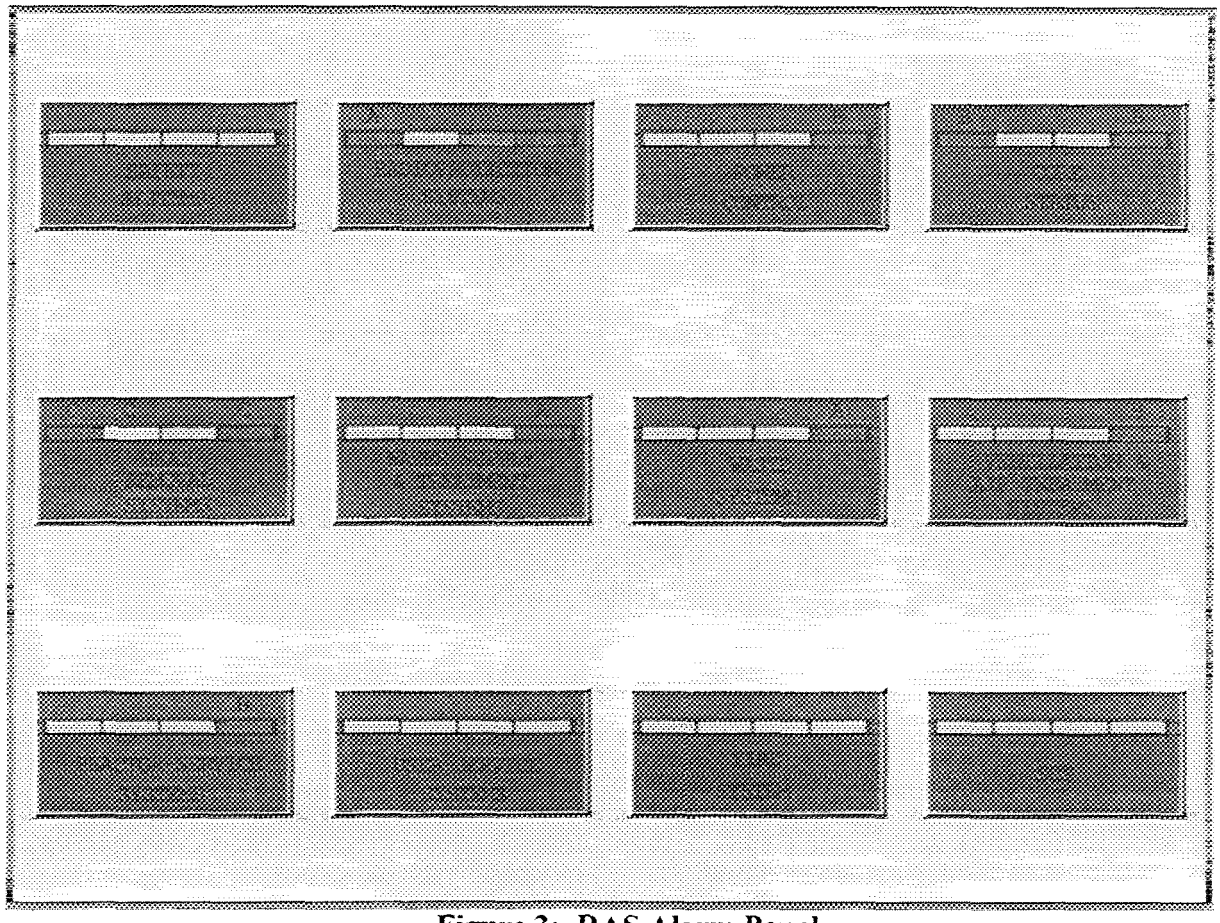


Figure 3: RAS Alarm Panel

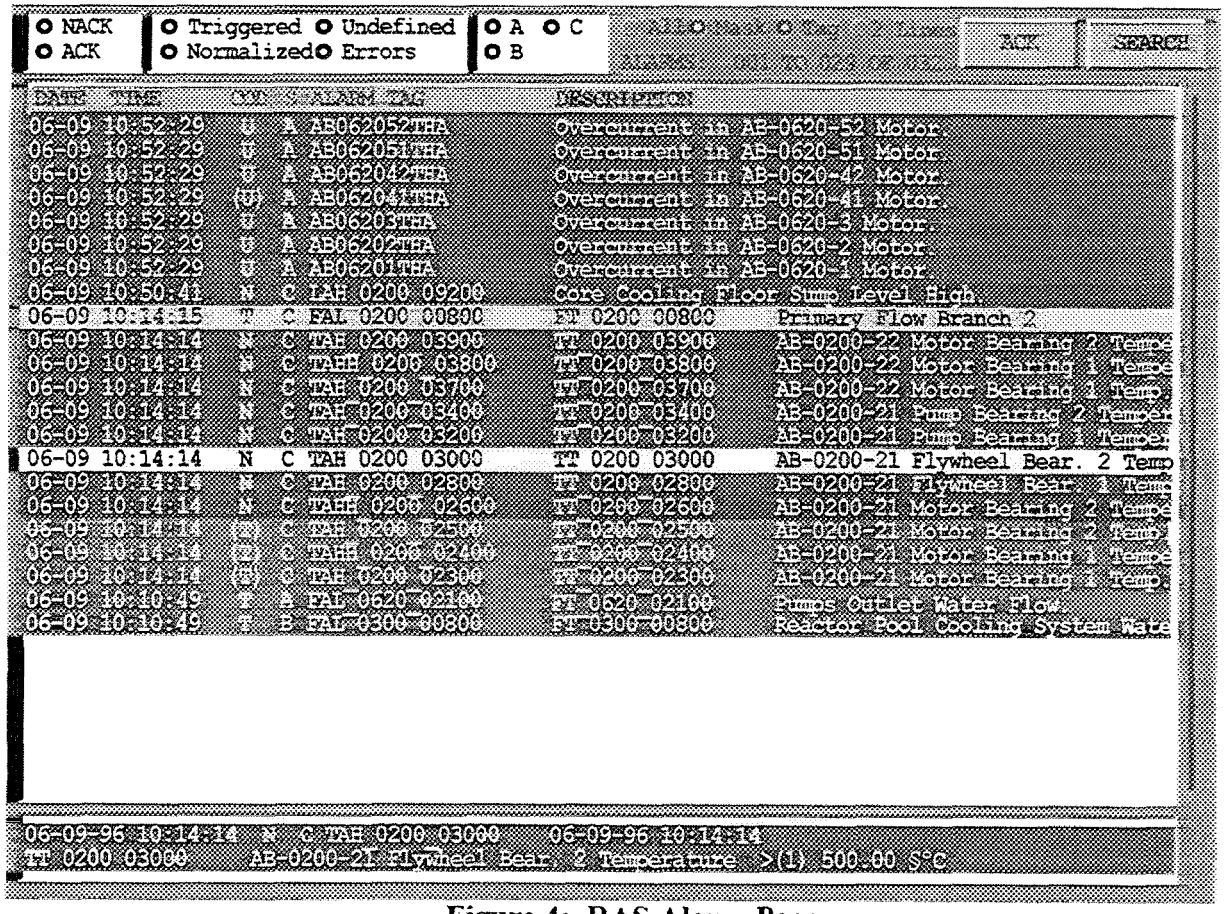


Figure 4: RAS Alarm Page

6.3 Alarm Masking

In order to avoid overcrowded alarm displays, the system enables on-line selection of particular alarms the operator wants to visualize.

Alarm Masking display process filters the presentation of all unimportant alarm information in order to reduce the presentation.

This means that the system displays only those alarms that meet the conditions set by the operator. For example, when an alarm gets activated due to very high level, it makes no sense to display a high level alarm.

Three ways of reduction are fulfilled using the following alarm masking methods:

- Priority masking (hiding less relevant alarms when safety related alarms are requested),
- Hierarchy masking (hiding "high" level alarms whenever "very high" level alarms are active), and
- Cause-effect relation masking.

The operator can select which masking method to apply. Method combination is also permitted.

Masking process just filter the alarm presentation, never suppress an alarm. The masked alarms could be presented to the operator by demand at any time.

Should masked alarms exist after any masking method is applied, a notification will be generated in a system status screen.

6.4 Alarm Inhibition

Alarm Inhibition tasks are implemented in order to avoid non-significant alarms messages, therefore the system inhibits the trigger of some alarms according to process states. For example a component is not in service all associated alarms are disabled.

In order to reduce the amount of active alarms displayed on screen, the system can perform conditional alarm suppression of non-relevant alarms.

This means that the system can ignore certain alarm activation under specific conditions. Each alarm has its own conditioning parameters. When an alarm exceeds its threshold it gets activated only upon conditioning parameter activation.

As an example, low pump discharge pressure alarm is not activated while the pump is turned off:

> Alarm: low pump discharge pressure
> Conditioning parameter: pump turned on

It is important to note that the system doesn't stop processing alarm information, it just structures and prioritizes its presentation so that it makes sense in a specific situation.

An specific RAS task may inhibit, or not, the alarm triggering of all alarm groups according the state and substates of reactor plant (Operation, Maintenance, Refueling and Testing).

6.5 Alarm Color and Attributes

The use of different color and attributes in display information allows the operator to know the plant state in clear and simple way.

Each alarm displayed is identified by a code which could be blinking or not depending on the alarm condition and state of acknowledgment.

All possible codes meaning are:

- 'T' (blinking): Triggered alarm that remains without acknowledgment.
- 'T' (static): Triggered alarm that has been acknowledged.

- 'N' (blinking): Normalized alarm that remains without acknowledgment.
- 'U' (blinking): Undefined alarm that remains without acknowledgment.
- 'U' (static): Undefined alarm that has been acknowledged.

The following tables show the alarm condition and their associated color and attribute.

Alarm State	Color	Code (*)
Triggered Alarm	Red	T
Triggered Warning	Yellow	T
Normalized	Green	N
Undefined	Blue	U

Alarm Acknowledgment	Color	Code (*)
Not acknowledged	Blinking	*
Acknowledged	Static	(*)

6.6 Arrangement Presentation

6.6.1 Presentation Ordering

Alarm ordering criteria for operator display are the following:

- Chronological activation ordering
- Safety level ordering
- Activation/Normalization ordering
- Acknowledged unacknowledged classification
- Relevance classification
- Subsystem classification

6.6.2 Filtering

Different display filtering option are available for VDU's alarm presentation. Users can harness the filter option in a easy and quickly manner, through special keys or sensitive option selection touchscreen area.

This options are:

- Filter non acknowledged alarms
- Filter acknowledged alarms
- Filter safety alarms.
- Filter safety related alarms.
- Filter non-safety related alarms.

Filter options are displayed at the upper sector of an alarm page. There are sensitive buttons for proper selection through touchscreen and trackball pointing devices.

6.7 Access Control

RAS system has an hierarchical operator access command control.

Through access control the system enables or disables certain options depending on operator hierarchy level assigned to the system. Control access is implemented by personal passwords.

As an example, main control room operators don't need to introduce a password to acknowledge an alarm, but a maintenance operator requires to input a password to acknowledge a maintenance alarm meanwhile is completely forbidden for his hierarchy to recognize any alarm related to main control room operation.

Any action to change an alarm parameter requires a determined hierarchy level and input a password.

6.8 Historic Alarm Page

The historic alarm page presents a list of detailed alarm messages that has been generated during a period of time.

RAS system manages an historic alarms data base which log all alarms events. Alarm pages retrieve the necessary alarms data produced during a user-defined time frame.

Also this historic reports can be printed in a hard copy.

Figure 5 shows an example of Historic Alarm Page.

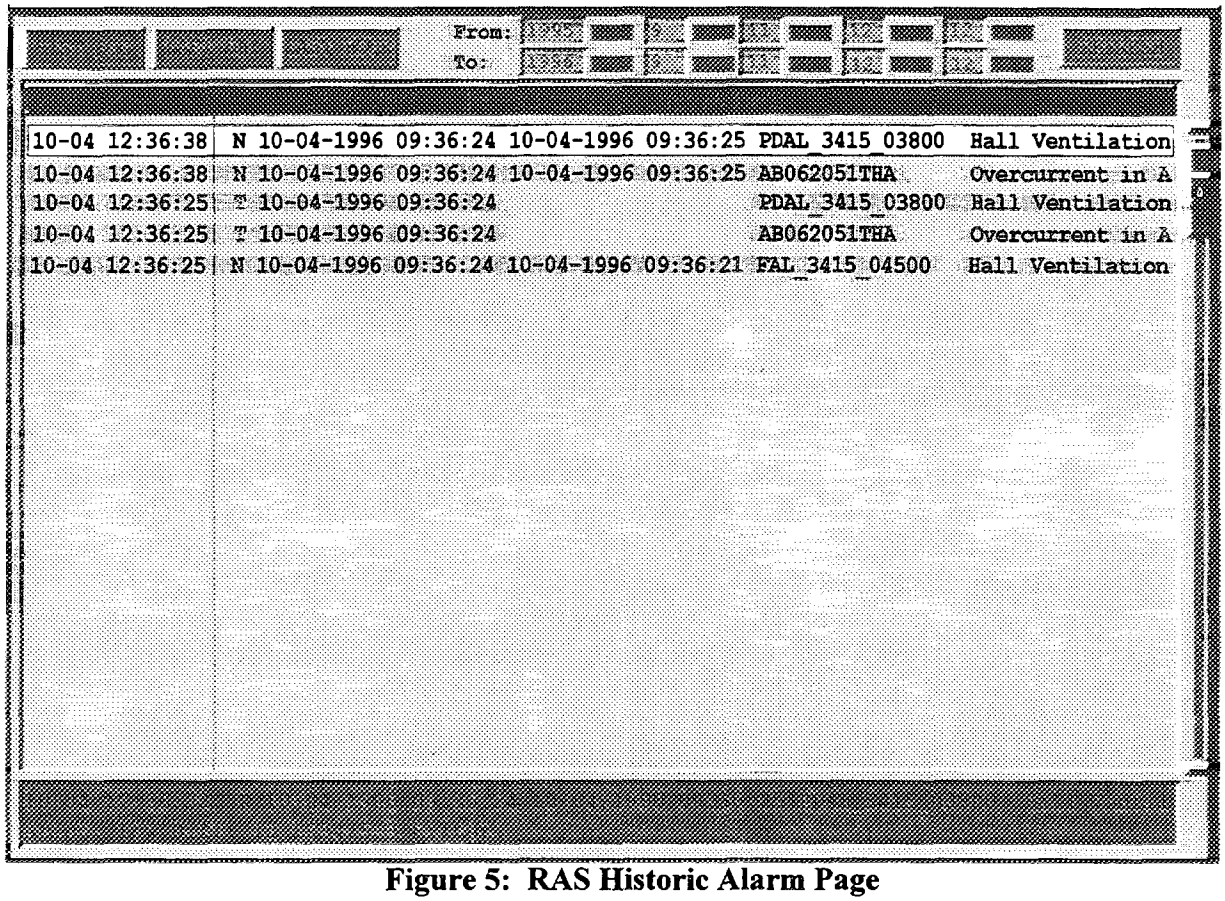
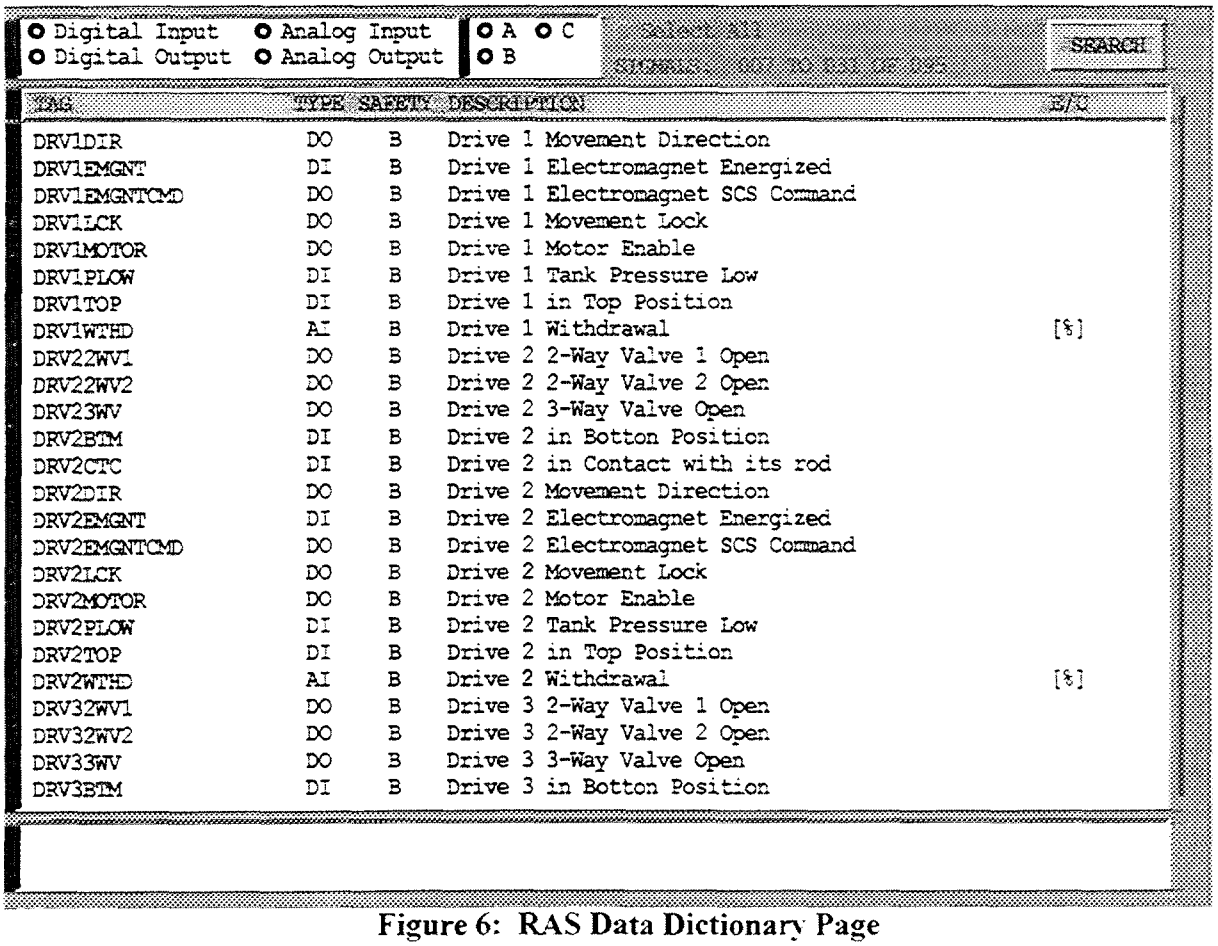


Figure 5: RAS Historic Alarm Page



TAG	TYPE	SAFETY	DESCRIPTION	E/U
DRV1DIR	DO	B	Drive 1 Movement Direction	
DRV1EMGNT	DI	B	Drive 1 Electromagnet Energized	
DRV1EMGNTCMD	DO	B	Drive 1 Electromagnet SCS Command	
DRV1LCK	DO	B	Drive 1 Movement Lock	
DRV1MOTOR	DO	B	Drive 1 Motor Enable	
DRV1PLOW	DI	B	Drive 1 Tank Pressure Low	
DRV1TOP	DI	B	Drive 1 in Top Position	
DRV1WTHD	AI	B	Drive 1 Withdrawal	[%]
DRV22WV1	DO	B	Drive 2 2-Way Valve 1 Open	
DRV22WV2	DO	B	Drive 2 2-Way Valve 2 Open	
DRV23WV	DO	B	Drive 2 3-Way Valve Open	
DRV2BTM	DI	B	Drive 2 in Botton Position	
DRV2CTC	DI	B	Drive 2 in Contact with its rod	
DRV2DIR	DO	B	Drive 2 Movement Direction	
DRV2EMGNT	DI	B	Drive 2 Electromagnet Energized	
DRV2EMGNTCMD	DO	B	Drive 2 Electromagnet SCS Command	
DRV2LCK	DO	B	Drive 2 Movement Lock	
DRV2MOTOR	DO	B	Drive 2 Motor Enable	
DRV2PLOW	DI	B	Drive 2 Tank Pressure Low	
DRV2TOP	DI	B	Drive 2 in Top Position	
DRV2WTHD	AI	B	Drive 2 Withdrawal	[%]
DRV32WV1	DO	B	Drive 3 2-Way Valve 1 Open	
DRV32WV2	DO	B	Drive 3 2-Way Valve 2 Open	
DRV33WV	DO	B	Drive 3 3-Way Valve Open	
DRV3BTM	DI	B	Drive 3 in Botton Position	

Figure 6: RAS Data Dictionary Page

7. CONCLUSION

In retrospect, different evolutionary version of RAS have been installed in an uranium enrichment plant, a thermohydraulic test facility and two research reactors. It is also under pre-shipment qualification test for application in a 22 MW multi-purpose research reactor.

It can be easily verified that implementing a digital alarm system in a research reactors, and nuclear facilities contributes to increase the operators understanding of abnormal plant state, while simultaneously creating new duties.

In the past (one decade ago) this represent a "cultural" change to plant operation. Recently this picture has been changing drastically: Operators expect and cope with enhanced system functions.

In all applications the alarm system insertion has finally had a great acceptance by operational and maintenance personnel. Before a short period of use the users demand to incorporate new functions to the alarm system.

The final conclusion is that RAS, and probably all advanced alarm system, are successful in providing new capabilities for operators, and generate a continuous increase of user-demands which reflects the expectations placed on computer-based system.

SESSION IV

ALARM STRUCTURING AND DESIGN TOOLS

AN OBJECT-ORIENTED IMPLEMENTATION TO IMPROVE ANNUNCIATION

In-Koo Hwang, Jung-Taek Kim, Dong-Young Lee, Jae-Chang Park and Chang-Shik Ham
Korea Atomic Energy Research Institute
Republic of Korea

ABSTRACT

A computer-based alarm processing system for nuclear power plants is being developed in a G2 expert system software tool. In the G2 environment, every alarm is treated as an object of alarm class. The attributes of each alarm object include activation status, alarm message, process value, time, priority, acknowledgment state, and icon color. If an alarm is activated, its icon color, on an overview process mimic diagram changes corresponding to its priority which can be set initially or determined dynamically by reasoning rules and procedures. The process conditions, such as plant or equipment status and correlated alarms' states determine the priority of the activated alarm. The knowledge base of the system is constructed by process analysis of the plant and discussion with operators and nuclear plant experts.

1. INTRODUCTION

Although alarm information is the primary source for detection of abnormalities in nuclear power plants or other process plants, the conventional hardwired alarm systems, characterized by "one sensor-one indicator", has an alarm flooding problem[1]. Much research work has been done worldwide to help resolve this problem of cognitive overload [1-3]. The advanced I&C research team of the Korea Atomic Energy Research Institute (KAERI) is developing an Alarm and Diagnosis - Integrated Operator Support (ADIOS) system for computerized process monitoring, alarming, and diagnosis. As our initial effort, we are working on an alarm system using a G2 real time expert system shell[4] to devise the basic concepts of alarm processing and a generic architecture for processing and presentation.

The bases of implementing any expert system in G2 are production-system(IF-THEN-ELSE types of rules) and an object-oriented knowledge representation scheme. Various equipment of a nuclear power plant, such as condensate pumps or the pressurizer, and various alarms, like process alarms or temperature alarms, are hierarchically defined in G2 to take the advantage of inheritance of object properties. The attributes of each class or object are then determined to facilitate knowledge-based processing of alarm signals, sometimes augmented by raw process parameters.

In ADIOS, alarms are processed by several representative methods including state dependency, mode dependency, and a multi-setpoint relationship[1]. The processing of alarm signals is clearly seen on the process schematic diagram constructed using the graphic interface of G2. The equipment-related alarms(e.g., vibration or lubrication alarms of a pump) are separated from

the process alarms (e.g., temperature or pressure alarms of the main process) on the process mimic. Group alarms are introduced to assimilate several related alarms into one alarm[5]

This paper discusses the architecture of the knowledge base of ADIOS, focusing on alarm processing, along with the inference scheme. Also discussed herein are the advantages of, and some issues in, developing an improved alarm system in an object-oriented environment, and also using a real-time AI tool, such as G2.

2. CLASS DEFINITION AND OBJECT PROCESSING IN ADIOS

2.1 Definition of Alarm Objects

Every alarm is defined as an object of a subclasses of ***Alarm*** class, the attributes of which include message text, process value, set-point, activation status, priority, acknowledgment or reset status, causal alarm, level precursor, and so on , according to its class. Subclasses of alarms are defined for different use in the processing scheme of ADIOS: process alarms, e.g., a pressure alarm in the main process line, and equipment alarms, e.g., a vibration high alarm.

Each alarm object with those attributes contains most of the information necessary for alarm processing and display control. Some attributes of the alarm object change their values dynamically during a run of the alarm system. The process value of an alarm gets its value from the corresponding process variable of the plant or simulator. The attribute value of the acknowledgment or reset status is used to control the flashing display depending on the acknowledgment status of the alarm when it is activated or deactivated. Table 1 illustrates an attribute table of an alarm object.

The attributes of a causal alarm and level precursor are used in prioritizing the alarms based on the relationship among alarms. The processing of alarms is discussed below in more detail.

For implementing the state-dependency, ***relation*** provided in G2 has been used. Any alarm object which can be active as a result of any equipment state, for example, pump ON or pump OFF, is defined to have a relation to its corresponding equipment.

2.2 Alarm Prioritization

Dynamic prioritization is the most important feature of alarm processing in this system. Figure 1 shows how the alarms are processed and presented in ADIOS. As in conventional alarm systems, alarms are generated by set-point checking. They are activated when the associated process values exceed the alarm set-points, and deactivated when they return to their normal values.

The activated alarms then get into the prioritization phase to conclude their priority depending on several conditions related to them. Those conditions would be plant operation mode, equipment status, related alarm status and so on. They are called plant-mode dependency, equipment-state dependency, multiple set-point relationship (i.e., level precursor), causality and so on[2 - 5]. In

the present version of ADIOS, all alarms are initially given their own default priorities, and, those priorities can be decreased or increased by any processing algorithm dynamically during the run time of the alarm system.

The plant-mode dependency is used to de-emphasize those alarms that are activated as a consequence of the plant mode change. The equipment-state dependency is used to reduce the priority of those alarms that occur when equipment changes its status; e.g., the priority of the discharge pressure low alarm is lowered if it occurs after a pump stops. The multiple set-point relationship uses the relationship between several alarms on the same process parameter. For instance, when both the low and low-low level alarms of a steam generator are on, the priority of the low alarm can be lowered. The causality between alarms also allows us to prioritize alarms between causal and consequential alarms; the causal alarms require more attention than the consequential alarms.

2.3 Alarm Display

The prioritized alarms are displayed on the process overview mimic (Figure 3.), and the time-sequential list of alarms is given on another dedicated CRT, with those alarms categorized by systems shown on a third CRT acting as a spatially dedicated soft alarm panel. The process alarms are displayed on the main CRT either in red or yellow; priority 1 alarms are shown in red, priority 2 alarms in yellow, and priority 3 in white. The same color coding will be applied to the alarm texts in the alarm list, and also to the tiles on the soft alarm panel.

Activation of any equipment alarm makes the boundary color of corresponding equipment change to red on the process overview mimic diagram. When the operator wishes to look at the specific alarms, he/she can click on the equipment after first acknowledging the alarm. Then, the specific alarms are shown on its sub-workspace.

2.4 Alarm Grouping

In a conventional annunciation window tile system, many correlated alarms have their independent alarm tiles. For example, *SG 1 Water Level High-High, SG 1 Water Level Deviation High/Low, SG 1 Water Level Low,* and *SG 1 Water Level Low-Low* are all steam generator water level alarms, however they occupy independent alarm tiles. It is one of the causes that the annunciator becomes wide and complex in the control room.

For such cases, ADIOS only one representative alarm icon resides on the overview mimic diagram. It behaves according to its member alarms' states. The most severe alarm's priority of the activated member alarms conclude the icon color of the representative alarm. *High* or *Low* indication is implemented in graphic.

2.5 Alarm Ungrouping

Contrary to the above case, some alarm information is combined into one window unit. When *SG 1 Water Level Deviation High/Low* is activated, an operator should check the SG level

indicator if he wants to know whether it is high alarm or low alarm. If the alarm, *System AL Non TRN TROU/DISA,* is active, it is not easy to find out which component or actuator is *TROUBLE* or *DISABLE.* ADIOS will resolve those kind of combined alarms and present more detailed messages.

3. SYSTEM CONFIGURATION

Figure 2 illustrates the system configuration of the ADIOS prototype. Workstation (WS) 1 is the functional test facility (FTF) of KAERI which simulates the process behavior of Kori 3&4 nuclear power plants in Korea. WS2 is the host processor for alarm processing where the G2 real-time expert system shell runs and the alarms are processed.

This host gets process data of the plant from the FTF at a regular scan interval, and displays processed alarms on the process overview mimic and also on another dedicated CRT as a time-sequential list. As discussed, the third CRT presents the processed alarms as tiles on the soft alarm panel, as in conventional alarm systems, to allow the operator's investigation of the alarms arranged in systems.

4. BENEFITS OF USING G2 OBJECT-ORIENTED EXPERT SYSTEM TOOL

G2 is composed of a knowledge-base, real-time inference engine, procedure language, development environment, operator interface, and interface to external data servers. In the expert system, the knowledge of the system is incorporated explicitly in a separated part of the program and it is readable and easy to modify because it is built incrementally, where as in every conventional programming language the knowledge is expressed in the ordinary program code [6].

For implementing ADIOS, G2 has been an effective tool in developing and programming the alarm processing concept. It was very helpful in constructing alarm objects and their attributes as they are treated as an object instance of *Alarm* class at design stage. The other typical advantageous features of using G2 were:

- Introductive Guidance of Commands: If a programmer tries to create a rule or procedure for the knowledge-base, G2 shows available texts of program commands or items which can follow next to the current statement. It makes programming much easier than conventional language coding.

- Developmental Environment in Graphics: G2 provides easy way to create objects, define classes, edit icons, and inspect the knowledge-base graphically. Therefore it gives the benefit of rapid prototyping in the development stage.

- User Interface: By use of buttons and workspaces it is easy to design and construct user interfaces to communicate with the system.

- Off-line Simulation: The built-in simulator or procedure can provide effective simulation

or off-line testing without any difficulty.

- Interface with external systems: G2 exchanges data in a easy way with external systems by GSI(G2 Standard Interface) module.

- Distributed Environment: G2 can run a application knowledge base with Tele-windows for multi-users. It makes several users develop a application knowledge base and use it simultaneously.

5. CONCLUSIONS

This paper has described the overall algorithm for processing alarm signals of ADIOS. The processing and presentation of alarms have sometimes been considered separately. However, we believe these two aspects of an alarm system should instead be considered in an integrated manner.

In developing an G-2 based alarm processing system, several issues need to be clarified. First, the construction of a reliable knowledge base is required for the practical application of the alarm system. The knowledge base should produce a reasonable processing result even for unforeseen plant transients or alarm situation. Secondly, the alarms should be presented in accordance with the operator's mental model and cognitive processing, rather than a simple reduction in the number of alarms. It also appears important to provide a quick access to any alarm information upon the operator's request, without suppressing or filtering out any alarms. Thirdly, the verification and validation of the expert system software tool is a concern and a barrier to the practical installation of the alarm system. Lastly, the G2 shell does not provide any flexible function to produce various tones of sound.

The ADIOS prototype is still under development for more advanced alarm processing and is also forwarded to a practical scale for a real application to nuclear power plants.

REFERENCES

[1] L.R.Lupton, P.A.Lapointe and K.Q.Guo, "Survey of International Developments in Alarm Processing and Presentation Techniques", *NEA/IAEA International Symposium on Nuclear Power Plant Instrumentation and Control,* Tokyo, Japan, May 18-22, 1992.

[2] I.S. Kim, "Computerized Systems for On-Line Management of Failures: A State-of-Art Discussion of Alarm Systems and Diagnostic Systems Applied in the Nuclear Industry", *Reliability Engineering and System Safety* 44 (1994) 279-295.

[3] J.M. O'Hara, W.S. Brown, J.C. Higgins, and W.F. Stubler, "Human Factors Engineering Guidance for the Review of Advanced Alarm Systems," NUREG/CR-6105, U.S. Nuclear Regulatory Commission, August 1994.

[4] Gensym Corporation, G2 Reference Manual, Version 4.0, September 1995.

[5] I.S. Kim, I.K. Hwang, D.Y. Lee, J.C. Park, and C.S. Ham, "An Integrated Approach to Alarm Processing," *2nd American Nuclear Society Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technology,* University Park, Pennsylvania, USA, May 1996.

[6] Ola Mattsson, "An Expert System for OSI", *Doc. No. CODEN:LUTFD2/(TFRT-5428)/1-89/(1990)*, Department of Automatic Control Lund Institute of Technology, Sweden, December 1990.

PZR-LVL-HI, a level-alarm	
Notes	OK
Item configuration	none
Names	PZR-LVL-HI
Tile message	"Pressurizer Level Hi"
P value	68.2
Status	off
Acknowledge or reset	initialized
Priority	1
Default priority	1
Setpoint	70
Kind	hi-alarm
Causal alarm1	none
Causal alarm2	none
Level precursor	pzr-cont-lvl-hi
Time on	"13:33:29"
Time off	none

Table 1: Attributes of an Alarm Object

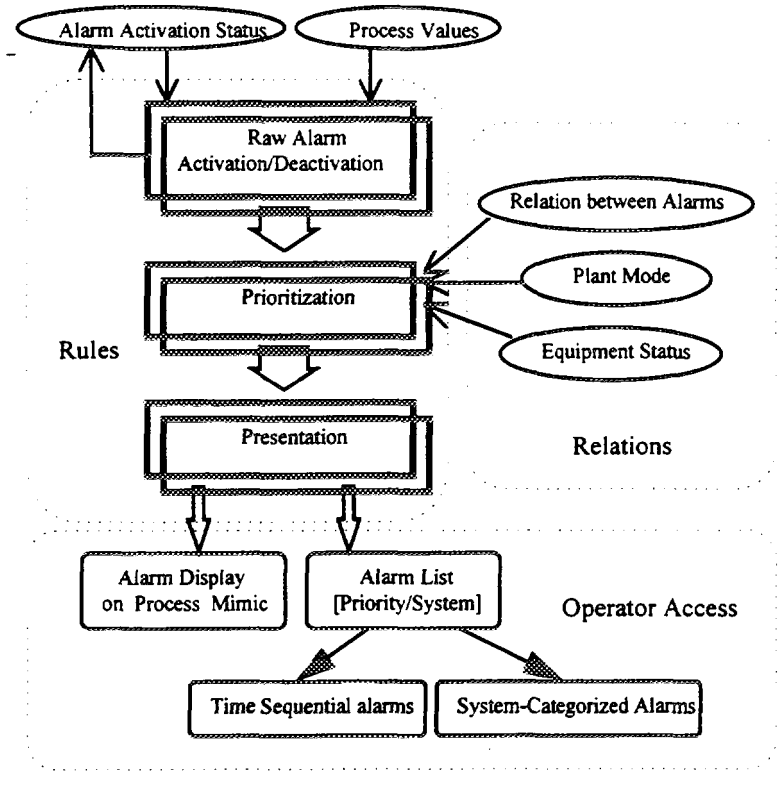


Figure 1: Alarm Processing Flow in ADIOS

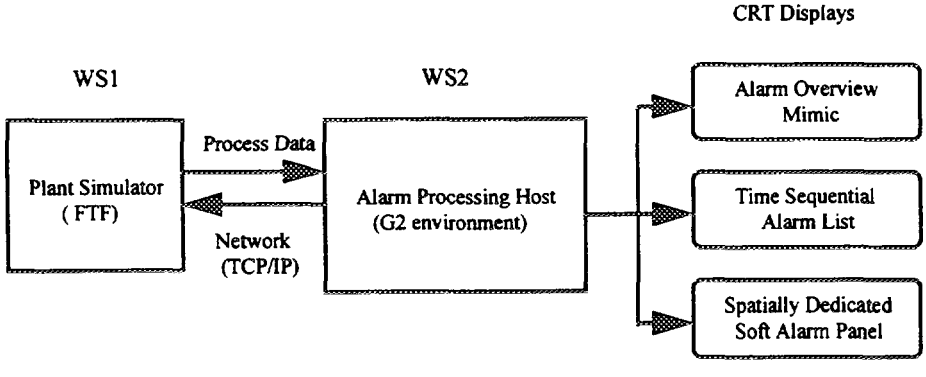


Figure 2: System Configuration of ADIOS Prototype

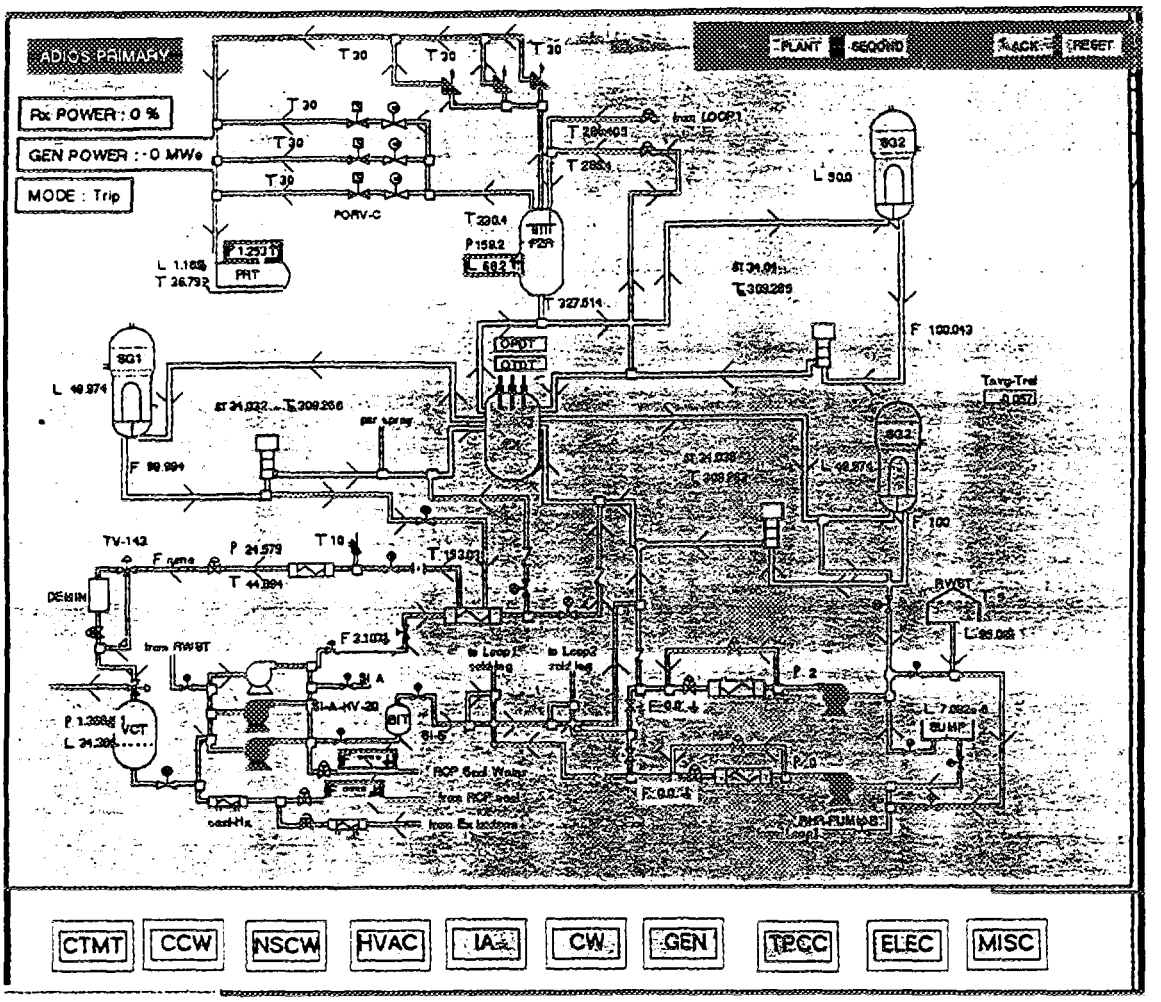


Figure 3: An Alarm Overview Mimic in ADIOS

ALARM HANDLING SYSTEMS AND TECHNIQUES DEVELOPED TO MATCH OPERATOR TASKS

Andreas Bye and Bard R. Moum
Institutt for energiteknikk, OECD Halden Reactor Project
Norway

ABSTRACT

The OECD Halden Reactor Project has for several years been working with revision, design, implementation, test and evaluation of advanced alarm annunciation systems. The methods explored include alarm processing and presentation, model-based fault detection and function-oriented plant surveillance. The systems are studied through experiments in HAMMLAB (HAlden Man-Machine LABoratory).

This paper covers alarm handling methods and techniques explored at the Halden Project, and describes current status on the research activities on alarm systems.

Alarm systems are often designed by application of a bottom-up strategy, generating alarms at component level. If no structuring of the alarms is applied, this may result in alarm avalanches in major plant disturbances, causing cognitive overload of the operator. An alarm structuring module should be designed using a top-down approach, analysing operator's tasks, plant states, events and disturbances.

One of the operator's main tasks during plant disturbances is status identification, including determination of plant status and detection of plant anomalies. The main support for this is provided through the alarm system, the process formats, the trends and possible diagnosis systems. The alarm system should both physically and conceptually be integrated with all these systems.

It is important to have flexible and powerful tools to simplify design and maintenance of advanced alarm systems. COAST (COmputerized Alarm System Toolbox) was developed to facilitate implementation of diverse methods for alarm generation and structuring in new alarm systems for different industrial processes. The first application using COAST, CASH (Computerized Alarm System for HAMMLAB), is an advanced alarm system utilizing different alarm processing and presentation techniques to reduce the operator's cognitive load. For additional information when he/she is diagnosing disturbances, possibilities for interactive search for relevant information in the alarm system is provided. Thus the alarm system provides the operators with information needed in different phases of a process disturbance.

CASH is used in alarm experiments in Hammlab, and different presentation means and different degree of suppression are tested in this alarm system.

1. INTRODUCTION

One of the main tasks for operators in nuclear power plants is to identify the status of the process when unexpected or unplanned situations occur. The alarm system is the main information source to detect disturbances in the process, and alarm handling has received much attention after the Three Mile Island accident in 1979 [1]. It was realized that conventional alarm systems created cognitive overload for the operators during heavy transients.

In the early eighties, the Halden Project developed an alarm system called HALO (Handling Alarms using LOgic) using logic filtering to reduce the number of active alarms during process transients [2]. HALO has been subject to a number of evaluation experiments with different presentation techniques [3].

Early Fault Detection (EFD) by use of model-based alarms has been a research topic at the Project for several years. The method used is to run small, decoupled models which calculate the state of the process assuming no faults, in parallel with the process. The behaviour of these models is then compared with the behaviour of the real process, and if there is a deviation, an alarm is issued. One will only get one EFD alarm for one fault, and operators thus get better time for recovery actions. Prototypes developed for simulators and installations in real power plants, e.g. the Imatran Voima owned plant in Loviisa, Finland, have demonstrated the feasibility of this methodology, provided that enough measurements are available for the process area considered [4].

In case of major disturbances in a plant with a large number of alarms, a function-oriented approach is often used to monitor plant status. Instead of looking at single systems or variables and alarms within a system, one monitors critical safety functions in terms of whether these functions are challenged. The Halden Reactor Project investigated the Critical Safety Function concept in several studies in the period from 1983 to 1987 in cooperative projects with Combustion Engineering, U.S.A., and the Finnish utility Imatran Voima. Particularly, the human factors experiment with the Success Path Monitoring System (SPMS) did clearly show distinct improvements in operator performance with respect to taking appropriate corrective actions in disturbance situations [5].

Another example is the post trip guidance system SAS-II [6]. It surveys four critical safety functions, which are defined in terms of logic diagrams. These are also a part of the interface to the operator. Colour coded logic diagrams are used to explain why the critical safety function is challenged.

Four years ago the Halden Project took up the thread making new alarm systems. We realized that effective handling and integration of different types of alarms in one system improve the operator's overview and thereby the overall safety of an industrial plant. To enable building of specific alarm systems for different plants with varying demands, we made a generic COmputerized Alarm System Toolbox, COAST [7]. The first application utilizing COAST is the new alarm system in Hammlab, CASH (Computerized Alarm System for Hammlab) [8]. A top down design was utilized, putting the operator in focus, and the requirements for the alarm system were based on his/ her work situation and capabilities.

Our research laboratory HAMMLAB is an experimental control room equipped with the PWR simulator NORS (NOkia Rescarch Simulator) as process. Currently 16 screens are available for

process displays, alarm displays, or displays for other systems. The laboratory is our main facility for carrying out human factors research and operator support system evaluation.

2. OPERATOR TASKS

The operator's work consists partly of routine tasks and handling of known situations and planned changes. However, the real challenge for operators is to handle unexpected and unplanned situations. A model of operator's tasks can be given as: Status Identification, Action Planning and Action Implementation. To be able to handle unknown process situations, the operator should have access to an alarm information system which is adapted to his status identification task. He should be able to shift between different levels of information according to his own problem solving strategy.

2.1 Status Identification

Fig. 1 shows a simplistic model of the process in case of a disturbance situation, and the corresponding operator tasks within status identification: Detect that something is wrong and determine plant status, diagnose initiating event, and predict possible effects. Sometimes there

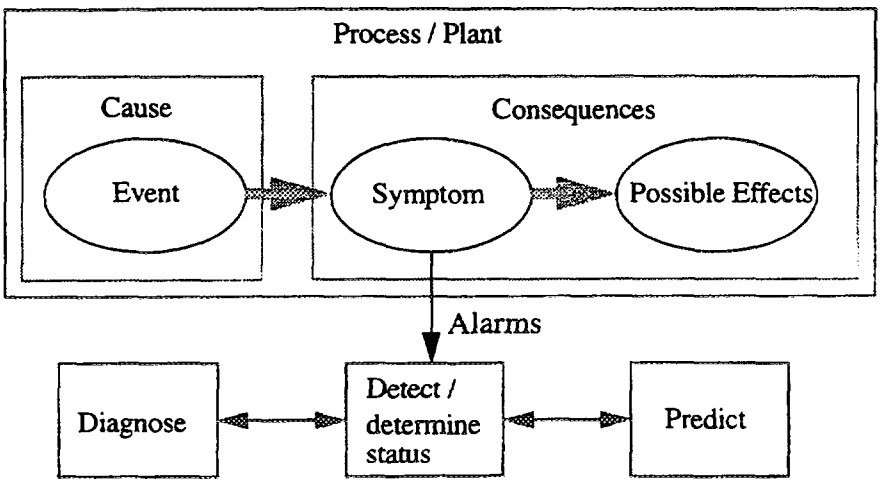


Fig. 1 A simplified model of the plant and corresponding operator tasks.

is not time to find the cause of the disturbance, and the main concern is always to maintain the plant in a safe state. Instead of trying to diagnose the initiating event, the operators then monitors important symptoms and critical safety functions in terms of whether these functions are challenged.

If the operator has the time to investigate further, he/she tries to diagnose the initiating event. He/she may use all kinds of systems for this task, e.g. process formats, trends, alarms and possible diagnosis systems. An alarm system should give the operators a better overview of the situation and a better background for his/her diagnosis.

One example of a system which not diagnoses the fault, but issues a more accurate alarm, is Early Fault Detection [4]. It gives early warnings on failures, and pinpoints the place in the process where something is wrong. The detailed diagnosis is then left to the operator/ plant engineer (or to a detailed diagnosis system).

3. OBJECTIVES OF ALARM SYSTEMS

Our definition of an alarm is:

Alarm: An alarm indicates an abnormal state or combination of states which requires attention from the operator.

The main objective of an alarm system is that it should fulfil the following four basic functional criteria, see Ref. [2].

- It should **alert** the operating staff to the fact that a process or system deviation exists.
- It should **inform** the operating staff about the priority and nature of the deviation.
- It should **guide** the operating staff's initial response to the deviation.
- It should **confirm,** in a timely manner, whether the operating staff's response corrected the deviation.

The alertion of an alarm is typically performed by use of visual and/or audible effects, and these are reset automatically or manually. In the initial phase of a transient the priority and nature (information) of the deviation can also be encapsulated in the alarm. The alarm system should guide the operating staff in the right direction, towards the current abnormalities in the process, by helping them to select the right information and neglect the non-important information. When they do corrective action(s) or monitor the automatic actions performed, the alarm system should contribute to the operator's knowledge: After the action(s) is initiated the alarm system should confirm whether this response affected the process situation.

Even though each individual alarm might fulfil the above requirement, there is no guarantee that the overall alarm system fulfils it. Thus the inform and guide objectives stated above may lead to different conclusions dependent on whether one is working with and designing single alarms in the generation phase (bottom-up), or designing the whole alarm system by applying structuring (to-down). On each alarm the proper alerting, information and guiding only depends on the alarm annunciation. However, for the whole system one has to consider whether the single alarm is relevant within the total situation of the plant.

Increased processing performed by the alarm system will influence the allocation of functions between man and machine. Much emphasis must be put on what kind of alarm information which should be presented, and how the alarm information should be presented. When moving tasks from the operator to the computer there may be a possibility that the operator becomes too confident in the computer, failing to rely on his own process knowledge when computers arrive at conflicting conclusions. The alarm system should be designed to assist the operator, help him to diagnose correctly, and to increase his knowledge, all by presenting only relevant data.

4. DESIGN OF THE NEW ALARM SYSTEM, CASH

The main goals to be achieved by CASH are stated as follows:

- Be a flexible alarm system fittod to experimental purposes in HAMMLAB, reached by
  - highly flexible and maintainable software.

- Exemplify a beyond state-of-the-art alarm system, including
  - a high degree of suppression of non-important alarms, and
  - an efficient Man-Machine Interface.

- Be compatible for new and retrofitted control rooms.

4.1 General Design Principles

An optimal alarm system should be tailor-made to the human's mental limitations and capabilities. The limitations are mainly in areas like memory and work load capacity. On the advantage side, the human brain has strong associative and pattern recognition capabilities, which are very flexible and may be adapted to several working situations. The information presented to the operators should be selected so that both the number of conceptual units to be mentally processed, their associated processing times, and the number of stages in the mental processing are at their minimum.

When the operator has to rely on fewer information units, it is not good enough to only reduce the number of alarms. One should make new information units including more information, which are directly related to the operator's mental model of the plant. By such highlevel conceptual units, e.g. high-level alarms, the operator can fast understand the situation at hand. Thus it is not always so that making new types of alarms will increase the load of the operator. By introducing these high-level conceptual units the load may instead be decreased, concretely by replacing several other alarms.

An overview display should integrate alarm and process information, since the operators in their mental model of the process use as input both process parameters and alarms. To minimize cognitive overload and human-system interactions, alarm and process information should preferably be presented on one overview display, because the operator does not have to extract relevant alarm and process information from different displays and put it together in his mental model of the process. His information gathering and cognitive workload are thereby reduced. Also, the human-computer interaction, i.e., the number of display retrievals, use of keyboard, trackerball, etc., is minimized.

A key factor in the design of an efficient alarm system is the level of alarm discrimination, i.e., the alarm system's ability to suppress all non-important alarms from the overview display. To obtain a high degree of alarm discrimination, it is mandatory to build into the system an extensive amount of detailed process knowledge. To support operator decision-making the system should not remove any information, *only suppress* non-important alarms from the overview display. "Suppress" means that the alarm message is not presented on the overview display, however it is still available on additional displays, like selective displays. When time is available, the operators can get supportive and complementary information from these displays. While efficiency and high relevance are the issues on the overview display, flexibility and details are keywords for selective displays.

This supports the different operator tasks stated in chapter 2: The overview display is the main source for determination of plant status. For more detailed diagnosis of plant anomalies, additional information sources like process displays and selective displays (or also early fault detection systems or diagnosis systems) are used.

Three stages are defined: Alarm generation, alarm structuring and alarm presentation. The alarm generation, including determining which signals to give alarms and what priority to make these alarms, should be done in a bottom-up approach. The engineer has to determine locally that this signal could require operator attention, and how urgent an alarm might be (to determine the priority). The alarm structuring, determining which alarms should be presented on the overview and on the process displays in different process states, should be done globally, in a top-down approach. In this way plant system states (like turbine trip) or plant modes (like shutdown) may be included to determine whether alarms should be shown or not.

4.2 CASH Alarm Presentation

High-level conceptual units are used in the presentation. They are defined according to the operator's mental model of the plant, based on his training and experience. For instance, "turbine trip" means something very specific for an operator. In his mental model of "turbine trip" a lot of information and plant knowledge is embedded. The set of high-level conceptual units includes all well-defined plant modes and plant system states in addition to key alarms.

Being the main alarm system in our man machine laboratory HAMMLAB, one major goal with CASH was to be able to test different ways of presenting alarms. CASH is utilizing the highly flexible Picasso-3 system [9] for presenting alarms, thus the flexibility of the presentation part is very high.

The first prototype of CASH was finished in 1994, and an MMI with two hierarchical levels of information was made [8]. Level 1 is the **overview display** that supplies the operators with plant wide key process information and non-suppressed alarms. Level 2 is composed by alarm **selective displays,** which show more detailed alarm lists, and NORS **process displays,** which include alarms. Two screens are used for the overview, one for the primary and one for the secondary side.

All irrelevant information is removed from the overview level to avoid information overload. The **dark screen concept** is important to obtain optimal working conditions:

- When a plant/process is operating normally without malfunctioning, NO alarm signals should be on.

The dark screen concept is a logical consequence of the alarm definition, that something must be wrong when alarms are issued, or else the situation would not require attention from the operator.

In the overview display, a major characteristic is that the spatial allocation of conventional alarm systems is partly kept and combined with chronological alarm lists. Except for key process parameters, the overview is based on the dark panel concept. The overall process is represented, but divided into 10 main system/function groups. Each group has an allocated window for presentation of all the related alarms. In addition, area is allocated for presentation of a selected set of key process parameters, active plant mode and plant system states, and alarm statistics, refer Fig. 2. The alarm groups help the operators to immediately locate the disturbance. This solution allows to some extent spatial recognition to identify alarms. Each group contains a finite number of messages in chronological order to facilitate scanning and assimilation.

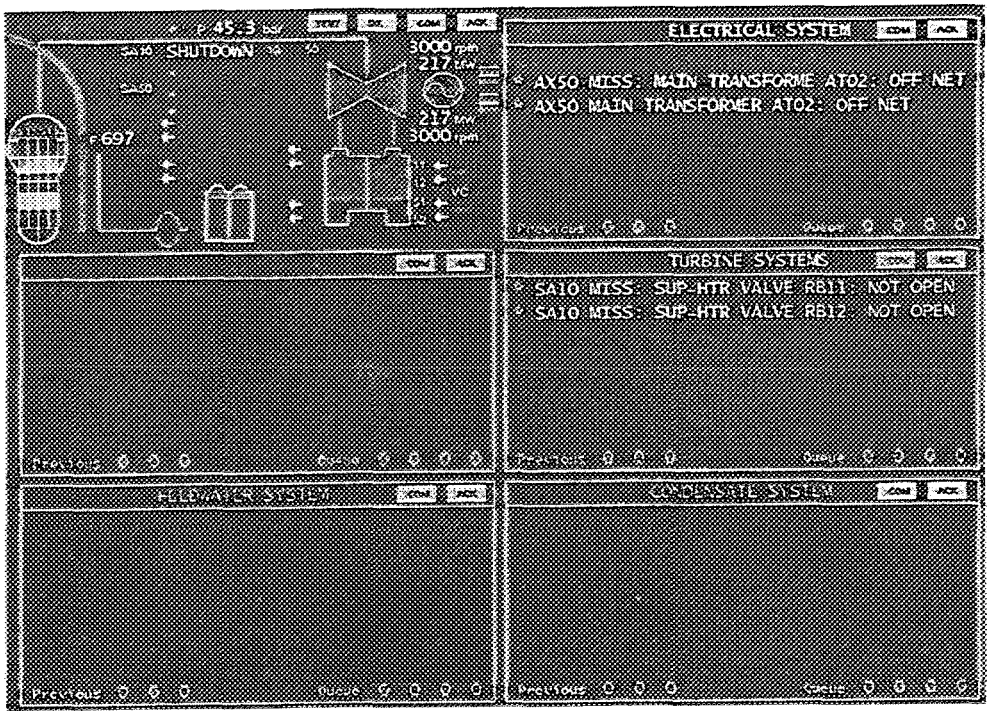


Fig. 2 Layout of the Secondary Side CASH Overview Screen

The selective displays in the first prototype provide the operators with additional information about abnormalities in the plant. They have the flexibility of choosing different alarm lists according to their needs and preferences. These displays represent a major improvement to the existing alarm systems, because they will help operators understand what is happening, assisting them in their diagnosis tasks, and confirming or disconfirming their hypothesis. Trend displays will also be available from CASH as well as the other process related displays. In the future also events should be included in the selective displays. Fig. 3 shows the selection part of the selective displays, where the operators may select from which systems and what kind of alarms to be displayed.

The dark screen concept and the definition of an alarm applies to the overview display snrl the initial slertion of the r)nerntorc. However this consent is not valid for the selective and process displays: Alarms are not removed from the system, but are presented on these other displays with static alarm priorities as status information, which is normal today in many control rooms. The advantage is that the operator knows by a glance that there is for example a high level in a tank if there is a red spot in the process picture. However, suppressed alarms are not alerted with sound to the operator, even if they're still present in these displays. Thus this way of designing the alarm system concedes both to the ideal definition of an alarm, and to the use of an alarm system as a tool to investigate the process.

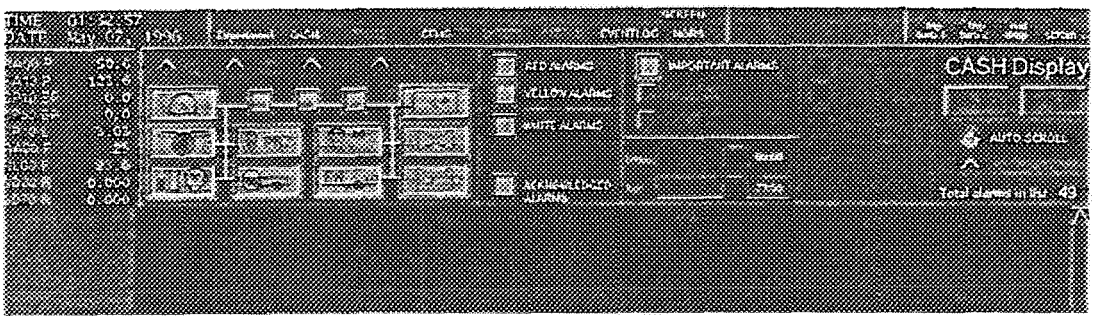


Fig. 3 Upper Part of the Selective Display

The COAST feature of generating new alarm lists on-line is fully utilized in the selective displays. Actually, when different buttons are pushed in the display in Fig. 3, the condition for selecting alarms into a new alarm list is generated and sent on-line to COAST which makes a new alarm list.

The prototype of CASH was used in staffing and human error experiments in HAMMLAB the autumn 1995. The alarm system was not the main issue, so we do not yet have an evaluation of this presentation.

However, we are now conducting major alarm system experiments in cooperation with the US NRC. Three different types of alarm presentation are tested: Tiles (simulated on eight screens), alarm lists on two screens, and a mixed approach with lists on two screens and key alarms on two tile screens. All three approaches utilizes process overview on two screens in addition to detailed process formats. In the pure list based approach alarms are integrated in the process displays, in the other two not. Fig. 4 shows the secondary part of the mixed approach, with key alarms in tiles and alarm lists on the upper screens, and process overview below:

In addition the testing is handling different levels of alarm suppression. No results are available from these experiments yet, but the process of making both different structuring and several different displays has gone very smooth.

4.3 Alarm Generation in CASH

The alarm generation module generates different types of alarms which we classify as **Basic alarms or High-level alarms.** Basic alarms are generated either directly from binary signals or when analog signals violate their respective alarm limits. Examples are conventional alarms, rate of change alarms and automatics/process deviation alarms.

High-level alarms are generated by means of any logical or arithmetic calculation using several alarms and/or process measurements. These high-level alarms are intended to inform the operator about unexpected changes in the availability of major plant systems. They may also inform about challenged plant functions. Examples are group alarms, plant system state alarms, and missing alarms. Missing alarms are generated when expected alarms do not occur.

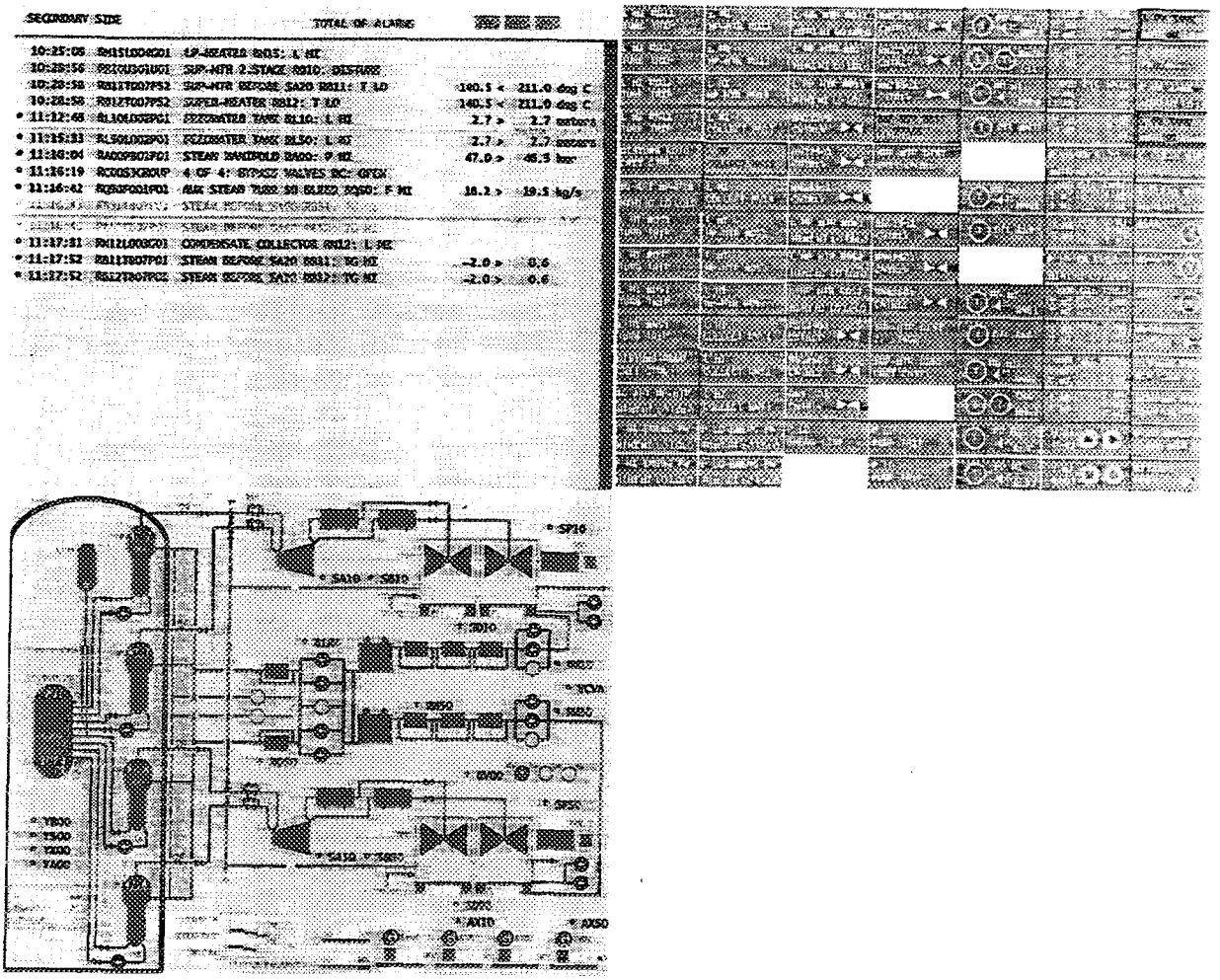


Fig. 4 Secondary Side of One Alarm Experiment Set-up with Mixed Lists and Titles in Addition to Process Overview

Two static priorities are defined in CASH: First priority (red), requires immediate operator response, while second priority (yellow), requires operator response within limited time.

4.4 Alarm Structuring in CASH

In the HALO work, it was shown that a significant amount of alarms may be filtered. However, they were removed from any presentation, and one should be very certain that the operators do not need an alarm before it is filtered in this way. An important requirement in CASH was not to remove any alarms completely from the reach of the operator. There was given a set of predefined alarms in the simulator (like on most plants). The goal of CASH with respect to alarm reduction, was therefore to devise methods, so that the set of defined alarms are only presented when they really are alarms according to the alarm definition. Another goal was to be

able to test varying suppression levels, thus putting high demands on flexibility. This is reached through utilizing the alarm system toolbox COAST [7].

The most important objective of alarm structuring is to reduce the avalanche of alarms during a major plant disturbance. An important objective is also to group and sort alarms in such a way that the presentation is optimized with respect to the operators' information needs. Structuring is here being considered as a method to reduce the information load on the operators without removing any significant alarm information from the alarm system itself.

Several alarm reduction techniques are provided that actually do not constitute well-separated suppression methods with sharp boundaries. The operators do not need to discriminate the different techniques, but will use the results from the different grouping and sorting criteria. The high level conceptual units work as the main suppression conditions at the top level.

- *Plant Mode Suppression:* At any time, CASH defines a unique plant operative mode which is used for alarm suppression, e.g. Power Operation and Start-up.

- *Plant System State Suppression:* Status of major plant components and plant subsystems are defined and used for alarm suppression as well as for alarm grouping. For example, if a process part is by-passed, all alarms within the area will be suppressed. Other examples of defined plant system states are: Turbine trip, trip of main circulation pump, repot, scram.

In the current implementation of CASH, plant mode suppression is not used as extensively as plant system state suppression. Similar degree of suppression as when using plant modes may be reached by utilizing a combination of plant system states. The plant system state suppression is simpler to implement and easier to maintain, because it is more distributed, so one plant system state suppresses fewer alarms. Thus the physical relationships are easier to find and verify.

- *Dynamic Suppression Limits* are a new feature introduced in CASH to handle consequence alarms. After a well known disturbance, such as a turbine trip, related process parameters fluctuate and violate their alarm limit. To some degree, this behaviour is however "normal" for the given process situation, and the alarm can be suppressed. By using simple techniques, bounding curves are defined and will suppress the alarms as long as the measurements do not violate the expected domains. This method maintains the possibility of annunciating an alarm if the value of the measurement fluctuates more than normal in a given transient.

Logic is used extensively to fulfil many types of structuring. Boolean algebra and the logic operations are well defined and extensively used throughout the world. Logic operators are used in all sciences and are also suitable for alarm filtering and suppression.

One important feature of CASH is the possibility to organize all the alarm information on the operator's demand, and requirements put up by the design of the overview. Several different grouping and sorting criteria are required for the overview display, but also for the selective displays. Some examples of grouping criteria that support operator pattern recognition are: Plant system, alarms specified by filtering condition, alarm priority, alarms suppressed by Plant mode or Plant system state, and alarms specified by time criteria.

A CASH alarm object sheet is used to define an alarm and its suppression conditions. It was found to be a good feature to implement structuring conditions and methods, and it provides a systematic overview of the implementation.

5. COAST

COAST is a generic tool for building and executing alarm systems for complex industrial processes, like oil production platforms or nuclear power plants. The emphasis is on alarm generation by means of diverse methods and alarm structuring by means of several and flexible techniques.

To enable building of specific alarm systems for different plants with varying demands, COAST is made generic and object-oriented. For the validity and the correctness of the alarm system, it is important that the alarm system designer is given the opportunity to construct the alarm system in a clear and straight-forward way, with a good overview of the system at hand.

In COAST, features such as declaring generic descriptions of system components in alarm classes and then specifying many objects from one class, simplifies the construction of an alarm system. Coupling to different processes is easily made through an application programmer's interface.

COAST contains basic functionality for generating alarms by several different methods, e.g. model-based and function-oriented alarms, inside the same framework. COAST also contains strong functionality to filter and suppress conventional alarms, as well as good possibilities for other types of structuring of alarms through user specified relations. This feature may be used to define cause consequence relations between alarms.

COAST has no graphic capabilities, but will feed any graphical system with the required alarm information and alarm lists. However, COAST provides powerful on-line selective capabilities through which users may interact with the alarm system in very flexible ways. Thus, COAST opens for construction of advanced alarm systems which not only will be the alarm annunciation system, but also a major information source for operators when diagnosing the cause of the plant anomaly.

The experience gained from the work with various alarm systems was utilized when designing the basic functionality of COAST. The goal was to be able to easily apply advanced alarm handling methods to several different processes, e.g. nuclear power plants or oil production platforms, and to be flexible regarding which methods to use in different applications. It should thus be possible to utilize COAST to make most kinds of alarm systems.

COAST is meant to be an add-on possibility to conventional process control systems. It is also easy to couple COAST to an existing alarm system. Existing alarms will then be structured or filtered by COAST before presentation. Fig. 5 shows how COAST may be coupled to existing systems.

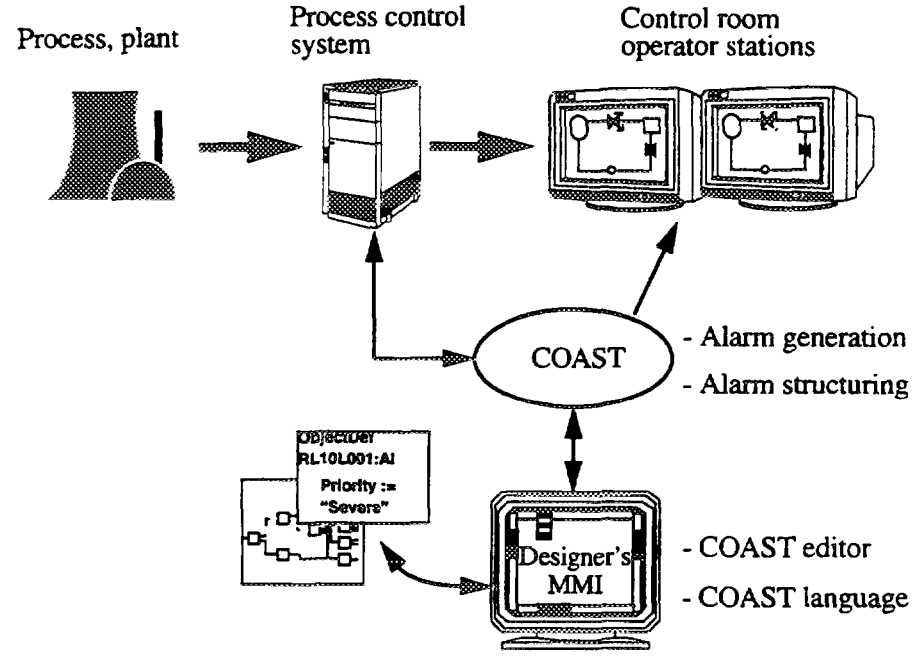


Fig. 5 COAST as an add-on module to a process control system

Main features of COAST:

Alarm System Definition: A COast LAnguage, COLA, is available to build alarm systems. It is a high level language influenced by natural language, it supports object-orientation and has strong expressive power for arithmetic and logic expressions. COLA's high abstraction level saves the users of COAST from low level programming. A beta version of an editor is also made. It emphasizes reuse of alarm classes through class libraries and structuring of the alarm system through alarm object hierarchies.

COLA is a declarative language, where one may write down the definitions and couplings between alarms without thinking of the sequence in which they have to be updated and so on. Therefore it is easy to make definitions which correspond directly to the structure in the CASH alarm object sheet; i.e. the mapping between the conceptual alarm system and the implementation is very easy, making the code itself very simple. This also simplifies verification of the alarm system implementation versus the design.

On-line Alarm Processing: The COAST kernel is running on-line, utilizing the definitions made in COLA. The kernel is event driven and takes care of all processing of alarms when process data are entered to the system by external applications through the Application Programmer's Interface, API. The API is a function library which is included in external application programs, and process data may be either measurements or (pre)generated alarms. The results from the processing in the kernel are fed to a graphical system. Note that COAST does not present anything itself, but the coupling to external systems is easy, so COAST may feed any graphical system with the resulting alarm lists.

Alarm List Extraction: In order to get access to the alarms generated by the COAST kernel, the external application asks the kernel for a selection of alarms. These selections are written using COLA-light, a subset of COLA containing the selection facilities of COLA, offering the

possibility to search among existing alarm objects. It does not define new objects in the kernel. An example of such a selection could be all alarms that have status on, and belongs to a certain subsystem of the plant. These selections can be predefined, or new selections can be specified on-line by application programs in order to obtain new lists of alarms, as done in the CASH selective displays. This provides a very powerful and flexible possibility to create selective displays which the operator may use in his investigation. Whenever new alarms occur which fit a selection criterion, they are automatically sent to the application.

COAST facilitates easy modification of alarm generation and structuring. As an example, when designing a new overview display in CASH we wanted to know how many active non-suppressed alarms of first and second priority we had on each process format. This was easily solved by adding one attribute and two methods to our main alarm class.

6. CONCLUSIONS

Proper design of alarm systems should take into account the role of the alarm system within the total I&C system at the plant, and especially the role of the alarm system versus the operators' tasks in the control room.

The staffing and human error experiments in HAMMLAB the autumn 1995 proved that the first version of CASH was reliable and had a satisfying performance to act as the main alarm system in all scenarios tested in the experiments, which included accident transients.

Different alarm presentation and structuring are now tested in HAMMLAB. The flexibility of CASH, both with respect to alarm processing and alarm presentation, is crucial to be able to set up different systems for experiments. By using COAST we can easily modify alarm generation and structuring, while Picasso-3 ensures flexible presentation solutions.

The main goals of CASH: A high degree of alarm suppression, efficient MMI, flexible software fitted for experimental purposes and compatibility for other control rooms, are reached through:

- Presenting key alarms and process information in one overview display supporting detection of disturbances and determination of plant status.
- Presenting suppressed alarms in process displays and in selective displays, supporting diagnosis of the initiating event of the disturbance.
- Utilizing high-level units which are compatible with the operator' s mental model of the plant in the presentation and as suppression criteria.
- Use of COAST and Picasso-3, which has made CASH a flexible alarm system fitted to experimental purposes.

COAST provides the flexibility needed to implement advanced alarm systems for research. It also enables building of specific systems for different plants, as "add-on" to the existing process control systems.

7. REFERENCES

[1] J.G. Kemeny, *Final Report of the President's Commission on the Accident at Three Mile Island,* Washington D.C. (1979).

[2] F. 0wre and E. Marshall, "HALO - Handling of Alarms using LOgic: Background, Status and Future Plans," *Proceedings of the International ANS/ENS Topical Meeting on Advances in Human Factors in Nuclear Power Systems,* Knoxville, Tennessce, USA (1986).

[3] E. Marshall, C. Reiersen and F. 0wre, "Operator Performance with the HALO II Advanced Alarm System for Nuclear Power Plants- A Comparative Study," *Proceedings of the ANS Topical Meeting on Artificial Intelligence and Other Innovative ComputerApplications in the NuclearIndustry,* Snowbird, Utah, USA (1987).

[4] A. S0renssen, "Early Fault Detection at the Loviisa Nuclear Power Plant by Simulation methods",*Modelling & Simulation, Proceedings of the 1990 European Simulation Multiconference,* Nuremberg, Germany (199O).

[5] E. Marshall, S. Baker, C. Reiersen, F. 0wre and P. Gaudio Jr., "The Experimental Evaluation of the Success Path Monitoring System", *IEEE Fourth Conference on Human Factors and PowerPlants,* Monterey, California, USA (1988).

[6] F. 0wre, S. Nilsen, T. Forsman and J.E. Stenmark, "An Operator Support System for a Swedish Nuclear Power Plant Control Room", *Proceedings, EPRI conference on Expert System Applications for the Electric Power Industry,* Boston, Massachusetts, USA (1991).

[7] A.Bye, T.W.Storberget, F.Handelsby and S.Nilsen: "COAST, a System for Advanced Alarm Handling and Interactive Alarm Analysis", *ANS Topical Meeting on Computer Based Human Support Systems: Technology, Methods and Future,* Philadelphia, Pennsylvania, USA (1995).

[8] B. Moum, N. F0rdestr0mmen, C. Decurnex, B. Torralba, "CASH: An Advanced Computerized Alarm System", *ANS Topical Meeting on Computer Based Human Support Systems: Technology, Methods and Future,* Philadelphia, Pennsylvania, USA (1995).

[9] K.A. Barmsnes, 0. Jakobsen, T. Johnsen and H.O. Randem, "Developing Graphics Applications in an Interactive Environment," *Proceedings, 1994 SCS Simulation Multiconference,* San Diego, California, USA (1994).

THE CANDU ALARM ANALYSIS TOOL (CAAT)

E.C. Davey, M.P. Feher and L.R. Lupton
Control Centre Technology Branch
Ontario, Canada

ABSTRACT

AECL undertook the development of a software tool to assist alarm system designers and maintainers based on feedback from several utilities and design groups. The software application is called the CANDU Alarm Analysis Tool (CAAT) and is being developed to:

- *reduce by one half the effort required to initially implement and commission alarm system improvements,*
- *improve the operational relevance, consistency and accuracy of station alarm information,*
- *record the basis for alarm-related decisions,*
- *provide printed reports of the current alarm configuration, and*
- *make day-to-day maintenance of the alarm database less tedious and more cost-effective.*

The CAAT assists users in accessing, sorting and recording relevant information, design rules, decisions, and provides reports in support of alarm system maintenance, analysis of design changes, or regulatory inquiry.

The paper discusses the need for such a tool, outlines the application objectives and principles used to guide tool development, describes the how specific tool features support user design and maintenance tasks, and relates the lessons learned from early application experience.

1. INTRODUCTION

This paper describes a software application tool for the initial specification and maintenance of the thousands of alarms in nuclear and other process control plants. The software program is used by system designers and maintainers to characterize, record and maintain the alarm information and configuration decisions for an alarm system. The tool provides a comprehensive design and information handling environment for:

- the existing alarm functions in current CANDU and other process plants,
- the new alarm processing and presentation concepts developed under CANDU Owners Group (COG) sponsorship that are available to be applied to existing CANDU plants on a retrofit basis, and
- the alarm functions to be implemented in new CANDU and other process plants.

The balance of this paper:

- reviews the need for improved support for the initial specification and on-going maintenance of annunciation system information,
- outlines the objectives and principles used to guide tool development,
- describes how specific tool features support user tasks, and
- discusses the lessons learned in applying the tool in support of the implementation of specific alarm system improvements.

2. THE NEED FOR AN ALARM ANALYSIS TOOL

2.1 Cost-Effective Support for Initial Design and Ongoing Maintenance

CANDU plants employ a computer-based alarm system to alert operating staff to abnormal conditions and changes in state as a result of the automatic responses of the control system. In current plants, the main alarm system is implemented as part of the digital control computer software. Each of these alarm systems contain a database of several thousand alarms that provide coverage for all plant safety and power production functions.

The initial specification of alarms for a new plant requires the application of project specific rules, strategies and guidelines for classifying, prioritizing and conditioning alarms to create the alarm database. Past experience has shown this task to be very labour intensive, susceptible to error, and thus costly.

Over a station's life, there is a continual need to make changes to the alarm system to improve on the existing design or add new alarm functionality to better meet production and safety needs. The impetus for change can be as a result of several factors, for example:

- increased production targets (e.g., tightening of operating margins),
- improvements to station operational practices (e.g., addition of new alarms to provide operators with better support for procedures), and
- compliance with evolving regulatory requirements.

2.2 The Alarm System Design Task

The implementation of alarm system changes and improvements requires the incorporation of station specific rules, strategies, and guidelines for classifying, prioritizing, and conditioning alarms to be entered into the alarm system database and/or alarm processing program. This information is collected from the station's operating policies and principles, design documentation, emergency operating philosophy and procedures, operating manuals, and from station staff experienced in both safety and production activities. This is a design task and the effort to analyze and record the alarm design decisions for all plant alarms must be practical, manageable, and not too costly relative to the potential operational benefits.

While it may be possible to manage this design task manually, the large amount of information that needs to be consulted, recorded, checked for consistency, and reviewed for consensus

between several experts makes conventional manual and paper-based management of the information labour intensive, time consuming, and prone to error. Time and time again, utility staff have stated that they have been reluctant to pursue alarm system improvements due the perceived large effort to analyze and record the information for the several thousand alarms in the plant. For example, the annunciation systems in several plants contain a conditioning capability that is largely unused due to the perceived cost and difficulty to analyze plant alarm conditioning relationships.

2.3 Recent Development of Alarm System Improvements

AECL in partnership with CANDU utility staff, have developed several improvements for CANDU alarm systems under COG sponsorship [1,2]. A prototype system, called the CANDU Annunciation Message List System (CAMLS), has been developed to demonstrate and evaluate the proposed improvements. CAMLS introduces several new alarm system functions, namely:

- dynamic reprioritization of alarms based on plant operating conditions,
- cause-consequence conditioning of alarms to improve relevance,
- combination of similar or channelized alarms into a single summary alarm,
- generation of alarms identifying the failure of expected automatic actions,
- separate presentation of alarms identifying problems in the plant from those identifying only non-problematic changes in state, and
- organization of the presentation of fault alarms by order of importance.

The operational benefits of the CAMLS annunciation concepts have been proven in simulator based evaluations at the Point Lepreau and Darlington generating stations [3,4].

In comparison to the current plant annunciation, CAMLS significantly improves operators':

To support the implementation of the CAMLS improvements, several changes and additions must be made to alarm information contained in the alarm system database. During the course of the CAMLS development program, it became apparent that a key to realizing the benefits of any improvements in existing plants or in a new plant design would be the availability of an effective tool to support the analysis and categorization of alarm and related information.

3. OBJECTIVES AND PRINCIPLES

3.1 Tool Objectives

To better support designer and maintainer needs, AECL undertook to develop CAAT to improve the tasks associated with the initial specification and maintenance of the thousands of alarms in CANDU plants. At the beginning of the development program, objectives were established in five areas:

- Application Scope

Support alarm definition and maintenance for the existing alarm functions in current CANDU plants, and the CAMLS alarm processing and presentation concepts for application to existing CANDU plants on a retrofit basis and to new CANDU plant and other process plant designs.

- Capital Cost and Schedule Reduction

  Reduce the initial design effort by half for alarm database creation.

- Operation, Maintenance and Administration Cost Reduction

  Reduce the station costs for ongoing alarm system changes so that incremental alarm system improvements will be more affordable.

- Station Production

  Enhance station production and operations by assisting with improvements to alarm information relevance, understanding and consistency.

- Maintainability and Licensibility

  Provide better documentation of the basis for alarm-related decisions to better assist with future alarm system maintenance and regulatory review.

3.2 User Support Principles

The following user support principles were established to guide application development:

- Provide features to support specific designer/maintainer tasks,
- Record and make accessible design rules and design decisions so that they can be readily reviewed and used to guide design decisions,
- Automate labour-intensive designer/maintainer tasks to simplify alarm database creation and maintenance,
- Provide communication and interfaces to station/design organization information sources to eliminate the need for transcription of information between systems,
- Support station customization of the alarm maintenance environment, and
- Reduce the potential for and consequences of human error by designing to prevent and mitigate human error in alarm information entry.

4. FUNCTIONALITY

4.1 CAAT Functions

CAAT provides a computer-based design environment for performing analysis, design and review tasks associated with a plant alarm database. It assists users in accessing, sorting and recording relevant information, design rules, decisions, and provides reports in support of system

maintenance, analysis of design changes, or regulatory inquiry.

CAAT supports the recording, tracking and review of design decisions concerning the specification of:

- plant modes (i.e., plant operating regions) and supporting parameters within which to define alarm relevance and priorities,
- plant alarms including the:
  - condition and threshold(s) that define when the alarm should be generated,
  - type of alarm (i.e., fault or status),
  - format and contents of alarm message text, and
  - relevance of the alarm for each operating mode (i.e., plant operating state),
- appropriate priorities for each alarm in each relevant operating mode (i.e., dynamic prioritization),
- situations under which individual or groups of alarms are suppressed (i.e., conditioning),
- situations where several similar alarms can be combined into a single message for presentation (i.e., coalescing and function-based alarms),
- alarms that alert operators to expected conditions that fail to occur (i.e., expected-but-not-occurred alarms), and
- supporting alarm details, including:
  - source instrumentation references,
  - flowsheet references,
  - group affiliations (i.e., system, parameter group, function), and
  - response procedures.

CAAT provides features to assist with specific designer and maintainer tasks, for example:

- enabling utility users to customize the tool via configuration menus and design rule entry to specify the station rules to be followed for alarm database definition (e.g., priority assignment rules),
- presenting a framework for making alarm design decisions that promotes an operations perspective, as well as consistency and completeness of alarm database entries (e.g., each alarm should be examined for operational relevance in each plant operating region),
- storing both the design rules and the results of their application within a common database so that the effects of changes to design rules on the alarm database can be consistently applied and immediately observable,
- substantially simplifying information recording and searching tasks by automating the repetitive and labour-intensive task aspects in comparison to conventional paper-based methods,
- providing electronic access via plant information system servers to the supporting information to assist with making specific design decisions (e.g., alarm response procedures, historical plant parameter and annunciation logs), and
- enabling the comparison of design decisions among multiple station analysts to determine overall alarm database consistency and identify outstanding discrepancies.

4.2 Operations Environment

CAAT is intended for office use at power/process plants or in design organizations. For alarm information definition and maintenance, the tool can be used in a standalone configuration or connected via a network LAN to plant or design databases to access supporting sources of information or print reports. When information from CAAT is required by an annunciation system (e.g., CAMLS), it can be transferred by authorized personnel to the specific system via a LAN or dedicated connection.

4.3 Implementation Architecture

CAAT is a software application that operates from any Microsoft Windows 3.1 compatible computing platform. The CAAT application encompasses two software modules:

- a user interface module, created using PowerBuilder, that manages a user's requests to create, modify or view database information and organizes the presentation of database information,
- a relational database module, created using Watcom, that stores the entered alarm database. Other relational databases are also supported.

5. TASKS SUPPORTED

5.1 Alarm Database Specification

Development of an alarm database involves two types of tasks. The first task (i.e., criteria definition) defines the basic database structure (e.g., names and number of plant modes). This activity establishes the database architecture and selection options for specific information categories that will be used in the second phase of the design process. The second task involves entering information into the database for individual and groups of alarms or related supporting information. Two examples of data entry screens are shown in Figures 1 and 2. The alarm specification screen for a steam generator level high alarm is shown in Figure 1. The prioritization specification screen for the same alarm is shown in Figure 2.

CAAT enables a developer to look at alarm information in several ways to support the work approach chosen, for example information can be grouped to view:

- all information with respect to an individual alarm,
- all alarms with respect to a specific alarm category,
- the priorities for each relevant mode for an alarm,
- all alarms with respect to a specific conditioning or expected-but-not-occurred initiating trigger,
- all groups of alarms that are replaced by a single coalesced alarm,
- alarms judged not be relevant for a specific plant mode, and
- all alarms with respect to an operating manual or procedure.

In addition, the following facilities are provided to support developers in establishing operational

relevance, completeness and accuracy of alarm entries:

- selection of alarm entries from predefined lists of possible values to simplify the manual task of database entry and promote database integrity,
- the use of text fields to record the rationale for specific alarm information choices,
- search of the alarm database to identify alarms with similar specified properties,
- copying of database information for one alarm to new entries for similar alarms to facilitate working on multiple related alarms simultaneously,
- comparison of database entries for specified alarms, and
- indication of database completion for each type of information stored.

5.2 Alarm Database Use and Review

The CAAT database contains information to support existing CANDU annunciation systems as well as the CAMLS annunciation improvements developed under COG sponsorship. Support for other annunciation concepts is possible through application customization. Once the information for an alarm system is created, it can be downloaded directly to a specific annunciation system for use. The capability to transfer alarm database information into existing CANDU Digital Control Computer (DCC) annunciation software modules has not been implemented. The need for such a capability will be established as part of annunciation retrofit discussions with specific stations.

Once an alarm database is created and used to support a fielded annunciation system, periodic changes to the database will likely be required to accommodate changes in plant configuration, reference material, operational practices or procedures. The same properties of the tool that assist with initial alarm specification should support annunciation system engineers, safety analysts, and operations staff in reviewing database entries and defining new database entries as required.

6. APPLICATION FINDINGS

6.1 Applications

The core functionality of CAAT was developed and demonstrated during 1994. During this development period, key functions of the tool were proven and the effectiveness of CAAT in supporting alarm system designers was assessed through the analysis of alarms to demonstrate CAMLS annunciation concepts. Since then, CAAT has been used to analyze alarms and build alarm databases for:

- CAMLS simulator-based validation trials at the Point Lepreau and Darlington, stations,
- a CAMLS annunciation retrofit feasibility study undertaken for the Darlington station,
- the CANDU 9 CAMLS implementation in a control room mock-up, and
- a demonstration of an improved Emergency Core Cooling system interface.

6.2 Alarm Database Creation Effectiveness

Through the several application examples undertaken to date, we believe that the development objective of reducing the initial alarm database design effort by 1/2 can be exceeded. For example, a controlled study of the time required to build an alarm database was conducted as part of the CAMLS annunciation retrofit feasibility study undertaken for the Darlington station. In this study, a single analyst developed an alarm database for 130 representative plant alarms in 15 days. The scope of tasks included:

- entry of alarms and message text into the alarm database,
- prioritization of each alarm across 29 plant modes,
- definition and entry of 18 conditioning and coalescing relationships,
- definition and entry of supporting rationale for prioritization and conditioning decisions, and
- review and revision of the initial alarm database with a senior analyst.

In comparison, previous analysis experience before CAAT was available indicates that performing the same tasks for 130 alarms using a paper-based form-filling approach would require 32 to 38 days.

Based on this and other project experience and allowing for an effort reduction of 3 to 1 as a result of the typical distribution of similar alarms in a plant database, we estimate that a complete plant alarm database of 6000 alarms could be analyzed by two analysts within six to eight months.

6.3 Future Directions

AECL is continuing to work with utility and design staff to refine CAAT functionality to better meet designer and maintainer needs. Areas of future improvement include:

- the use of pre-defined formats for organizing alarm text elements and selection of message component terms from predefined lists of acceptable entries to simplify and standardize alarm text definition,
- hierarchical definition of parent alarms from which the alarm attributes for a group of similar alarms can be automatically derived to reduce the need to repetitively enter or copy alarm attributes to each group member, and
- incorporation of alarm definition design guide forms as application screens within CAAT to simplify the tasks of initially defining alarms for an annunciation database.

7. CONCLUSIONS

AECL has developed an alarm system design tool (i.e., CAAT) that provides a computer-based design environment for performing analysis, design and review tasks associated with the alarm database for nuclear and other process control plants. Use of CAAT in place of conventional

approaches is expected to substantially reduce the time spent by:

- alarm system developers or maintainers in defining the information elements for a new alarm entry by 1/2, and
- alarm system reviewers by 1/3.

In addition, use of the tool is expected to result in a more consistent, better documented and more easily licensable alarm systems. Such savings and benefits will make future alarm system improvements more affordable and reduce station operations and maintenance costs associated with on-going alarm system maintenance.

The user-support concepts implemented within CAAT are expected to be essential to the cost-effective implementation and maintenance of future CANDU annunciation improvements. For example, several CANDU stations are considering annunciation system upgrades based on the CAMLS concepts. In addition, AECL has adopted the CAMLS annunciation concepts for use in future CANDU stations. It is expected that CAAT will play a key role in the implementation of CAMLS improvements to current station alarm systems and future designs.

8. ACKNOWLEDGMENT

Several people have been influential in the development of CAAT. The authors would like to acknowledge the key roles played by Rick Basso and Ken Guo in CAAT concept development and refinement. We also would like to acknowledge the helpful comments and suggestions of AECL alarm analysts and CANDU station staff:

- Davelyn Hickey and Dave Elder of AECL,
- Debbie Scott-Gillard, Gary Cleghorn and Glen Smith of Darlington,
- Bryan Patterson, Harry Storey and Herb Thompson of Point Lepreau,
- Terry Karaim of Pickering, and
- Jorgen Hertzum-Larsen and Angie Kozak of Bruce A/B.

9. REFERENCES

[1] GUO, K.Q., BHUIYAN, S.H., FEHER, M.P. and DAVEY, E.C., "Developments in Improved Alarm Annunciation". Proceedings of the 1994 Canadian Nuclear Society Conference, Montreal, Quebec, (1994).

[2] DAVEY, E.C., FEHER, M.P. and GUO, K.Q., "An Improved Annunciation Strategy for CANDU Plants". Proceedings of the American Nuclear Society Conference on Computer-based Human Support Systems: Technology, Methods and Future, Philadelphia, Pennsylvania (1995).

[3] DAVEY, E.C., FEHER, M.P., MCCALLUM, J.F. and LONG, T., "CANDU Annunciation Messages List System (CAMLS): Operational Benefits and Validation Results", Proceedings of the Second CANDU Owners Group Computer Conference,

Markham, Ontario (1995).

[4] FEHER, M.P., DAVEY, E.C. and LUPTON, L.R., "Validation of the Computerized Annunciation Message List System", Proceedings of the IAEA Specialist Meeting on Experience and Improvements in Advanced Alarm Annunciation Systems in Nuclear Power Plants, Chalk River, Ontario (1996).

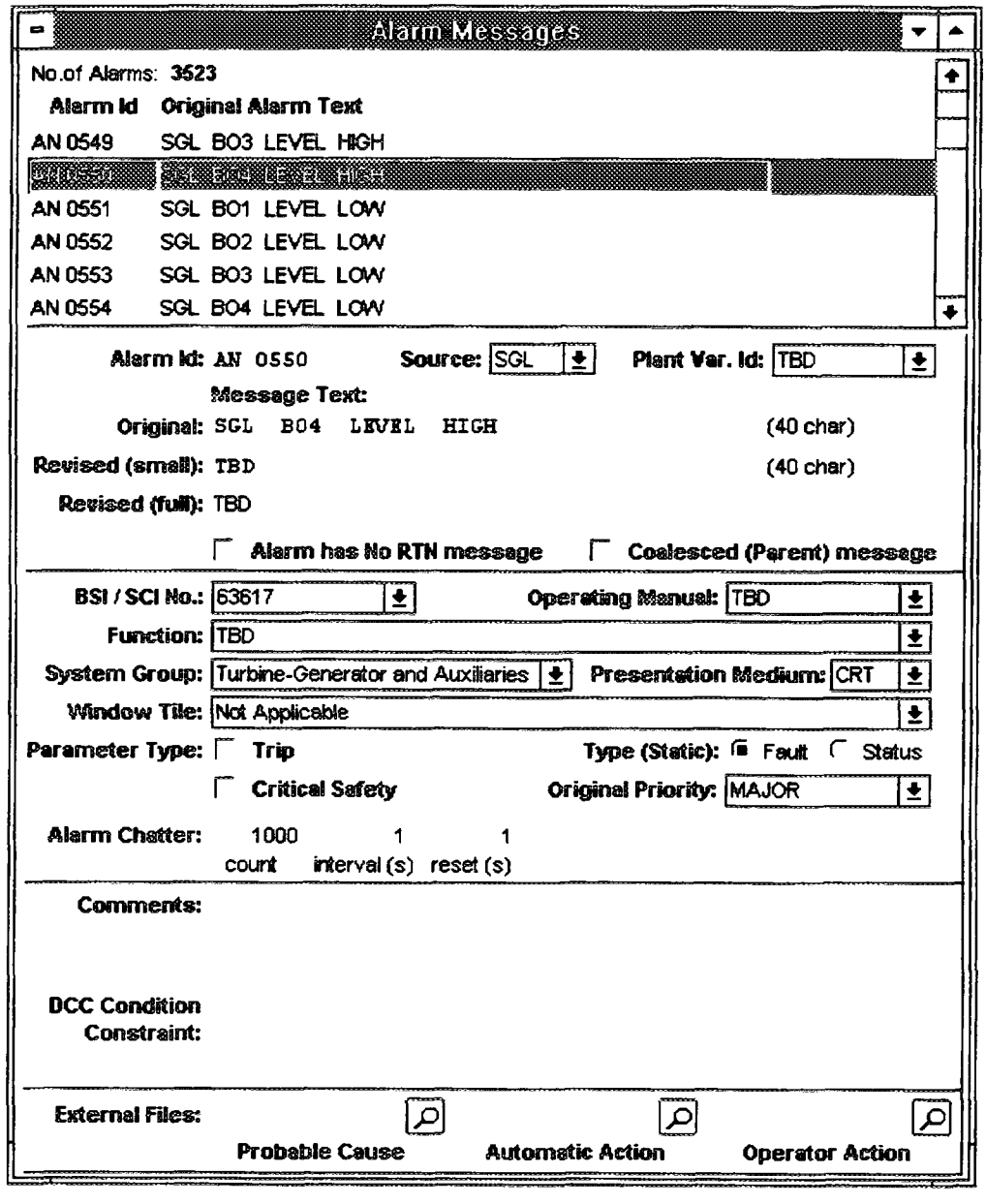


Figure 1: Example of an Alarm Specification Screen.

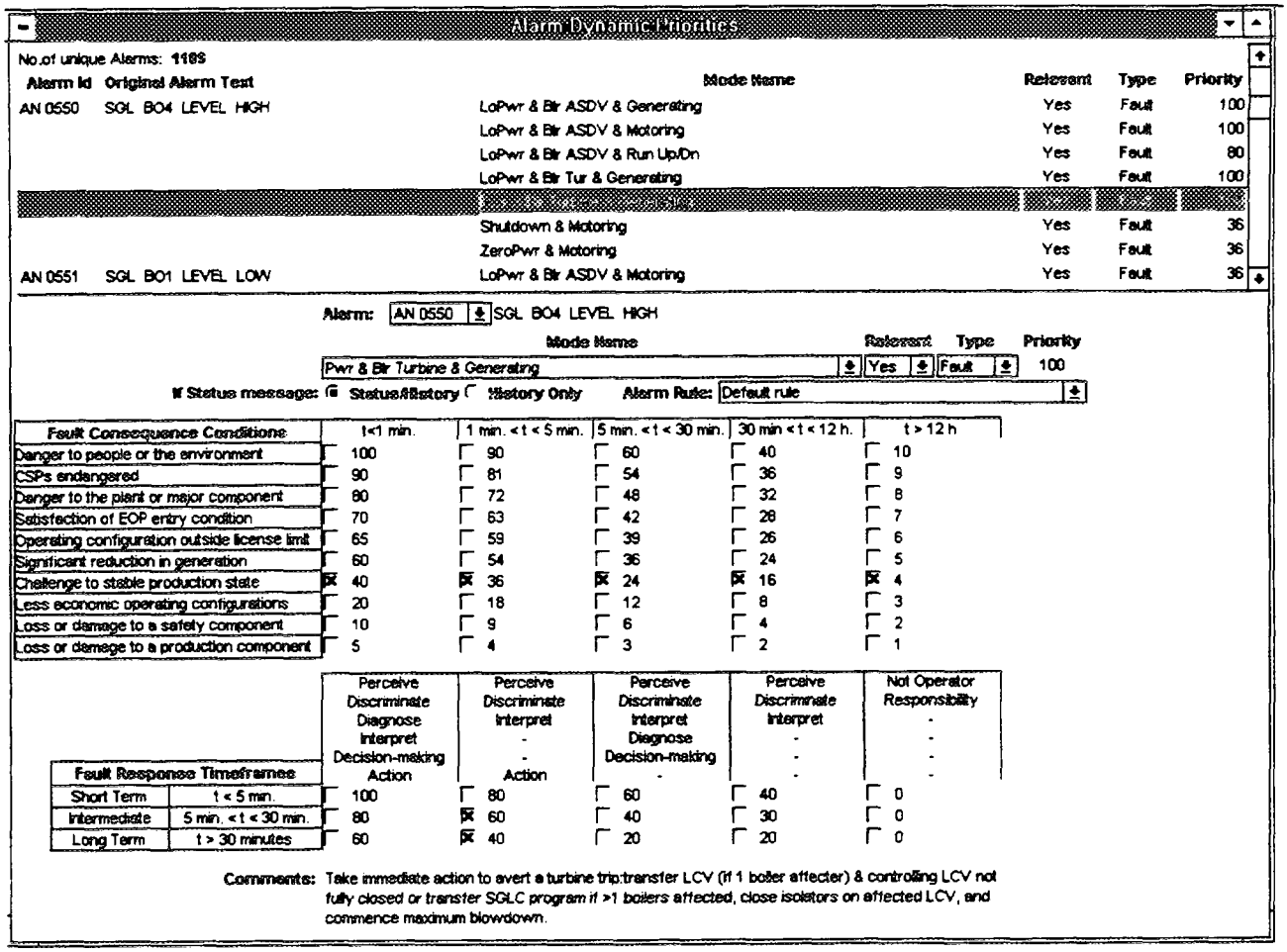


Figure 2: An Example of a Prioritization Specification Screen.

SESSION V

MODERATED DISCUSSION:

"ARE WE ADDRESSING THE REAL ISSUE?"

Moderated Discussion: Are we addressing the "real" issue?

Moderator: Mark Feher
AECL
Chalk River, ON

1. INTRODUCTION

Session 5 was a moderated discussion on the topic of "Are we addressing the "real" issue. The Moderator opened the session with the following question areas to stimulate discussion.

Questions Part 1:

Is the concept of alarms and alarm systems still valid? Are we designing for physical features rather than information that has to be conveyed? Are we addressing the essential annunciation needs or are we attempting to implement patch-work solutions to solve specific problems?

Is the design process so firmly established in organizations that a major change is required to result in different and improved approaches?

Will the cost of increasing scrutiny for Software QA make advancement impossible or too costly?

What is the role of overview displays in accident management and how do imbedded alarms play a role? Is the need for reliable signals adequately addressed (or can it be)?

Questions Part 2:

Should we include automated diagnosis and decision making with annunciation?

What is the role of the operator? Is the operator some one who only follows fixed procedures, or is he/she a responsible authority, or both?

Does the focus on safety-first divert the attention away from other important issues, such as operational efficiency?

Does the concept of "hard-wired" annunciation still apply given advancements in reliability of computer systems?

How do we shorten the design and implementation time period cost effectively while still improving the performance?

Questions Part 3:

Does the discussion of problems with existing systems in order to identify areas for improvement result in retrofit for change to existing facilities demanded by regulators?

How can innovations in the design of annunciation (or other) systems be credibly linked to the economic benefits for the change?

Complex design leads to support for complex design, which in turn leads to more complexity - why not simplify the design in the first place?

2. SUMMARY OF THE DISCUSSIONS

This summary represents highlights of statements made and does not necessarily reflect consensus of opinion amongst the participants.

- The role of annunciation includes two levels of information: overview and detailed.
- The level of quality assurance (QA) required of computerised annunciation systems should be based on the impact of the system on safety and a probabilistic model for failure (reliability).
- The concept of reliability is not being applied in the same way for hardware versus software systems.
- For reliability estimates to be adequate for truly assessing safety, the estimate must be based on a measure of the closed loop reliability of the system as a whole (which includes humans).
- The use of hard-wired back-up technology for computerised systems requires that the back-up system be integrated into normal operational use. This restricts the capabilities of the computerised system to achieve its full potential. Designs are targeting highly reliable computer systems such that the primary systems can be available and used for more than 99% of the operation.
- Several experiences have shown a trend where Regulatory scrutiny of software systems is delaying or denying design changes that would otherwise improve operational performance and therefore overall plant safety.
- There appears to be considerable overlap between "annunciation systems" and "plant display systems". The issue should not be "how we design annunciation systems" but "how we represent all the information about the plant to the operating team".
- We need more objective measures of performance to address overall reliability of the system (including the human operator).
- Annunciation around the world is being described in different ways; an operator aid, a key part of safety critical actions, and everything in between.
- Is the concept of software categorization for QA and regulatory needs "real" in the context of the whole system without closing the loop with the human operator in the system?

3. CONCLUSIONS

As with many discussions in the nuclear industry, the topic of Quality Assurance and software qualification diverted attention from key topics in improving the information systems for nuclear power plant operators. Although QA is important and reliability is needed, we must focus more attention on designing more operationally effective systems if we are in fact going to achieve high overall reliability. With limited resources available, the QA and regulatory process may be a net contributor to reduced reliability. We need to resolve the question of reliability and level of quality assurance in order to benefit from innovations.

It is clear that the concept of annunciation has undergone considerable change over the past several years. The definition of annunciation is almost as diverse as the options to implement it. The presentations over the week have clearly identified the need to alert operational personnel by redirecting their attention to important "information" about the plant. The nature of the information (problems, faults, successful versus unsuccessful changes of state, detection of events, procedural requirements, etc.) has resulted in a confusion of terminology that is masking the more creative discussions about how to better represent information to enhance operational effectiveness. The research, development, design, and regulatory community need to focus more on describing the issues in terms of information needs and use rather than focusing on the terminology used to describe it.

The nuclear industry has generated wonderful new ideas and technologies that we should all better understand and learn how to exploit for maximum benefit. There is overwhelming consensus on the problems with existing designs and there is clear evidence, as presented this week, that the industry is turning the corner and has resolutions for many of them.

In closing, let us recognise the need to develop and learn new technology, but let us not lose sight of the need to select technology and tools based on well understood operational and performance needs and not on the existence of the technology itself.

SESSION VI

INTEGRATING ANNUNCIATION AND DIAGNOSIS

DEVELOPMENT EXPERIENCE AND STRATEGY FOR THE COMBINED ALGORITHM ON THE ALARM PROCESSING & DIAGNOSIS

Hak-Yeong Chung
Korea Electric Power Research Institute
Taejon, Korea

ABSTRACT

In this paper, I presented the development experience on the alarm processing and fault diagnosis which has been achieved from early 1988 to late 1995. The scope covered is the prototype stage, the development stage of on-line operator-aid system , and an intelligent human-machine interface system.

In the second part, I proposed a new method(APEXS) of multi-alarm processing to select the causal alarm(s) among occurred alarms by using the time information of each occurred alarm and alarm tree knowledge and the corresponding diagnosis method based on the selected causal alarm(s) by using the prescribed qualitative model. With more knowledge base about the plant and some modification suitable for real environment, APEXS will be able to adapt to a real steam power plant.

1. INTRODUCTION

Recently, the need for an efficient alarm processing and fault diagnosis in power systems is continuously increasing as high quality electricity is demanded. An alarm represents an abnormal state of a power plant and can e an essential information for identifying malfunctioned states of the power plant. Note that, because of the physical function relationship among subsystems in a whole plant, multiple alarms may be fired simultaneously and consecutively[1]. In the situation of the multiple alarms, the operators should make a mental process to find out the causal alarm(s) and take some speedy managerial counter-action. Multiple alarms an overwhelm the operators in inferencing and decision making due to heavy cognitive requirements. It is also known[7] that about 40% to 50% of the shut-downs of a nuclear power plant are attributed to operator errors, some of which are caused by the huge volume of information presented to an operator.

Much work has been done for processing abrupt alarms[1-8]. In describing the knowledge of the functional and causal relationships between alarms and the plant structures, various modes were proposed including decision tables, alarm trees[15], fault trees[9], cause-consequence trees[1,4], alarm transition tables and alarm allocation models[8]. As for decision-making, methods such as pattern matching[5], prioritization rules[6], search algorithm[1,4,6], and alarm grouping

according to the plant modes[1,6] have been used to achieve alarm reduction and find the cause of malfunction.

Naito and Ohtsuka[8] developed an alarm processing system using alarm allocation models which are constructed by human expertise. Domenico et al.[6] developed an alarm processing system using model-based reasoning and object-oriented techniques. And Cheon et al.[1] proposed a prototype of an expert system for alarm processing and diagnosis. They performed alarm processing using priority grading of the plant-wide global alarms as well as the system-wide local alarms and alarm processing knowledge units which consist of cause-consequence alarm trees. Also, Cheon and Chang[3] & Chung et al[16] proposed a pattern matching method using neural networks for identifying the causal alarm(s) and the fault origin.

Chang et al. presented an on-line operator aid system (OASYS). In this paper, the OASYS is discussed by focusing attention on the importance of the operator's role for nuclear power plants (NPPs). The OASYS has been developed to support the operator's decision-making process and to enhance the safety of NPPs by providing operators with timely and proper guidelines according to a plant operation mode[17]. In 1996, Choi et al. also proposed a development strategies of the next generation man-machine interface for the nuclear power plant[18].

In many previous methods for alarm filtering, one of the major issues of concern is about "which alarms are fired ?", but sincere consideration is not made on "when are the alarms fired ?", or "what are the sequence of occurred alarms ?"[1,4,6]. Hence these conventional methods may not respond appropriately to the alarm network(or loop) problems or to the situation in which multiple alarms are fired irregularly due to some faults. In this paper, we could solve these problems using the fired time information of the multiple alarms and through alarm tree analysis.

Many algorithms on fault diagnosis have been proposed in [9,10,12]. Most of them are concerned with small part of huge plants, which are not applicable to large scale systems. Also it is very difficult to analyze the dynamics of each subsystem due to its physical complexity. So, we propose a fault diagnosis method using the knowledge of the expert operators to construct the qualitative model of each part of the plant and comparing the real trends of sensors with those from qualitative models. For the alarm processing together with fault diagnosis, the alarm processing unit is designed, based on a cause-consequence tree technique in the knowledge representation of alarms while, in alarm suppression, fired(occurred) time information together with using the priority grading of plant-wise and system-wise alarms is used to find out the causal alarm among the fired multiple alarms. And subsequently faulty components or instruments is examined in more detailed manner in the fault diagnosis module. The combined system is presented with the alarm processing and fault diagnosis modules. We construct the qualitative model with the knowledge of the expert operators in which the trends of each sensor of the plant is described as qualitative state trees.

Part 1 describes the development experience and their brief contents. Part 2 depicts the currently developed alarm processing and diagnosis method.

2. DEVELOPMENT EXPERIENCE

This section describes the development experience of the alarm processing, fault diagnosis, and man-machine interface system which are performed in a teamwork with Korea advanced Institute of science and Technology.

(a) A prototype expert system (ESAPD) for the multiple alarm processing and diagnosis has been developed for the Kori-2 nuclear power plant (NPP). ESAPD is capable of assisting the operator to identify a primary causal alarm among multiple fired alarms and to diagnose the plant malfunction quickly.

The overall plant-wide diagnosis is performed at the alarm processing stage, and the specific diagnosis for the primary causal alarm is performed at the alarm diagnosis stage. The system can also provide the emergency actions and the follow-up treatments to the operator.

The Knowledge base is partitioned into several knowledge units to handle many rules effectively. Therefore, the inference engine can handle the knowledge-base efficiently, and the knowledge units can be easily and simply updated and revised. The alarm processing knowledge units are represented as the object-oriented concepts. Also, the cause-consequence relations among alarms are represented as the alarm processing frames. In this way, the development process and the management of the knowledge base are to be simplified comparing with the traditional alarm processing methods. Based on this prototyping and a better understanding of the development problems, we have been planning to develop an on-line alarm processing system in connection with a plant computer[1].

(b) By focusing attention on the importance of the operator's role for nuclear power plant(NPPs). The On-Line Operator Aid system(OASYS) has been developed to support the operator's decision-making process and to enhance the safety of NPPs by providing operators with timely and proper guidelines according to a plant operation mode.

The OASYS with sufficient and consistent knowledge is expected to help operators and reduce operator's cognitive burden with the following activities:

- Monitoring major parameters using graphics and colors at a normal operation condition

- Identifying a malfunction state

- Providing the AOPs (Abnormal Operating Procedures) to recover the system function and to prevent a reactor trip at an abnormal condition

- Tracking dynamically the Emergency Operating Procedures (EOPs) for safe shut-down and prevention of radioactive material release[17].

(c) An intelligent human-machine interface (HMI) has been developed to enhance the safety and availability of NPPs by improving operational reliability. The key elements of the proposed HMI are the Large Display Processors (LDPs), which present synopsis of the plant status, and the compact, digital workstations for monitoring, control, and protection functions. The workstation consists of four consoles: a dynamic alarm console (DAC), a system information console(SIC), a computerized operating-procedure console (COC), and a safety related information console (SRIC). The LDPs provide a spatially dedicated, continuously viewable, integrated mimic presentation of the plant status and the compact, computerized workstations enable a single operator to operate an NPP during a normal state with the following features.

- All operating information is displayed in Korean as much as possible to help the operator's comprehension, considering his Korean culture. The configuration of the workstations and the layout of the CRT displays were designed by focusing attention on the importance of the operator's role for NPPs.

- Alarm hierarchy was established on the basis of the physical and functional importance of alarms to show the propagation of alarm impact from equipment level to plant functional level through success paths. In addition, alarm information is logically processed from generation to presentation.

- EOPs are electrically displayed and traced with skill and rule-based procedure steps automated. During stressful conditions such as abnormal or emergency operation, the related P&ID information is automatically provided on the SIC without time-consuming information navigation by linking the SIC with the DAC and the COC[18].

3. ARCHITECTURE OF APEXS

This section shows the recently developed method for alarm processing and diagnosis (APEXS). This system must also be able to do on-line monitoring of the process states, analyze the existing alarms, diagnose the fault, and inform the operator what to handle.

Figure 1 shows the simplified software configuration of APEXS with alarm processing and fault diagnosis functions for steam power plants. APEXS consists of several parts. The preprocessing unit gets all the occurred alarms and process signals from external systems such as process control system or data acquisition systems. This process data are filtered and modified to the conformable types of the database. The filtered signals are transmitted to the relational database ORACLE, which manages many kinds of data, including instrument specifications, operator supporting messages as well as all the alarm and sensor signals of the process control system. Using the data from the database and the knowledge base, the inference engine of the alarm processor searches cause alarm(s) among all the existing alarms. The data type of knowledge base is the cause-consequence alarm trees for the target plant. In case of the causal alarm related to the critical fault in the system, the fault diagnose starts to diagnose the faulty region using a

qualitative model, which describes the behavior of plant parameters. If any faulty element or cause is detected, its information would be reported through AIS. Also, as a graphic shell under X window/MOTIF environment, AIS has basic ability of on-line monitoring for all process data.

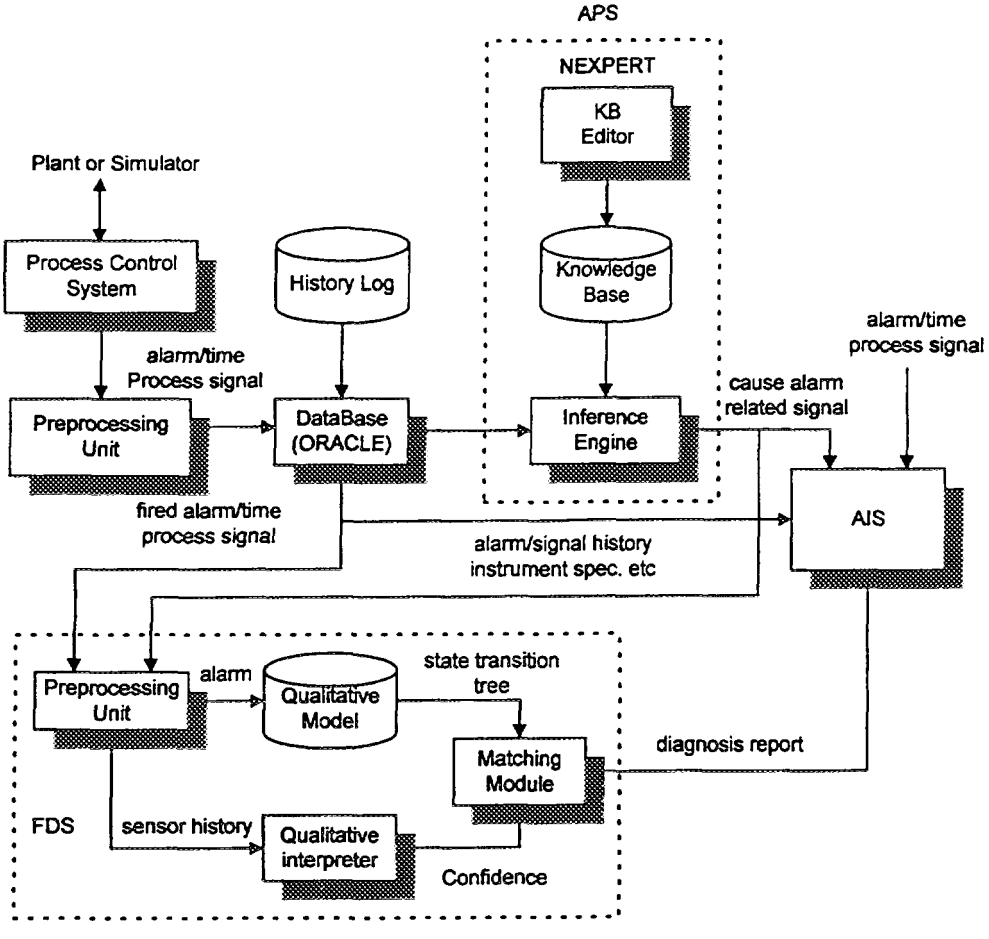


Figure 1: Simplified Software Configuration of APEXS

To have sufficient computing power, two SUN SPARC10 workstations with high resolution VGA monitor are used for APS and AIS, respectively. For the simulation of steam power plant, we used two VME racks, compatibly equipped with Force CPU30 boards and data acquisition boards, as a process control system. As a real-time OS for the process simulator and controller, VxWorks is embedded on processor boards. The related data between the process control system and APEXS are communicated through TCP/IP protocol on Ethernet cables.

4. ALARM PROCESSING AND FAULT DIAGNOSIS

4.1 Alarm Processing System with Time Information

The objectives of an alarm processing system are to reduce the number of alarms presented, find the cause alarm(s) and display suitable alarm messages. To detect the cause alarm(s), the developed alarm processing system uses a knowledge base, in which the cause-consequence alarm trees together with prioritized plant-wise alarms are stored. The knowledge base for alarm processing is formed by operators' heuristic knowledge, the analysis of piping and implementation (P&ID) and the understanding of plant structures. The cause alarm can be searched by an inference engine with the pre-performance of the alarm processing meta-rules which determines the execution procedures as shown in Table I. We executed all engineering jobs for alarm processing in the NEXPERT object.

Considering multiple faults simultaneously occurred or incompatible types of knowledge, the inference engine in NEXPERT object acquires the fired time information as well as the fired alarms. The inference algorithm describes as below. In a cause-consequence alarm tree, if a alarm has effect on the other one, we can call the alarm as *priori alarm* to the other one. Select an alarm among all the occurred ones. Among all earlier alarms other than the selected one, if there isn't any other priori alarm, then the selected one is considered as a cause alarm.

Table 1: Alarm Processing Meta Rules

No.	Rule	
No. 1	[IF]	there are descendant alarms against a selected alarm
	[THEN]	remove the descendant alarm from the dynamic memory
No. 2	[IF]	there is a precedent alarm against a selected alarm
	[THEN]	remove the selected alarm from the dynamic memory
No. 3	[IF]	there are both failure and nonfailure alarms
	[THEN]	remove the nonfailure alarms from the dynamic memory
No. 4	[IF]	there are both plant-wide and system-wide alarms
	[THEN]	remove the system-wide alarms from the dynamic memory
No. 5	[IF]	there is a group of plant state alarms
	[THEN]	remove this group of alarms from the dynamic memory

4.2 Fault Diagnosis System

The developed fault diagnosis system was implemented by using a prescribed qualitative model and an interpreter(QMI). QMI monitors noisy data and uses a qualitative model in order to diagnose the system from observed dynamic output[5].

In this paper, we adopt a new QMI algorithm using cause alarms, which are obtained from APS and the related plant dynamic data. We analyze the trend of sensor outputs which are related to a given alarm and construct all the possible state-transition trees for the available faults. For trends of two sensor outputs, an example of state-transition tree is shown in figure 2. In which, we

classify the sensors into dominant sensors(P) and subdominant sensors(Q). If the value of a dominant sensor goes over the set value of an alarm, then the alarm occurs. And we divide the values of sensor outputs into three qualitative regions for dominant sensors(N: normal, H: high, L: low) and two qualitative regions for subdominant sensors(A: normal+high, B: normal+low). The possible state transitions are represented by arrows.

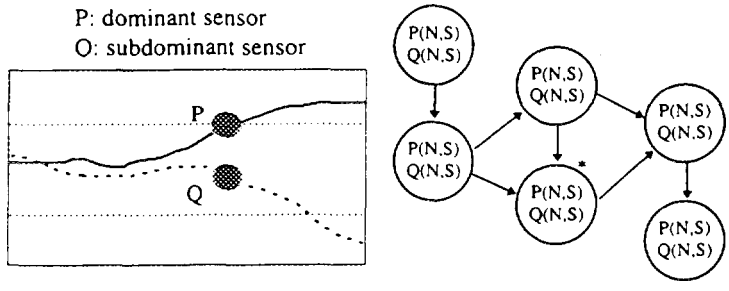


Figure 2: A State-Transition Tree for Two Sensors

The qualitative interpreter determines the confidence that each reading of sensor outputs is increasing, decreasing, or steady based upon the slope of a least squares line drawn through recent data. These confidences are then used to provide an overall confidence in a qualitative state suggested by the models. Given the confidences provided by the qualitative interpreter, fault diagnosis unit compares the qualitative states of the power plant to the states proposed by the state-transition trees.

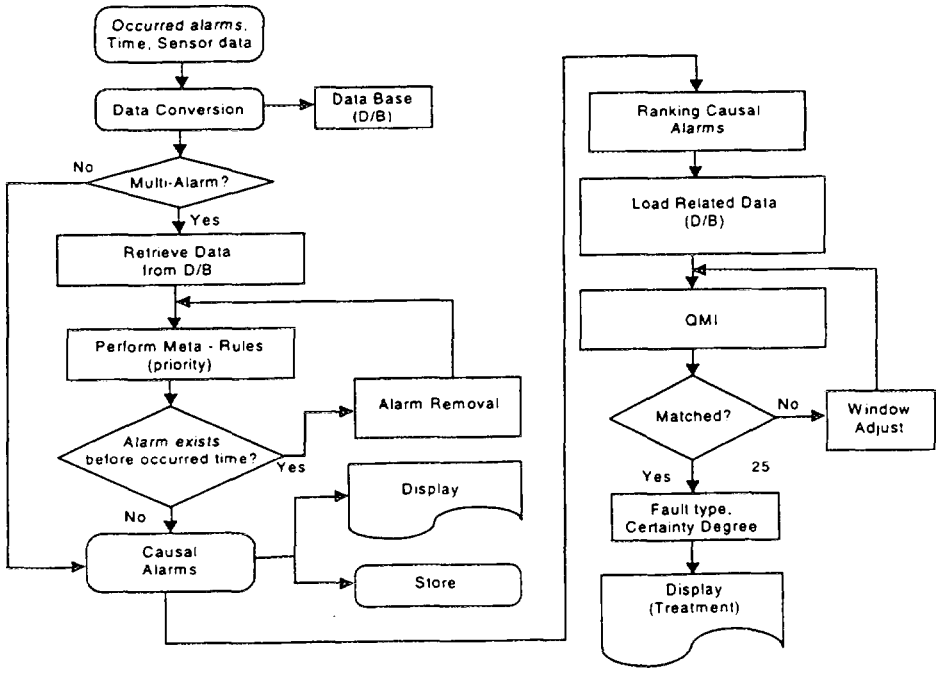


Figure 3: The Flow Chart of Alarm Processing and Diagnosis

When it matches a plant state to a qualitative state in a state-transition trees, it outputs the fault, i.e. the cause of a given causal alarm, and traces the previous states of the plant behavior and increases/decreases the certainty factor for the corresponding fault. The confidence in a qualitative state is the minimum confidence of each sensor being in that state which follows the standards of the fuzzy logic "min-max" operation. Figure 3 shows the flow chart of the combined algorithm for alarm processing and diagnosis.

5. CONCLUDING REMARKS

We showed the development experience and recent result of the combined method (APEXS) for multi-alarm processing and diagnosis. Recent works show that the overload of the huge annoying alarms in power plants can be relieved by an alarm processing expert system. In this paper , in summary, when any multiple alarms are fired in order, APEXS detects the cause alarm(s) through knowledge-based inference, and then presents the diagnosis report to the operators.

With more knowledge base about the plant and some modification to real environment APEXS will be able to adapt to a real steam power plant.

REFERENCES

[1] **S.W. CHEON, S.H. CHANG and H.Y. CHUNG**, Development Strategies of Expert System for Multiple Alarm Processing and Diagnosis in Nuclear Power Plants, IEEE Trans. on Nuclear Science vol.40, no.1, pp. 21-30, 1993.

[2] **J.O. YANG and S.H. CHANG**, An Alarm Processing System for a Nuclear Power Plants Using Artificial Intelligent Techniques, Nuclear Technology vol.95, pp.266-270, 1991.

[3] **S.W. CHEON and S.H. CHANG**, Application of Neural Networks to Multiple Alarm Processing and Diagnosis in Nuclear Power Plants, IEEE Trans. on Nuclear Science vol.40, no.1, pp.31- , 1993.

[4] **B. FROGNER and C.H. MEIJER**, On-line Power Plant Alarm and Disturbance Analysis System, Electric Power Research Institute(EPRI) Project Report-1397, 1980.

[5] **H.E. DIJK and N.V. KEMA**, AI-Based Techniques for Alarm Handling, Third Sympo. on Expert Systems Application to Power Systems, Tokyo, April, 1991.

[6] **P.D. DOMENICO, E. MAH, D. CORSBERG, J.SOMSEL, J.K. CHANNANT and J. NASER**, Alarm Processing System, Conference on Experts Applications for the Electric Power Industry, Orlando, Florida, June 1989.

[7] **P.A. SACHS, A.M. PATERSON, and M.H.M. TURNER,** Escort: an Expert System for Complex Operations in Real Time, Expert Systems, vol.3, no.1, Jan. 1986.

[8] **N. NAITO and S. OHTSUKA,** Intelligent Alarm Processing System for Nuclear Power Plants, Nuclear Technology vol.109, pp.255-264, 1995.

[9] **S. PADALKAR, G. KARSAI, C. BIEGL, and J. SZTIPANOUTS**, Real-Time Fault Diagnostics, IEEE Expert, vol.6, no.3, pp.75-85, 1991.

[10] **K.S. KANG,** A Study on the Development of the on-Line Operator Aid System using Rule Based Expert System and Fuzzy Logic for Nuclear Power Plants, Ph.D Dissertation, KAIST Dept. of Nuclear Eng., 1995.

[11] **J.M. VINSON and L.H. UNGAR,** Dynamic Process Monitoring and Fault Diagnosis with Qualitative Models, IEEE Trans. on Systems, Man, and Cybernetics, vol.25, no.1, Jan. 1995.

[12] **J. ZHANG and A.J. MORRIS,** Process Fault Diagnosis Using Fuzzy Neural Networks, Proceeding of the American Control Conference, Baltimore, Maryland, June 1994.

[13] **A. WATERS, and J.W. PONTON,** Qualitative Simulation and Fault Propagation in Process Plants, Chem., Eng., Res., Des., vol. 67, July 1989.

[14] **E.A. SCARL, J.R. JAMIESON, and C.I. DELAUNE**, Diagnosis and Sensor Validation through Knowledge of Structure and Function, IEEE Trans. on Systems, Man, and Cybernetics, vol.17, no.3, May/June 1987.

[15] **D. PATTERSON,** Application of a Computerized Alarm Analysis System to a Nuclear Power Station, Proceedings of IEE, vol.115, pp.1858-1861, 1988.

[16] **HAK-YEONG CHUNG et al.,** Incipient Multiple Fault Diagnosis in Real-Time with Application for Large-Scale Systems, IEEE Tran. on Nuclear Science, Vol.41, No.4, 1994.

[17] **SOON HEYNG CHANG et al.,** Development of the On-Line Operator Aid system OASYS Using a Rule-Based Expert system and Fuzzy Logic for Nuclear Power Plants, Nuclear technology, vol.112, Nov. 1995, 266-294.

[18] **SEONG SOO CHOI et al.,** Development strategies of an Intelligent J\Human-Machine Interface for next Generation Nuclear Power Plants, IEEE TNS Vol. 43, No. 3, June 1996, 2096-2114.

AN EVALUATION APPROACH FOR ALARM PROCESSING IMPROVEMENT

Jung-Taek Kim, Dong-Young Lee, In-Koo Hwang, Jae-Chang Park,
N.J. Na and Soon-Ja Song
Korea Atomic Energy Research Institute
Taejon, Republic of Korea

ABSTRACT

In light of the need to improve MMIS of NPPs, the advanced I&C research team of KAERI has embarked on developing an Alarm and Diagnosis-Integrated Operator Support System, called ADIOS, to filter or suppress unnecessary or nuisance alarms and diagnose abnormality of the plant process. ADIOS has been built in an object-oriented AI environment of G-2expert system software tool, as presented in a companion paper. ADIOS then is evaluated according to the plan in three steps; (1) preliminary tests to refine the knowledge base and inference structure of ADIOS in such a dynamic environment, and also to evaluate the appropriateness of alarm-processing algorithms, (2) to ensure correctness, consistency, and completeness in the knowledge base using COKEP (Checker Of Knowledge base using Extended Petri net), and (3) the cognitive performance evaluation using the Simulation Analyzer with a Cognitive Operator Model (SACOM) in the KAERI's Integrated Test Facility (ITF).

1. INTRODUCTION

Although alarm information is the primary source to detect abnormalities in nuclear power plants or other process plants, the conventional hardwired alarm systems, characterized by "one sensor-one indicator", has a alarm flooding problem[1]. Much research work has been done worldwide to help resolve this problem of cognitive overload [1-3]. The advanced I&C research team of Korea Atomic Energy Research Institute (KAERI) is developing Alarm and Diagnosis - Integrated Operator Support (ADIOS) system for computerized process monitoring, alarming, and diagnosis as part of our effort to develop Diagnosis, Response, and operator Aid Management System(DREAMS). As our initial effort we are working on an alarm system using G2 real time expert system shell[4] to devise the basic concepts of alarm processing and a generic architecture for processing and presentation. However, the introduction of new alarm processing techniques have caused many problems in view point of human factors, such as information navigation in workstations, alarm processing and presentation strategies, and alarm control and information feedback. To solve these human factor problems, it is necessary to establish the human factor evaluation method and evaluate the cognitive performance in real operational environment.

ADIOS is planned to undergo several performance evaluations to ensure its validity especially during major upsets. At the outset, an evaluation plan is made in accordance with guidelines in EPRI-NP-3659 and NUREG/CR-6105, sometimes augmented by our own experience and insights. The plan involves establishing evaluation method, developing test scenarios, building up an evaluation environment, and preparing the assessment criteria on human-machine interactions of the alarm processing system.

ADIOS then is evaluated according to the plan in three steps: First, preliminary tests were carried out by establishing a data communication link between the ADIOS built in G2 and the KAERI's Compact Nuclear Simulator. The purpose of these tests was to refine the knowledge base and inference structure of ADIOS in such a dynamic environment, and also to evaluate the appropriateness of alarm-processing algorithms. Next, an evaluation of the correctness, consistency, and completeness in the knowledge base of the ADIOS system is carried out using an automated V&V tool, called COKEP (Checker Of Knowledge base using Extended Petri net)[5]. Lastly, the cognitive support of ADIOS to human-machine interactions will be tested and evaluated using the Simulation Analyzer with a Cognitive Operator Model (SACOM) in the KAERI's Integrated Test Facility (ITF)[6].

This paper first summarizes the methodology for alarm processing and presentation in ADIOS system. Next, we discusses the preliminary tests and lastly, an evaluation plan of the completeness in the knowledge base and the cognitive performance to human-machine interactions.

2. SUMMARY OF ADIOS

In ADIOS, alarms are processed by several representative methods including equipment-state dependency, plant mode dependency, alarm generation, cause-consequence relationship (sometimes called, direct precursor) and multi-setpoint relationship, in addition to some unique methods. Our unique methods include separation of the process alarms (e.g., temperature or pressure alarms of the main process) from equipment-related alarms (e.g., vibration or lubrication alarms of a pump), presentation of status alarms (e.g., PORV not closed) on the process mimic, representation of group alarms assimilating information from several related alarms.

Many process alarms are represented in group on the process overview mimic. For example, the alarms, e.g., those denoted as "Tavg", "ΔT", "Flux", and "SGL", represent several related alarms. As a specific example, the "SGL" group alarm includes high-high, high, low, and low-low steam generator level alarms. The group alarms take the highest priority among the associated subsidiary alarms that have been activated. Activation of any equipment alarm makes the boundary color of corresponding equipment change to red on the process overview mimic diagram. When the operator wishes to look at the specific alarms, he/she can click on the equipment after first acknowledging the alarm. Then, the specific alarms are shown on its sub-workspace.

Each alarm in ADIOS is initially classified into one of three different priority groups: (1) the first priority group of priority 1 or 2, (2) the second priority group of priority 2 or 3, and (3) the third priority group of priority 3. These classification of every alarm is based on its importance as to the promptness of the operators' response needed, or the effect of the alarm on the plant process or equipment. The prioritized alarms are displayed on the process overview mimic diagram, and also the time-sequential list of alarms is givens on another dedicated CRT, with those alarms categorized by systems shown on the third CRT as a spatially dedicated soft alarm

panel. The process alarms prioritized to 1, 2, or 3 are shown on the main CRT differently in red, yellow, or white, respectively. The same color coding is applied to the alarm texts in the alarm list, and also to the window tiles on the soft alarm panel.

3. PRELIMINARY FUNCTIONAL TESTS

Figure 1 illustrates the system configuration of the ADIOS prototype. Workstation (WS) 1 is the Functional Test Facility (FTF) of KAERI which simulates the process behavior of Kori 3&4 nuclear power plants in Korea. WS2 is the host processor for alarm processing where the G2 real-time expert system shell runs and the alarms are processed.

In the preliminary functional tests, the accident scenario of TMI-II nuclear power plant in 1979 was simulated to test the alarm processing methodology and to demonstrate the feasibility of the alarm system. Figure 2 shows a snapshot of the primary and secondary overview mimic diagram in ADIOS after the reactor trip. Many process alarms that have been activated are lowered in priority and are shown yellow; including the high flux rate alarm(labeled flux) and low pressure and flow alarms in the secondary system(condensated pump discharge flow low, condensated pump common discharge pressure low, feedwater pump NPSH low and so on). ADIOS presents only 36 alarms as the first priority alarms which require more attention from the operators relative to other second and third priority alarms.

4. A VERIFICATION OF KNOWLEDGE BASE

Most of alarm processing and operator support systems employ a rule-based formalism for knowledge representation since it is the simplest knowledge representation method to develop. In spite of this advantages, incorrectness, inconsistency, and incompleteness in a knowledge base may be inadvertently brought into the knowledge base because it is often built in an incremental process. In other words, such anomalies may occur at any stage in the knowledge transfer process that is to transfer expertise from the human expert into the computer by the knowledge engineers. Therefore, it is widely noted that assuring the reliability of knowledge-based system is very important, and it is also recognized that the process of verification is an essential part of reliability assurance for these systems.

As mentioned above, ADIOS has configured the knowledge base using G2 expert system shell. Although several strategies or tools have been developed to perform potential error checking of the knowledge base, they often neglect the reliability of verification methods. Because a Petri-Net provides a uniform mathematical formalization of knowledge base, we will employ an automated tool, called COKEP(Checker Of Knowledge base using Extended Petri net), for detecting incorrectness(redundant, subsumed, circular rules), inconsistency(conflict rules), and incompleteness(unreachable conclusion, unreferenced conditions, isolated, omitted rules) in a knowledge base of ADIOS alarm processing system.

4.1 Extended Petri Nets

An expended petri net is composed of six parts: a set of place P, a set of transition state place P', a set of transition T, input function I1, input function I2, and output function O. The input and output functions are related to transitions and places. P = { p1,p2, ..., pn} is a finite set of places, n >= 0. P' = {p'1,p2',....., p'm} is a finite set of transition state place, m>= 0. T = {t1,t2,...., tm} is a finite set of transitions, m>=0.

Input places of the transition are classified into two types. 'A' is the output place of a different rule, which is used for searching the path of chained rules. 'B' is the initial marking place, which is used for finding the known fact of chained rules(Figure 3). Input functions I1, and I2 are made by each input place, 'A' and 'B'. Place 'C' is the transition state place that informs whether transition is fired or not. Since the place 'A' and 'B' maintain the information of known fact, after firing transition, another place, 'C', is required to check the firing transition.

4.2 Anomaly Detection

As the detection of anomalies is based on the results of firing transition, verification problems of ADIOS knowledge base can be expressed as reachability problems. In order to solve these problems matrix analysis of the extended Petri net and backward chaining methods of the rule set are employed. The matrix analysis has some problems in checking anomalies. The result vector of firing transition tj in marking u is a necessary but not sufficient condition for reachability analysis in chained rule set. A backward chaining method is used for solving this problem. The result vector of firing transition is obtained by matrix analysis. Then, we find chained rule path using matrix D1 and backward chained method. The conditions for chained rule transition can be acquired by matrix D2 which has the information of initial marking places. The certainty factor checking is performed after finding the chained rule path. The general procedure of these checking process is shown in Figure 4.

5. AN EVALUATION PLAN OF HUMAN PERFORMANCE

5.1 An Evaluation Environment

As mentioned above, the cognitive support of ADIOS to human-machine interactions will be tested and evaluated using the Simulation Analyzer with a Cognitive Operator Model (SACOM) in the KAERI's Integrated Test Facility (ITF). The ITF is a human factors experimental environment to evaluate an advanced man machine interface design. The ITF includes a human machine simulator(HMS) comprised of a nuclear power plant function simulator, man-machine interface, experiment control station for the experiment control and design, human behavioral data measurement system(SCADA), and data analysis and experiment evaluation supporting system(DAEXESS). The most important features of ITF is to secure the flexibility and expandability of Man-Machine Interface(MMI) design to change easily the environment of experiments to accomplish the experiment's objects. Figure 5 illustrates the layout of ITF.

5.2 An Experiment Design Process

A process of the human factors experiment design must begin with an analysis of the purpose of the experiment and the requirements. The outcome of this analysis provides the basis for making decisions about training, supporting, material, performance observation, and measurements, data collection facilities, and needs, scenario descriptions, possible modification to the simulator, MMI design, selection of subjects - as well as to the analysis of the results. The second phase is the training of the subjects to be used(operators, crews, specialized subjects, experts, etc.). This phase also includes the preparation of the experiment, i.e. defining all the details of scenario description, developing supplementary facilities, modifying or developing procedures, MMI design and testing, preparing specific performance recording apparatus(eye tracking, physiological measures) etc. The third phase is the actual experimentation where the experiment is carried out in the ITF. This phase of the overall experiment requires scheduling the use of the simulator, subjects, instructors, experimenters, etc. The last phase is the analysis of results. The experiment is clearly not over until the results have been analyzed and interpreted vis-a-vis the purpose. The data analysis may require considerable support, e.g. for merging various performance records(logs, video, etc.), synchronization, iterative filtering and clustering, as well as specialized data analysis tools for physiological data, video recordings, etc. Table 1 represents the activities and requirements for each phase.

6. CONCLUSIONS

This paper has described the overall plan to evaluate the processing completeness and cognitive performance of ADIOS.

ADIOS then is evaluated according to the plan in three steps: First, preliminary functional tests were carried out by establishing a data communication link between the ADIOS built in G2 and the KAERI's Compact Nuclear Simulator. The purpose of these tests is to refine the knowledge base and inference structure of ADIOS in such a dynamic environment, and also to evaluate the appropriateness of alarm-processing algorithms. Next, an evaluation of the correctness, consistency, and completeness in the knowledge base of the ADIOS system is carried out using an automated V&V tool, called COKEP (Checker Of Knowledge base using Extended Petri net). Lastly, the cognitive support of ADIOS to human-machine interactions will be tested and evaluated using the Simulation Analyzer with a Cognitive Operator Model (SACOM) in the KAERI's Integrated Test Facility (ITF).

References

[1] L.R. Lupton, P.A. Lapointe and K.Q. Guo, "Survey of International Developments in Alarm Processing and Presentation Techniques", *NEA/IAEA International Symposium on Nuclear Power Plant Instrumentation and Control,* Tokyo, Japan, May 18-22, 1992.

[2] I.S. Kim, "Computerized Systems for On-Line Management of Failures: A State-of-Art Discussion of Alarm Systems and Diagnostic Systems Applied in the Nuclear Industry", *Reliability Engineering and System Safety* 44 (1994) 279-295.

[3] J.M. O'Hara, W.S. Brown, J.C. Higgins, and W.F. Stubler, "Human Factors Engineering Guidance for the Review of Advanced Alarm Systems," NUREG/CR-6105, U.S. Nuclear Regulatory Commission, August 1994.

[4] Kim, I.K. Hwang, D.Y. Lee, J.C. Park, and C.S. Ham, "An Integrated Approach to Alarm Processing," *2nd American Nuclear Society Topical Meeting on Nuclear Plant Instrumentation, Control and Human-Machine Interface Technology,* University Park, Pennsylvania, USA, May 1996.

[5] Il W. Kwon and Poong H. Seong, "A Knowledge-Based Verification of NPP Expert Systems using Extended Petri Nets", Proceedings of the Korean Nuclear Society Autumn Meeting, Seoul, Korea, October 1995.

[6] In S. Oh, Kyung H. Cha, etc., "Development of An Integrated Test Facility(ITF) for the Advanced Man Machine Interface Evaluation", Proceedings of the Korean Nuclear Society Autumn Meeting, Seoul, Korea, October 1995.

Phase	Contents, activities	Requirements
Analysis of requirements	- Definition of experiment purpose - Clarification of conceptual contents of investigation - Requirements to MMS functionality - Specification of expected results(general "ideal path") - Definition of independent and dependent variables - Identification of main constraints(time, money, people, customer expectations, etc) - Selection & devcelopment of specific experiment design	- Access to "customer" - Experience from previous experiments - Estimates of total available resources
Pilot experiment (prototyping)	- MMI design and testing - GUI development and testing - Prepare performance recording apparatus - Fine tune specific experiment design - Development supplementary facilities, procedures, etc.	- GUI design tools - ITF-STR - Measurement devices - Subjects (limmited)
Training and preparation	- Derivation of training requirements(needed conceptual and practical training) - Design of training program. and training aids - Selection of subjects - Implementation of training program - Evaluation of results - Define detailed scenario of actual experiment	- ITF-STR - ITF-MTR(partly) - Subjects - Instructors
actual Experiment	- Description of experiment conditions - Identification of possible sources of failure and safeguards against them - Execution of experiment - Measurement and data collection	- ITF-MTR - Subjects - Instructors - Observers
Analysis of results	- Transformation and merging of raw data - Analysis of performance registrations - Development of "ideal path" description for actual performance - Analysis of independent and dependant variables - Evaluation of total system performance - Interpretation of results in terms of specified purpose	- ITF-STR - Experiment data base - Analysis tools - Subjects(limited) - Customer

Table 1: The Activities and Requirements for each Experimental Phase

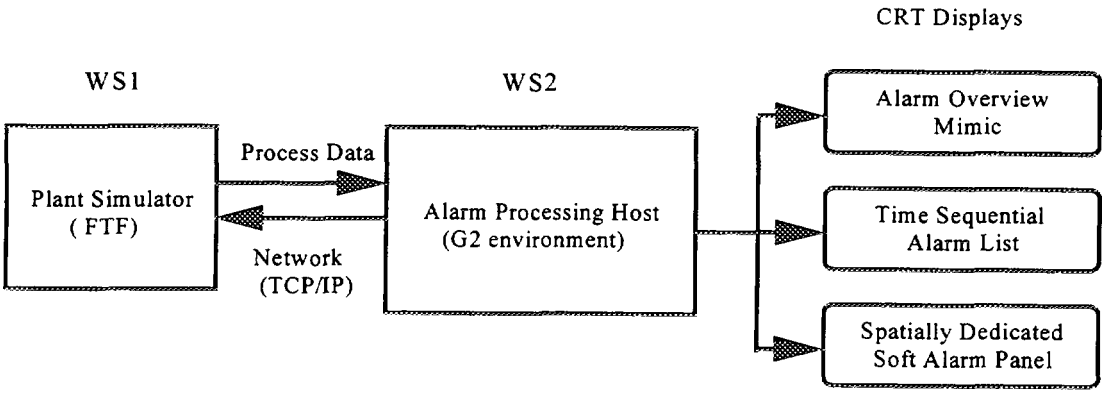


Figure 1: System Configuration of ADIOS Prototype

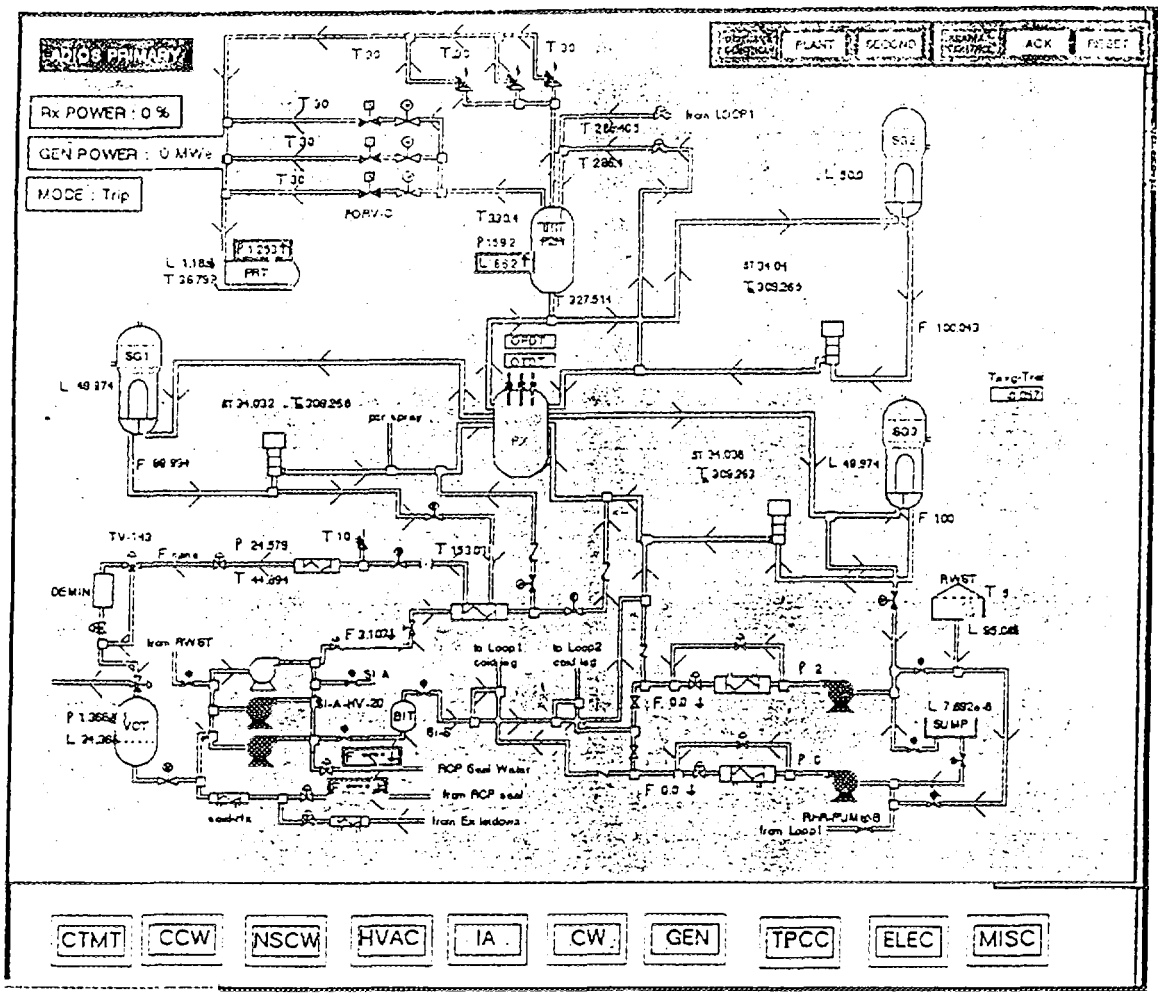


Figure 2: The Primary and Secondary Overview Mimic Diagram

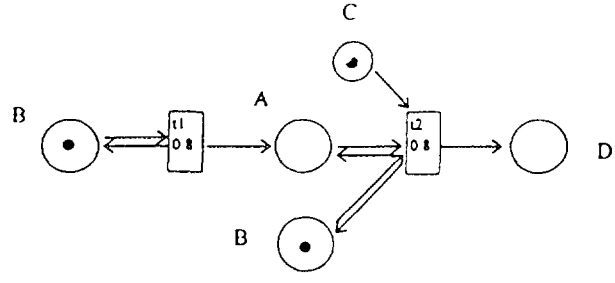


Figure 3: An Example of the Extended Petri Net Model

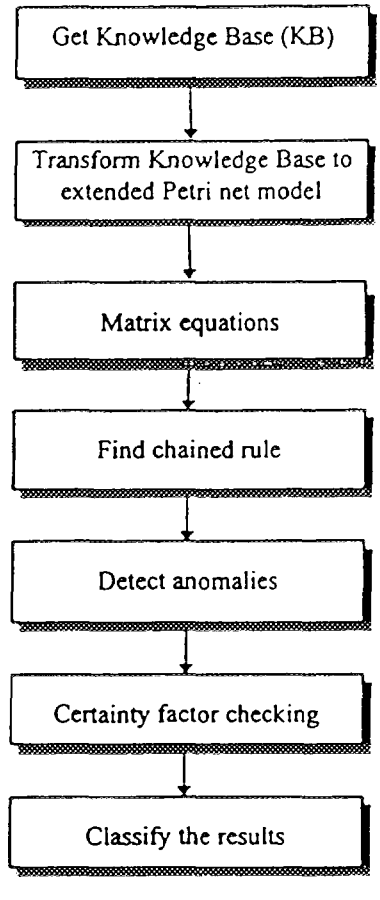


Figure 4: The Schematic Diagram of the Anomalies Detection Procedure

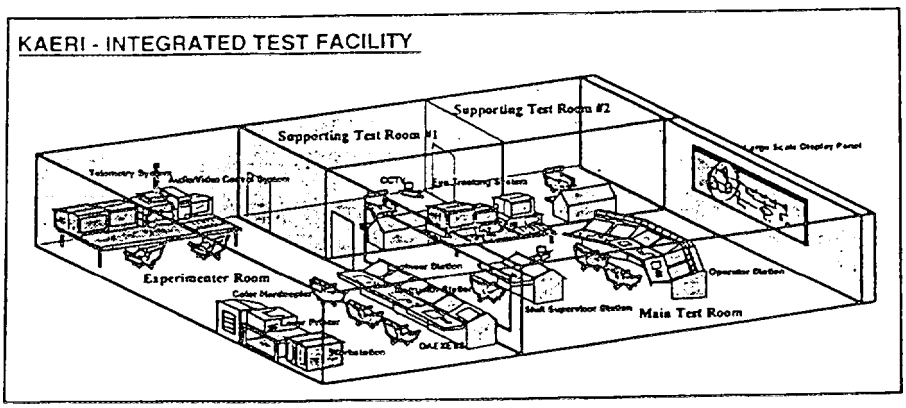


Figure 5: The Layout of ITF

A NEW DIAGNOSIS METHOD USING ALARM ANNUNCIATION FOR FBR POWER PLANTS

Y. Ozaki, K. Suda, S. Yoshikawa, K. Ozawa
Power Reactor and Nuclear Fuel Development Corp.
Ibaraki, Japan

ABSTRACT

We discuss the methodology diversity for diagnosis reasoning in autonomous operation system, and propose a new diagnosis method using alarm annunciation system. The methodology diversity is assured by preparing plural agents, each of which is based on its own different methodology, therefore, it is expected for the reliability in diagnosis to be improved. Meanwhile, the combination of annunciated alarms is expected to be peculiar to the anomalous phenomenon or accident. Moreover, as the state of affairs is developing, each appearance of the pattern is changing with time peculiarly to each anomaly or accident. The matter is utilized for the new diagnosis method. The patterns of annunciated alarms with progress of the events are prepared in advance under the condition of the anomalies or accidents by use of plant simulator. The diagnostic reasoning can be done by comparing the obtained combination of annunciated alarms with the reference templates, pattern matching method. On the other hand, we have another method, called as COBWEB used for conceptual classification in cognitive science, to reason for diagnosis. We have carried out the experiments using the loop type LMFBR plant simulator to obtain the various combinations of annunciated alarms with progress of the events under the conditions of anomalies and accidents. The examined cases were related to the anomalies and accidents in the water/steam system of the LMFBR power plant. We have obtained the conclusions that it is effective to reason the causes of anomalies using the annunciated alarms. We are going to apply the pattern matching technique or COBWEB method into the diagnostic reasoning to confirm the performance of the proposed diagnosis method based on the alarm annunciation.

1. INTRODUCTION

Since it is desired to enhance availability and safety of nuclear power plants operation and maintenance by removing human factors, there are many researches and developments for intelligent operation and diagnosis using artificial intelligence(AI) technique.

We have been developing an autonomous operation system for nuclear power plants by substituting AI for plant operators and in addition conventional controllers used in existing plants, taking the case of loop type LMFBR power plant (1). With autonomy in the autonomous operation system, the general idea is stated clearly from five items as follows: (1) to operate and maintain the plant fundamentally by itself based on its own given norm, (2) to operate the plant without being dependent on human operator under condition of normal operation mode and of design based anomalous phenomena, (3) to operate the plant as instructed by human under

condition of not-design based anomalous phenomena, (4) to inspect and maintain the plant in cooperation with human under normal operation mode, (5) to inspect and repair the plant components as instructed by human for periodical inspection and troubles or accidents of the plant functions. Therefore, it is essential to build up the autonomous operation and maintenance system for the plant by AI and intelligent robot techniques.

For the autonomous operation system, we have adopted a hierarchical distributed cooperative configuration to recognize its function, and a multi-agent architecture, in which each method performing individual function such as diagnosis of plant, state estimation, and operating control, is carried out by each agent respectively, to realize the distributed cooperative system. In the system, we have also proposed a methodology diversification, that consists on applying plural methods based on different principles to a specific task in diagnosis or control. It enables mutual backup to prevent loss of system functions caused by an obstacle occurred in an agent by isolating it, and facilitates the reorganization of the system function using remaining agents. And also, it is expected to improve reliability of diagnosis and to optimize control performance through the methodology diversification.

As the first step of the development, we have been developing the prototype system. As for the diagnosis systems, at present, they consist of two diagnostic reasoning levels, a plant level based on a hierarchical plant functional model, and a local level based on a physical causal network model using qualitative reasoning technique(2).

For the methodology diversification in diagnosis, we now attempt to supply a new diagnostic method besides the qualitative reasoning method. In the paper, we discuss the methodology diversity for the above-mentioned local level diagnostic reasoning, and propose a new diagnosis method using alarm annunciation system. The combination of annunciated alarms is expected to be specific to the anomalous phenomenon or accident. Moreover, as the state of affairs is developing, each appearance of the combination is changing with time specifically to each anomaly or accident. We intend to utilize the matter for the new diagnosis method.

2. DIAGNOSIS METHOD USING ALARM ANNUNCIATION

Regarding the methodology diversification of diagnosis in the autonomous operation system, plural diagnosis methods in which different principles are applied to the same anomalous phenomenon. The concluding diagnostic result is then made by a mutual agreement based on a rational standard from result obtained by each method.

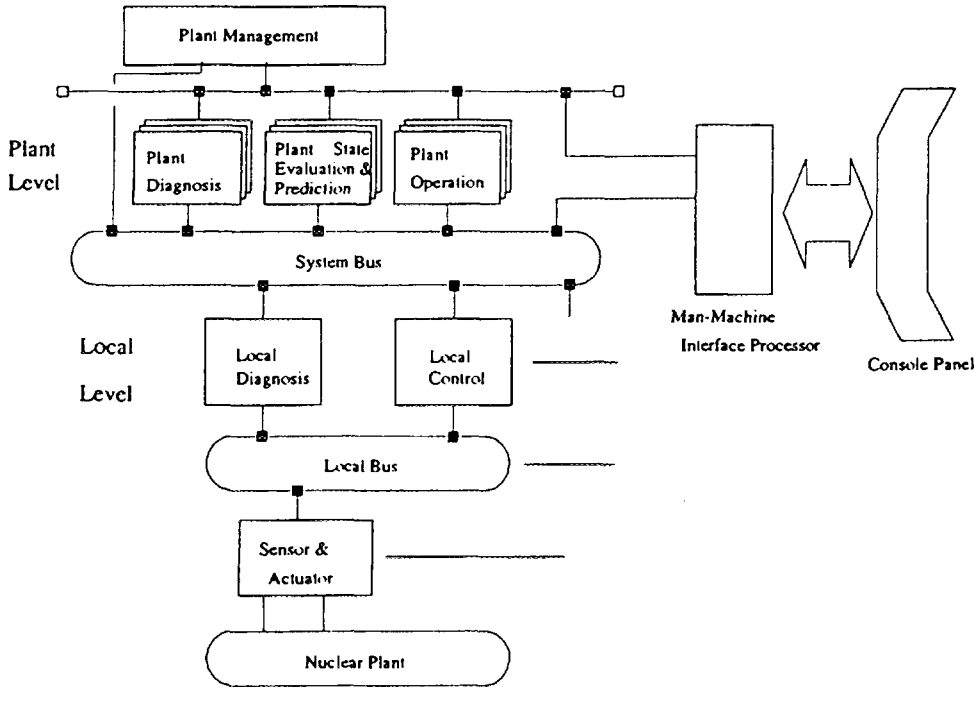


Fig.1: System Configuration of Prototype Autonomous Operation

Figure 1 shows the prototype autonomous operation system which we have been developing as the first step mentioned above. We now intend to discuss about the local level diagnosis in Figure 1. Relation between the methodology diversification in diagnosis and the mutual agreement for rational diagnostic result is shown in Figure 2.

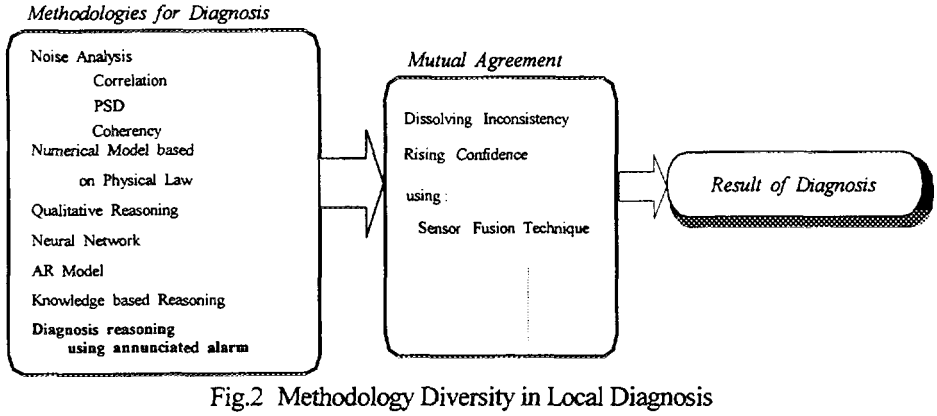


Fig.2 Methodology Diversity in Local Diagnosis

Besides, Figure 3 shows what are the mutual supplement and mutual agreement between the plural diagnosis in the methodology diversification. Various diagnosis methods are applied to the same anomalous phenomenon and rational and confident diagnostic result is obtained

through each result from respective diagnosis. At present, in the prototype system, we develop a new diagnosis method using alarm annunciation as a part of the methodology diversification in local level diagnosis system.

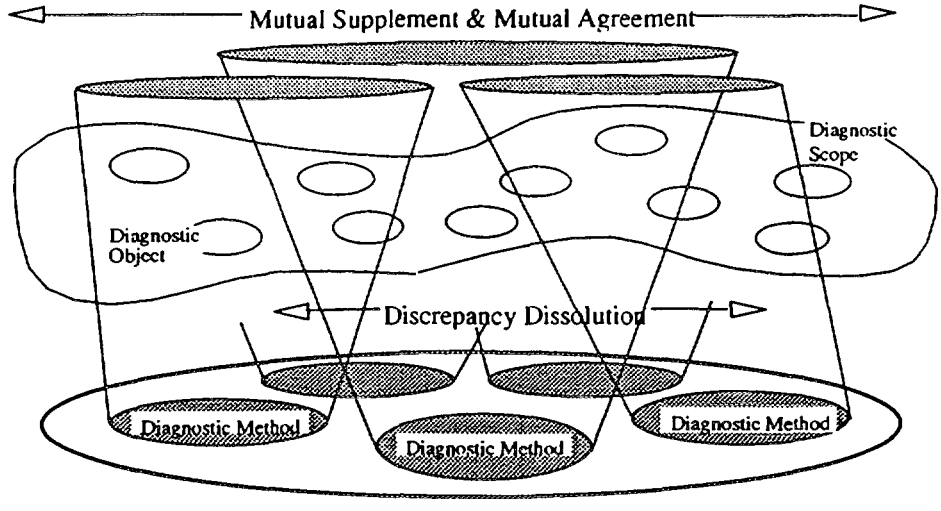


Fig. 3 Objective of Methodology Diversity

It can be said that the diagnosis method using alarm annunciation finds out the cause of anomaly by paying attention to the combination pattern of annunciated alarms and to the change of the annunciated alarm combination pattern as time developing when an anomalous phenomenon or an accident occur in plant. The combination patterns of annunciated alarms with progress of the events are prepared in advance under the condition of anomalies or accidents by use of plant simulator. Each combination pattern is utilized as the templates corresponding with each anomaly or accident, respectively. The diagnostic reasoning can be done by comparing the obtained combination of annunciated alarms with the templates. The diagnostic reasoning can produce the results with the degree of confidence given by the rate of agreement with the templates. Figure 4 shows what is an outline of diagnosis by pattern matching with an annunciated alarm combination pattern immediately after an occurrence of anomaly and the template pattern for diagnostic reasoning. However, it is thought to be difficult to identify the cause of anomaly only from the alarm combination pattern immediately after the occurrence. Therefore, it is necessary to improve a conviction degree of diagnostic result using time change of the alarm combination pattern with development of anomalous phenomenon. In other words, as for an aspect of each change of alarm combination pattern with development of phenomenon, there is expectation that peculiar characteristic behavior dependent on each anomalous phenomenon will be done. What is shown on the point that would be given conviction degree of diagnostic result by degree by using a change with time of the annunciated alarm combination pattern is Figure 5. Here is shown the technique to reasoning cause accompanied with conviction

degree for diagnostic result by agreement degree by a method of pattern matching with the annunciated alarm combination pattern and the template pattern as standard.

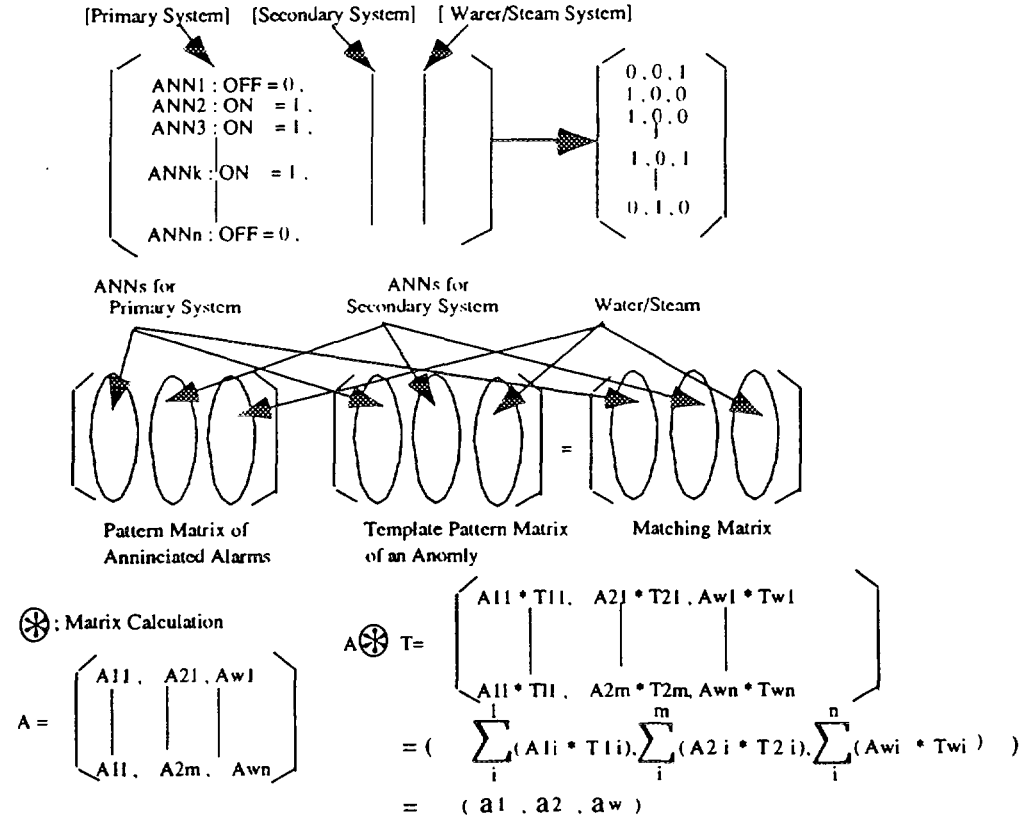


Fig. 4 Pattern Matching Method for Diagnosis

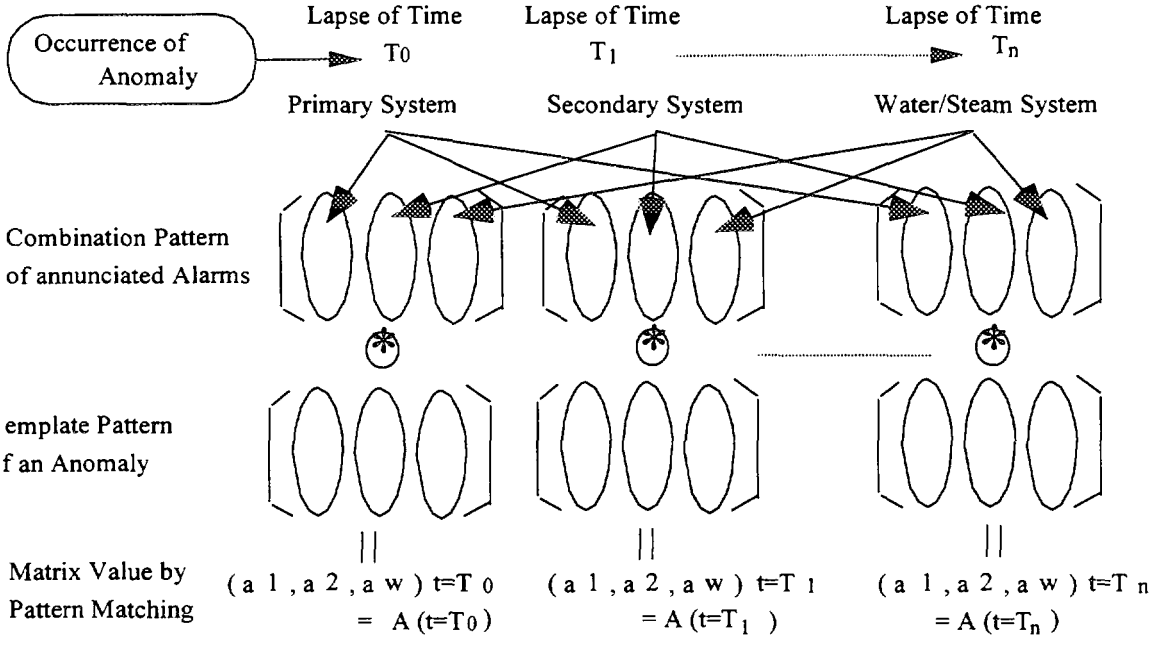


Fig.5 Pattern Matching Method between the Patterns of annunciated Alarms an Templat corresponding to an Anomaly using the Changes of Patterns as Time goes by

On the other hand, there is a different diagnosis method from the above mentioned method of pattern matching technique, that is, a method based on a conceptual clustering(3) as a kind of inductive learning called as learning from observation among unsupervised learning. The conceptual clustering method accepts a set of object descriptions like events, observations, and facts, and produces a classification scheme over the observations. The method does not require a teacher to preclassify objects, but uses a heuristic index, called as category utility for category evaluation based on concept of family resemblance used in the field of cognitive psychology, to discover classes with good conceptual descriptions. Clustering forms a classification tree over objects. Plural cases are classified into hierarchical classes according to their family resemblances by category utility. COBWEB method(4) is known to be a popular and effective method for the conceptual clustering. COBWEB is an incremental method for hierarchical conceptual clustering. The method carries out search just like a hill-climbing through a space of hierarchical classification schemes using operators which enable bi-directional transfer through the space. The method incrementally incorporates objects into a classification tree, where each class or node is a probabilistic concept which represents an object class. The incorporation of an object is a process in itself of classifying the object by going down the tree along an adequate path, renewing category utilities along the path, and executing an operator among four operators at each level class. The four operators are as follows: (1) to classify the object into an existing class, (2) to create a new class, (3) to combine two classes into a single class, (4) to divide a class into two classes, following the value of category utility.

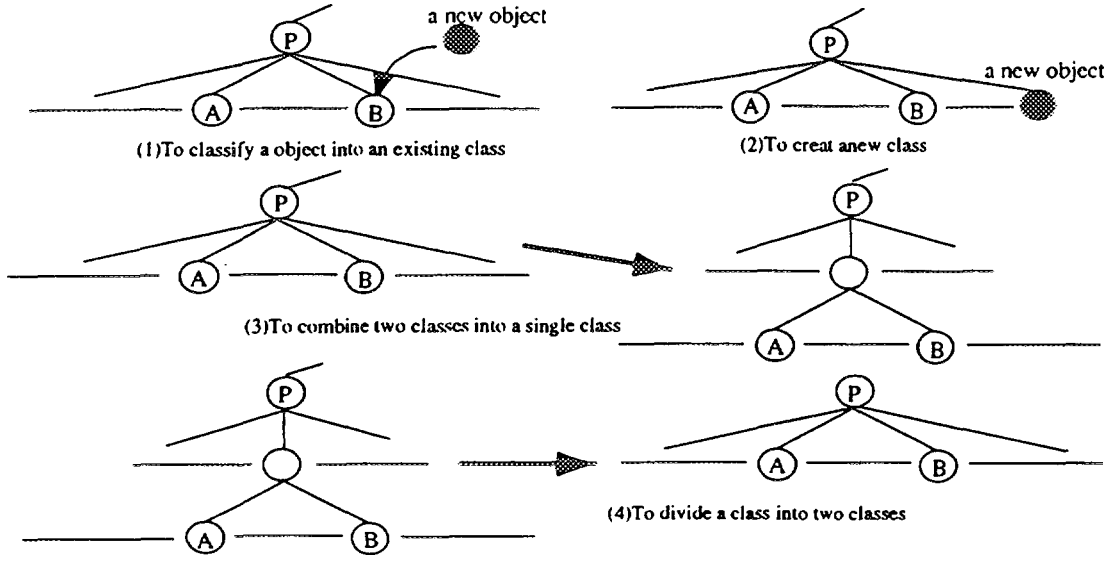


Fig. 6 Four Four Operators in COBWEB

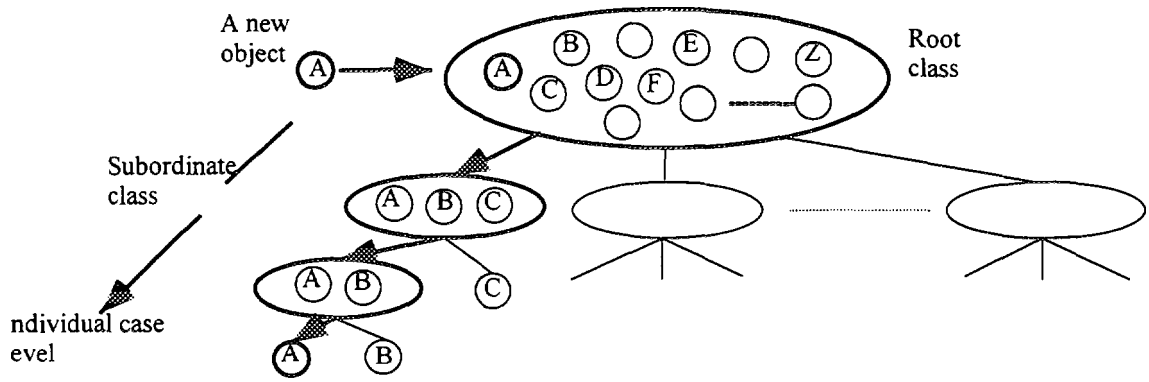


Fig.7 Outline of Process in Classificating a New Object

Figure 6 shows the four operators in COBWEB classification. Figure 7 shows an outline of a process in classifying a new object, that is, corresponding to a process in diagnosis reasoning when is obtained a new annunciated alarm combination pattern by occurring an anomalous phenomenon.

The matter above mentioned is, however, discussion about static objects or cases, that is, the conceptual clustering is done without consideration about attribute of time. In diagnosis for anomalous phenomenon occurred in plant, are important the momentary progress, transition, and propagation of the anomalous phenomenon as time goes by as from the occurrence. Therefore, it is necessary to consider the change of attribute (i.e., each annunciated alarm) as essential attribute for conceptual classification. When we applied COBWEB to the diagnosis using annunciated alarms, state of 'on' or 'off' of each annunciated alarm is regarded as attribute for the classification, and changing time from 'off' to 'on', or from 'on' to 'off' of each annunciated alarm, which is lapse of time starting from first alarm annunciation cased by occurrence of an anomalous phenomenon, is also regarded as attribute. It can be said that there exist two concepts in the conceptual classification, that is, one is a conceptual class made up of attributes of annunciated alarms, another is a conceptual class made up of attributes of changes of state, 'on' or 'off', with changing time of each annunciated alarm. The former conceptual class is called as 'schema class', and the latter is 'state class'(5). Therefore, each hierarchical conceptual schema class, built up from alarms annunciated by an anomalous phenomenon for diagnosis reasoning, involves state classes as time series attributes, respectively. The outline of the hierarchical structure made up of schema classes and state classes is shown in Figure 8. In conceptual classification for anomalous phenomena with time developing, it is divided with two parts, that is, the schema class formations and the state class formations, and it can be done by performing each class formation reflexively.

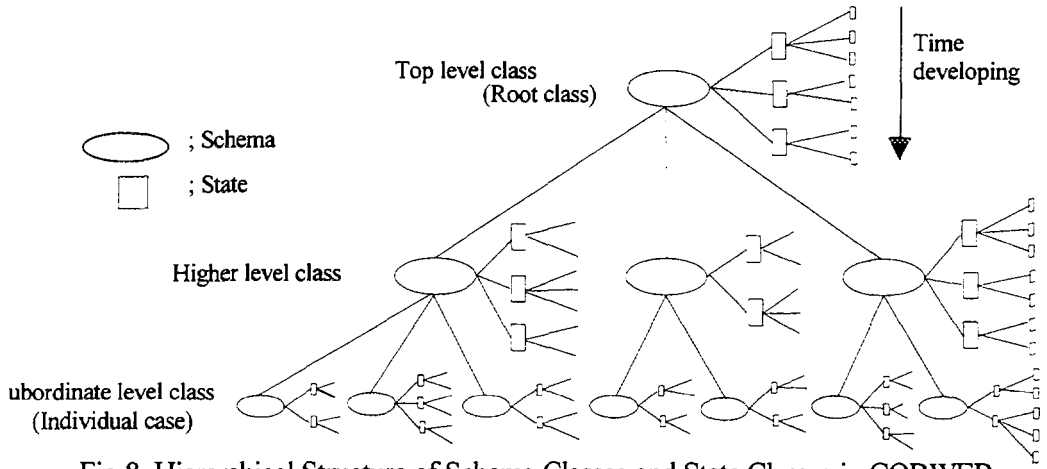


Fig.8 Hierarchical Structure of Schema Classes and State Classes in COBWEB

In actual diagnosis in plants, operators carry out momentary diagnosis reasoning using the annunciated alarms changing as time goes by as from the occurrence of anomalous phenomena. Namely, they do diagnosis reasoning roughly and produce some candidates of causes immediately after the occurrence, and as the state of affairs advances, they specify a candidate of cause gradually. In other words, their diagnosis reasoning become more and more unquestionable as the conviction degree rises higher. Both the pattern matching and COBWEB are the methods of diagnosis reasoning that can provide a reliable result of diagnosis reasoning gradually to us as way as the operators is doing the diagnosis reasoning in existing plants. It can be said that both reasoning methods are essentially equivalent with regard to diagnosis reasoning for dynamic phenomena having schema and state attributes just like an anomaly in plants. While, the pattern matching method is a conceptual classification using observed objects sampled at every specific time, COBWEB is, on the other hand, a conceptual classification involving attributes with all specific times of changes of state of itself.

In any case that the pattern matching or COBWEB method is used in diagnosis reasoning, it is essential that there are specific differences among the combination patterns of annunciated alarms with time developments obtained by occurrences of anomalous phenomena in FBR power plants.

3. EXPERIMENTS BY PLANT SIMULATOR

For confirmation of the propriety of the diagnosis method based on alarm annunciation, that is, the pattern matching method or COBWEB method, it is necessary to examine each combination pattern of annunciated alarms obtained by anomalous phenomena, in advance, using by a plant simulator if each pattern is peculiar to an anomalous phenomenon, respectively. Therefore, we have carried out the experiments using a 3 loop type LMFBR plant simulator to obtain the various combinations of annunciated alarms with progress of the events under the conditions of anomalies and accidents occurring. Figure 9 shows the block diagram of LMFBR modeled in the plant simulator.

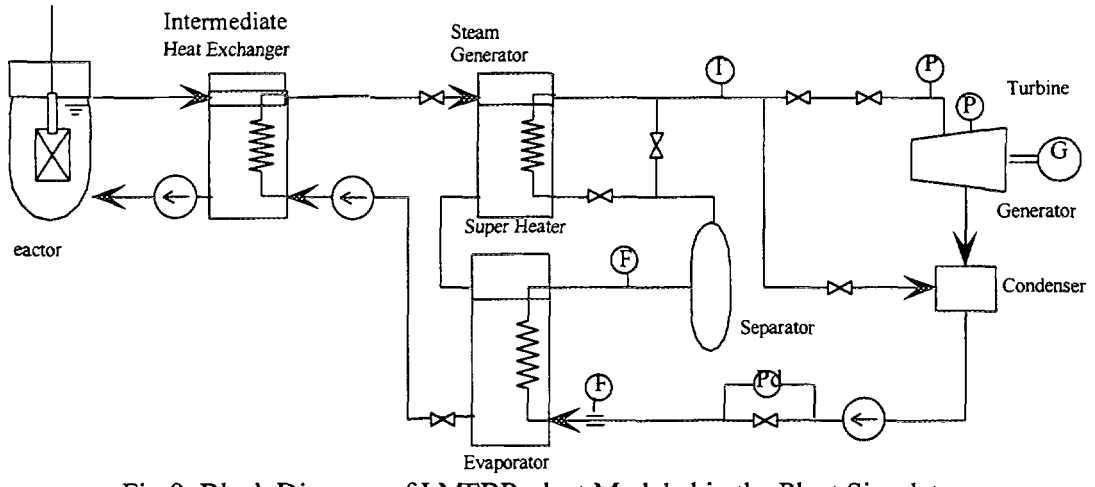


Fig.9 Block Diagram of LMFBR plant Modeled in the Plant Simulator Used in the Simulation Examination

The examined cases were related to the anomalies and accidents in the water/steam system of the LMFBR power plant. We have examined thirty four kinds of anomalous phenomena, taking time series data of annunciated alarms, events list, together with typical trend process data. And also, we carried out the examination two times at interval of one month to see if the state of affairs in annunciated alarms reappears for each anomalous phenomenon. The examined anomalous phenomena are listed in Table 1. These anomalies are registered as standard malfunctions in the plant simulator. All the examinations have been carried out under the condition that the plant is operated in 100% full power.

Figure 10 shows an example of the timing flowchart arranged from the events list of a series of annunciated alarms as time goes by as the anomalous phenomenon develops, in a case of W-13-01, that is, an anomaly of closing all stopping valves in 3 feedwater loops by mistake. All events lists obtained in the examination tabulated in Table 1 have been arranged into the timing flowcharts as shown in Figure 10, respectively. In the timing flowcharts, the lapse of time in the flowchart starts from the time when the first alarm is annunciated by the occurrence of anomaly. Then, from all the examined cases, it was observed that 201 alarms are annunciated all in examined 34 cases of anomalies on steam/water system of LMFBR plant. We have made the pattern of combination of annunciated alarms from the timing flowchart of events, at interval of specific time, respectively. For example, in Figure 11, is shown the pattern of combination of annunciated alarms obtained in the malfunction of W-13-01 at about 5 sec after the occurrence of anomaly that is regarded as an initial stage of anomaly. In this case, the initially annunciated alarms were 6 alarms of 'EV A FW FLW L/LL', 'EV A,B,C OUTL STM TMP CONT ABNML', 'W/S A OUTL PRS H', and 'FCV DIF CONT ABNML'.

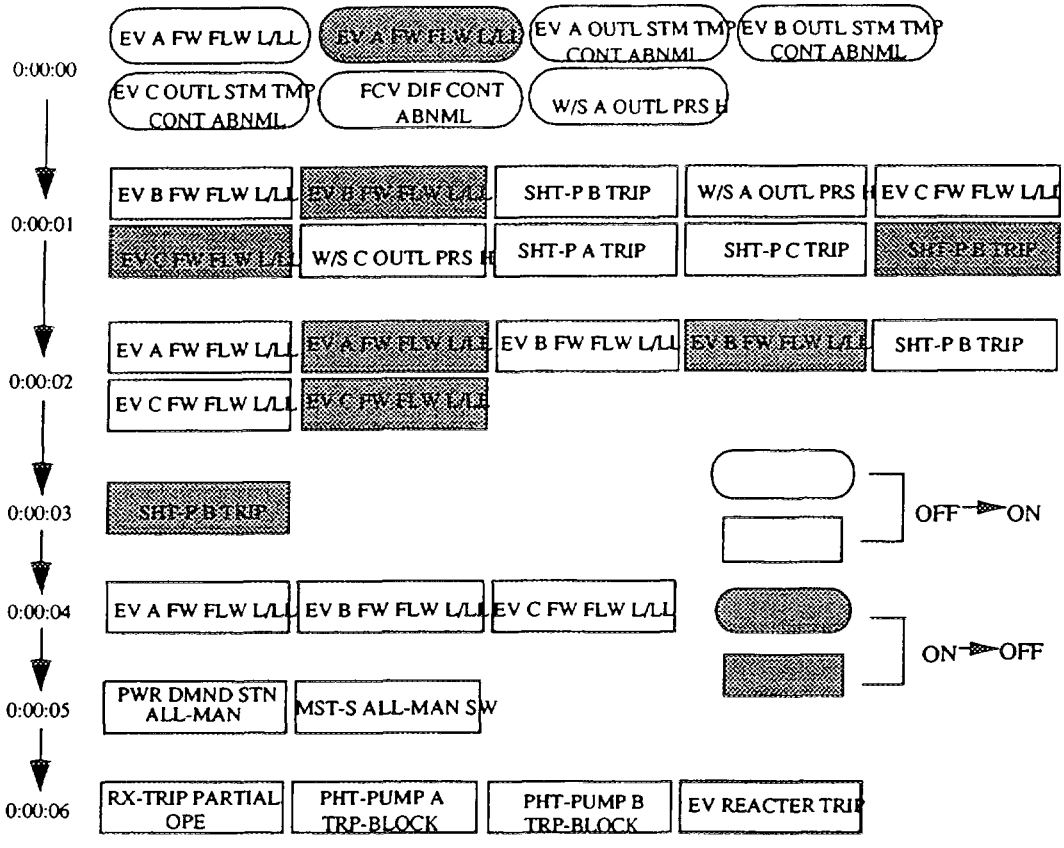


Fig. 10 Timing Flowchart Arranged from the Events List in Case of W-13-01 Corresponding to Anomaly of Closing all Stopping Valves in 3 Feedwater Loops

By the way, it was observed that there were plural cases in which the alarm, 'EV A OUTL STM TMP CONT ABNML', appeared as an initially annunciated alarm among the examined cases. These cases were the anomalies of W-06-01, W-08-01, W-09-01, W-11-01, W-13-01, W-13-02, W-17-01, W-18-01, W-27-01, and W-27-02 tabulated in Table 1. We can not define the cause of anomaly among the above mentioned candidates only from the initially annunciated alarm, 'EV A OUTL STM TMP CONT ABNML'. However, comparing the annunciated alarms in these cases at about 5 sec after the occurrence of anomaly such as shown in Figure 11, it was observed that, in the cases of W-06-01 and W-08-01, the alarms of 'EV B,C OUTL STM TMP CONT ABNML' and 'FCV DIF CONT ABNML' were annunciated initially, in the case of W-09-01, the alarm of 'EV B,C OUTL STM TMP CONT ABNML' was annunciated and the alarm of 'FCV DIF CONT ABNML' followed after that. Besides, in the case of W-11-01, there was not any alarm without the alarm of 'EV A OUTL STM TMP CONT ABNML', and in the case of W-13-01, were initially annunciated the above mentioned alarms and the alarms of 'PHT- PUMP A,B TRP-BLOCK', 'EV B,C FW FLW L/LL', 'SHT-P A,B,C TRIP', 'MST-S ALL-MAN SW', and 'RX-TRIP PARTIAL OPE' follow after that. In the case of W-13-02, it was almost similar to the case of W-13-01 except for annunciating the alarms of 'SHT W/STM TRIP DMND' and 'B,C FW SHT NA FLW MIS-MATCH'. There were no differences between the case of W-09-01 and the

cases of W-17-01, W-27-01, and W-27-02. The case of W-18-01 was similar to the case of W-13-01 except for annunciating the alarm of 'W/S A OUTL PRS H'. It was done to define each anomaly of W-11-01, W-13-01, W-13-02, and W-18-01 from the combination patterns of annunciated alarms at 5 sec after the occurrences, respectively. The other cases were regarded as an same group, and could not be distinguished each other. But we could see the differences between these cases difficult to distinguish, comparing the changes of annunciated alarms as time goes by after that. That is, seeing the timing flowchart of annunciated alarms corresponding with each anomaly, in the case of W-06-01, the alarm of 'EV A,B,C OUTL STM TMP CONT ABNML' once changed from 'on' to 'off' at 9 sec after the initial annunciation of alarm, and changed from 'off' to 'on' over again at 2 sec after that. In the case of W-08-01, the alarm of 'EV A,B,C OUTL STM TMP CONT ABNML' changed from 'on' to 'off' at 9 sec after the initial annunciation. In the case of W-09-01, the alarm of 'EV A,B,C OUTL STM TMP H/HH' was annunciated at 13 sec after. On the other hand, in the case of W-17-01, the alarm of 'EV A,B,C OUTL STM TMP H/HH' was annunciated at about 9 sec after. In the case of W-27-01, the alarm of 'FCV DIF CONT ABNML' changed from 'on' to 'off' at 10 sec after, and the alarm did not return to 'on' for about 90 sec after that, and, in the case of W-27-02, meanwhile, the alarm behaved in the similar way but returned to 'on' at about 30 sec after that. Besides, the alarm of 'HP-2HTR DRN LVL H/L' was newly annunciated at about 30 sec after.

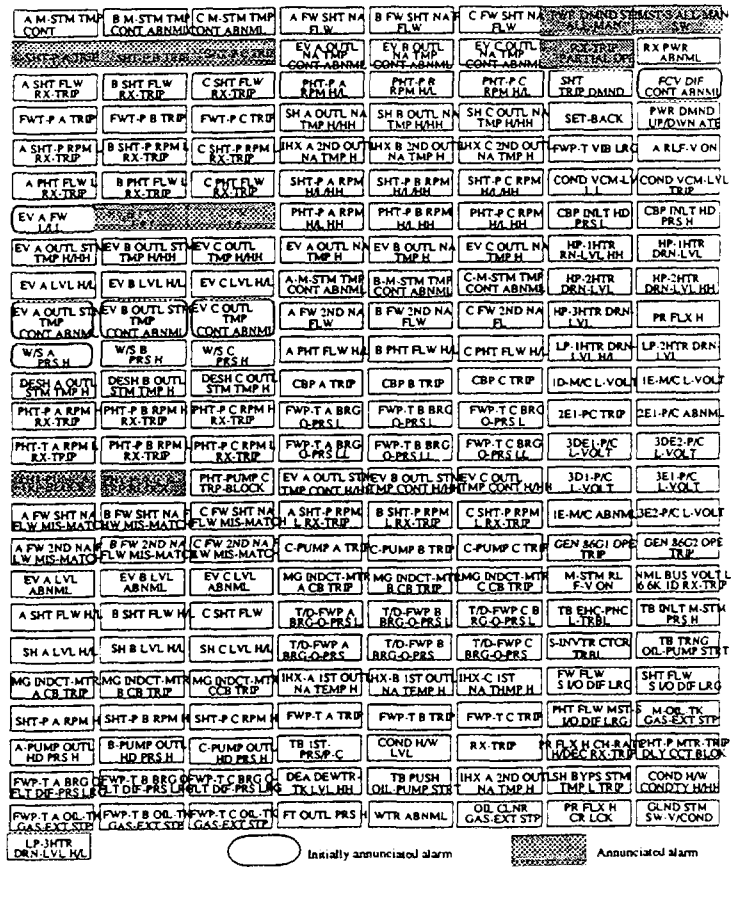


Fig. 11 Pattern of Combination of Annunciated Alarms Obtained at 5 sec after from the Initial Alarms for the Malfunction W-13-01 of the Simulation Test by the LMFBR Plant

As is mentioned above, when the alarm of 'EV A OUTL STM TMP CONT ABNML' was initially annunciated, are reasoned as candidates of causes of anomalies the cases of W-06-01, W-08-01, W-09-01, W-11-01, W-13-01, W-13-02, W-17-01, W-18-01, W-27-01, and W-27-02, and, at 5 sec after the initially annunciating, is distinguished the case of W-11-01, W-13-01, W-13-02, and W-18-01, respectively, among them, and, at 15 sec after that, is distinguished the case of W-06-01, W-08-01, W-09-01, and W-17-01, respectively, and lastly, at about 30 sec after, the case of W-27-01 and W-27-02, respectively, is finally rezoned. The sequence of the reasoning mentioned above is shown in Figure12. It can be said that it is possible to reason and distinguish each cause of anomalous phenomenon among all the anomalies in the water/steam system of LMFBR from the patterns of annunciated alarms with the changes of the patterns as time goes by.

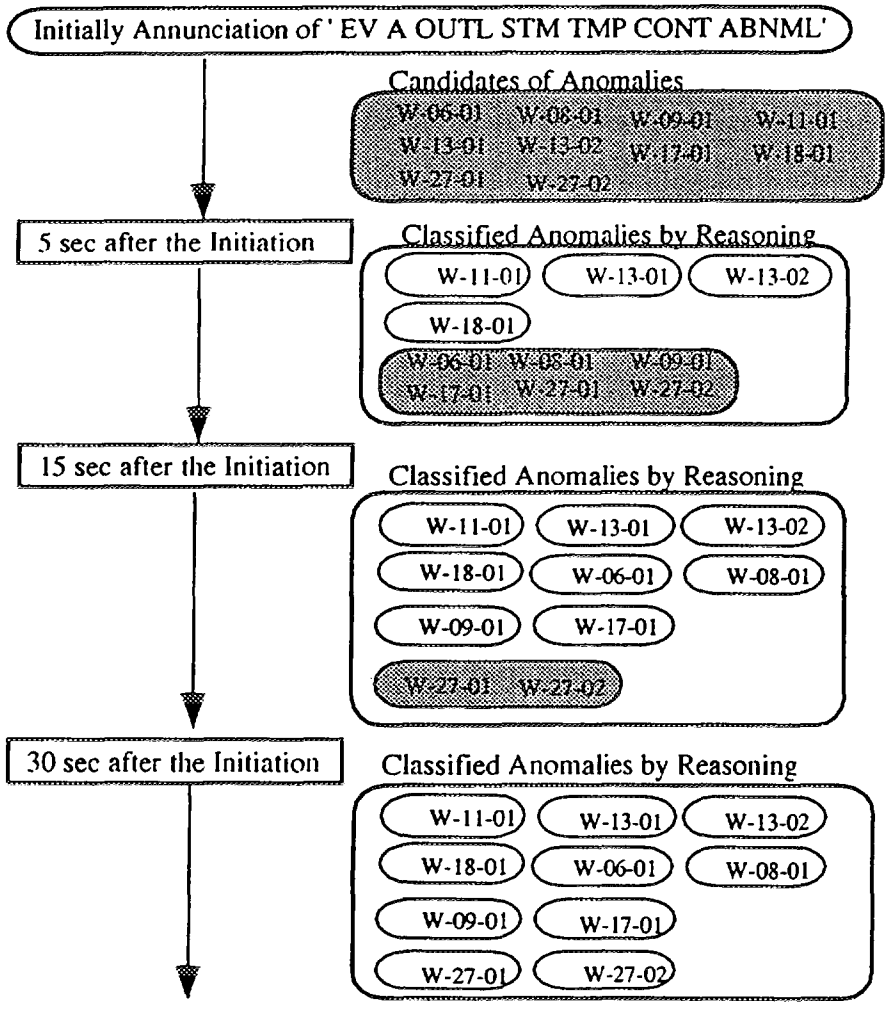


Fig. 12 Process of Reasoning the Cause of an Anomaly among the Candidate of Anomalies in the Case that a Same Alarm is Initially

Next, we have tried the classification of the above mentioned cases by COBWEB method. Firstly, has been done the classification without attributes of time when the status of alarms change from 'off' to 'on' or from 'on' to 'off', that is, considering only the status of 'on' or 'off' of alarms. The result of classification without attributes of time is shown in Figure 13. Secondly,

we have tried the classification of the cases with attributes of time when the status of alarms change from 'off' to 'on' or from 'on' to 'off', and Figure 14 shows the result of the classification. Seeing each result of classification, it may be said that both of the classification without and with attributes of time produce the appropriate conceptual classification, respectively, where resemble cases are classified into a single unit class. From the present results, we are sorry to say that there are no conspicuous differences between the results without and with attributes of time. However, at any rate, it has been found that COBWEB method has a potentiality to furnish an effective result of classification for diagnosis reasoning using only annunciated alarms without any knowledge about the plant constitutions and functions. But, on the other hand, there are some problems solved to apply COBWEB to diagnosis reasoning, that is, how to obtain the general result of classification independently on calculation parameters, how to calculate in real-time in spite of process using great many attributes for classification, and so on. These are future subjects.

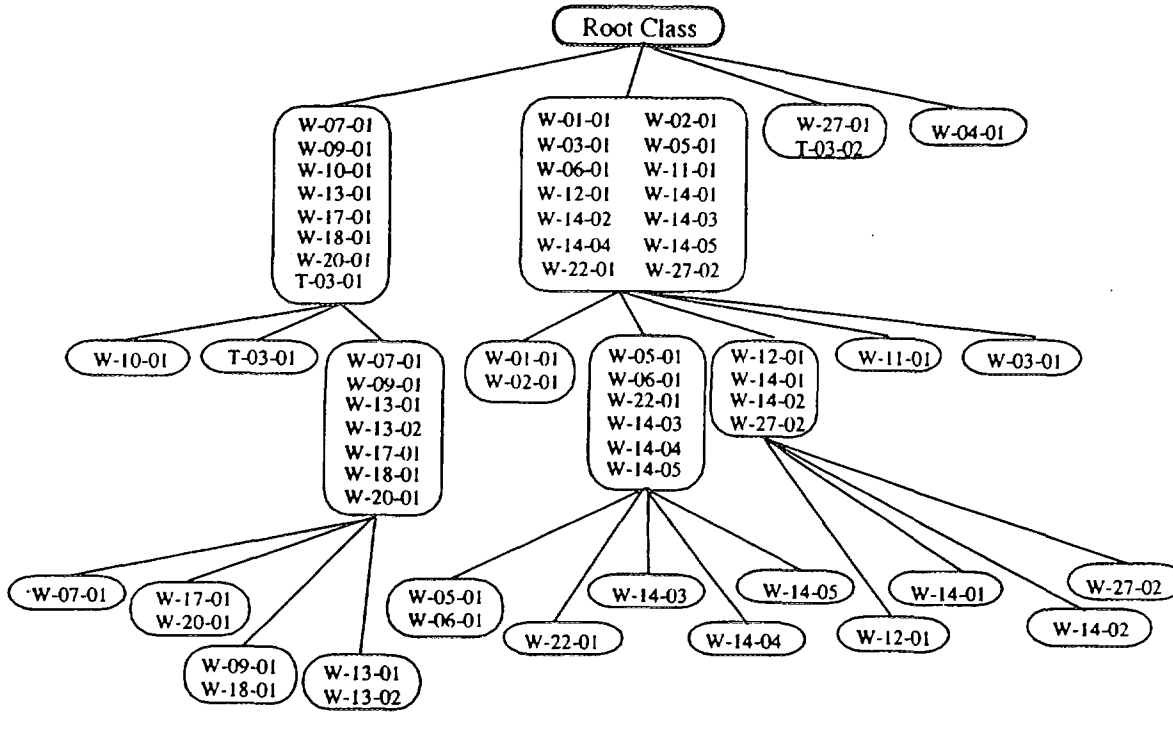


Fig. 13 Example of Classification for Anomalies Simulated Using Plant Simulator Without Attributes of Time

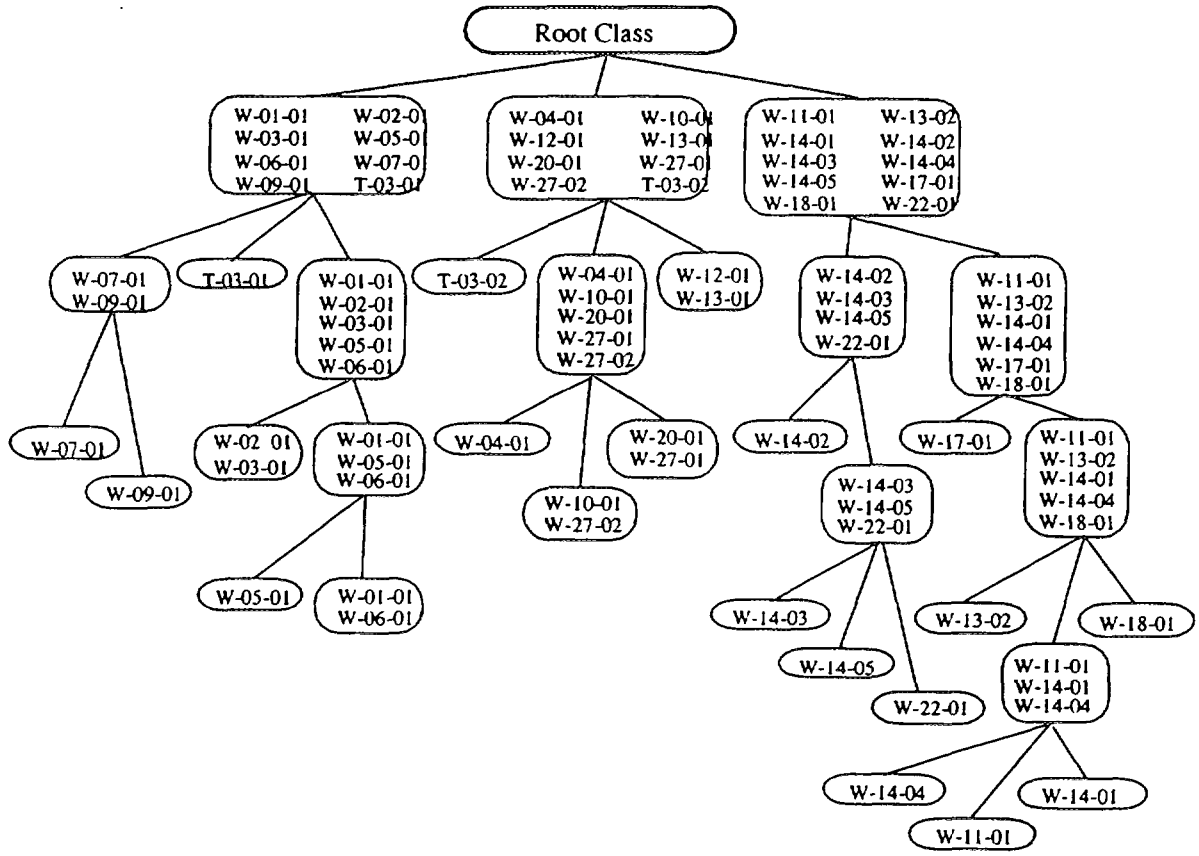


Fig. 14 Example of Classification for Anomalies Simulated Using Plant Simulator with Attributes of Time

4. CONCLUSIONS

We have now presented a new diagnosis method using alarm annunciation from a point of view of methodology diversification for diagnosis for autonomous plant operation system, and have also carried out simulation examinations to estimate the efficiency of the diagnosis method. We have obtained the conclusions from the results of examinations by plant simulator as follows:

(1) it is possible to reason and classificate the cause of anomalies from the patterns of annunciated alarms with regard to anomalous phenomena in the water/steam system.
(2) it is essential to utilize the change of the pattern of annunciated alarms with time for reasoning the causes of anomalies.
(3) it is expected to progress the reasoning and focusing among the candidates of causes of anomalies with improved conviction degree as time goes by from the occurrences of anomalies.

We have also found that it is promising to use the method of the pattern matching or COBWEB for diagnosis reasoning. There are, however, some subjects solved in applying the methods to diagnosis reasoning. We will investigate in the future which method is more effective for

diagnosis reasoning using annunciated alarms, the pattern matching or COBWEB, clearing the problems to be solved in applying to diagnosis reasoning for LMFBR plants.

5. ACKNOWLEDGEMENTS

We would like to thank H.YAMAMOTO for putting the massive data obtained in the simulation test by plant simulator in order. We would also like to acknowledge T. Odo, N. Koyagoshi, T. Okude, T. Kawanishi and other members of Monju Construction Office, PNC for supporting and cooperating in carrying out the simulation test by plant simulator. Further, we would like to thank A. Saiki of Industrial Electronics & System Laboratory, Mitsubishi Electric Corp. for calculating by COBWEB for conceptual classification with regard to the cases obtained in the simulation examination by the plant simulator.

REFERENCES

[1] K. OKUSA, et al., "Prototype a fully autonomous nuclear power plant operation system", 9th Power Plant Dynamics, Control & Testing Symposium, 24-26 May, 1995, Knoxville, Tenn., USA.

[2] S. YOSHIKAWA, et al., "Nuclear power plant monitoring and fault diagnosis method based on the artificial intelligence technique", 7th Symposium on Reactor Surveillance and Diagnosis,19-23 June,1995, Avignon, France.

[3] M. GLUCK, et al., "Information, uncertainty and the utility of categories", Proc. of the 7th Annual Conf. on Cognitive Science Society, Lawrence Erlbaum, Irvine, CA, pp.283-287, 1985.

[4] D.H. Fisher, "Knowledge acquisition via incremental conceptual clustering", Machine Learning, 2, pp.139-172, 1987.

[5] T.SAWARAGI, et al., "Dynamic diagnosis for plant anomalies and real-time supporting using conceptual formation from time series data", SICE,22nd Symposium on Intelligent System, Nov.,1995, Toyama, Japan, pp. 339-346, 1995 (in Japanese).

Table 1: Contents of Malfunctions as Anomalies Carried out in Examination using Plant Simulator

Malfunction No.	Contents of Malfunctions
W-01-01	Failure in SG Ooutlet Steam Temperature Controller (increasing Feedwater Flowrate in 3 ,i.e.,A,B,C ,Loops)
W-02-01	Failure in SG Ooutlet Steam Temperature Controller (decreasing Feedwater Flowrate in 3 Loops)
W-03-01	Opening Outlet Valve of SG Bypass Tube by Mistake
W-04-01	Opening Release Valve of SG Inlet in A Loop by Mistake
W-05-01	Opening Drain Valve of Water/Steam Seperator in A Loop by Mistake
W-06-01	Opening Bypass Valve of SH in A Loop by Mistake
W-07-01	Abnormal Condition of Bearing Oil System of main Feedwater Pump in A Loop
W-08-01	Failure in Differential Pressure Controller of Feedwater Flowrate Reguration Valve (into increasing)
W-09-01	Failure in Differential Pressure Controller of Feedwater Flowrate Reguration Valve (into decreasing)
W-10-01	Failure in Differential Pressure Controller of Feedwater Flowrate Reguration Valve (opening Valve)
W-11-01	Failure in Differential Pressure Controller of Feedwater Flowrate Reguration Valve (closing Valve)
W-12-01	Closing 1st Extraction Steam Valve by Mistake
W-12-02	Closing 2nd Extraction Steam Valve by Mistake
W-12-03	Closing 4th Extraction Steam Valve by Mistake
W-13-01	Closing Feedwater Stopping Valves in all the 3Loop
W-13-02	Closing Feedwater Stopping Valve in a Loop (A Loop)
W-14-01	Failure in Drain Water Level Controller of high Pressure 1st Heater Drain (Drain Valve Closure)
W-14-02	Failure in Drain Water Level Controller of high Pressure 2nd Heater Drain (Drain Valve Closure)
W-14-03	Failure in Drain Water Level Controller of low Pressure 1st Heater Drain (Drain Valve Closure)
W-14-04	Failure in Drain Water Level Controller of high Pressure 2nd Heater Drain (Drain Valve Closure)
W-14-05	Failure in Drain Water Level Controller of high Pressure 3rd Heater Drain (Drain Valve Closure)
W-16-01	Closing Inlet Header Pressure Reguration Valve of Extraction Air in Main Steam System by Mistake
W-16-02	Closing Inlet Header Stopping Valve of Extraction Air in Main Steam System by Mistake
W-17-01	Adhesion of Shaft of main Feedwater Pump in A Loop
W-18-01	Rapture of main Feedwater Tube of A Loop
W-20-01	Increasing of Friction in Bearing of main Feedwater Pump in A Loop
W-22-01	Leak by Rapture in Condenser Tube
W-23-01	Failure in Condensate Hotwell Water Level Controller (increasing Water Level to very highLevel)
W-23-02	Failure in Condensate Hotwell Water Level Controller (increasing Water Level to highLevel)
W-24-01	Trip by Overload in Condensate Pump
W-25-01	Trip by Overload in Condensate Booster Pump
W-27-01	Rapture of high Pressure 1st Heater Drain
W-27-02	Rapture of high Pressure 2nd Heater Drain
T-03-01	Failure in Steam Pressure Controller (closing main Steam Reguration Valve)
T-03-02	Failure in Steam Pressure Controller (opening main Steam Reguration Valve)
T-04-01	Steam Line Breaker

A BASIC DESIGN OF ALARM SYSTEM FOR THE FUTURE NUCLEAR POWER PLANTS IN KOREA

Cheol-Kwon Lee, Seop Hur, Jae-Hwal Shin, In-Soo Koo, and Jong-Kyun Park
Korea Atomic Energy Research Institute
Taejon, Korea

ABSTRACT

The design of an advanced alarm system is under way to apply to the new MMIS for the future nuclear power plants in Korea. Based on the alarm system design bases we established the design requirements and are now refining them with the results of evaluation through the prototype. To realize the advanced system new algorithms for alarm processing and display are implemented and various new devices are examined. The evaluation for the design is performed in accordance with the verification and validation plans and through the prototype.

1. BACKGROUNDS

The alarm system plays an important role in the operation of nuclear power plants (NPPs) since it provides the status changes of plant or process before other information display systems. As well, the system makes it easy for the operator to decide the necessary control actions under the abnormal conditions by providing information related to the changes.[1)] However the system has revealed a few of vulnerabilities in spite of its importance within the plant, and much efforts have followed to improve the system, especially since TMI accident. Entering the 1980s the design concepts for the new man machine interface system (MMIS) has begun to be established and the alarm system was included as a weighted system in the MMIS. The MMIS requires an alarm system to solve the problems reported on the conventional system and to be designed to add new features or to supplement its own functions in accordance with the MMIS design concepts.[2)]

In Korea, from the middle of 1980s the development of new MMIS design was started and the design concept was completed in the early of 1990s. Its design goals are to improve the plant safety, to be cost effective and to meet current regulatory requirements. The MMIS design includes the main control room design containing an operator-oriented compact workstation. From the MMIS design it is shown that the alarm system, as an integrated part of MMIS, should be an advanced one to solve the problems existed in the conventional alarm systems and to incorporate the new technologies and devices.[3),4)]

The design of alarm system is under way based on the MMIS design bases. The prototype is also being developed to evaluate the design requirements established, the functions assigned to the system, and the validity for the application of new technologies and devices.

2. DESIGN BASES OF ALARM SYSTEM

The design bases of alarm processing and presentation are, based on MMIS design bases, established as following;

- to provide the operator with alarm states in timely manner,
- to reduce the number of alarms effectively to reduce the operator workload,
- to be integrated with other information systems to facilitate the operator tasks.

The alarm information in the MMIS is represented on three plant information systems consisted of wall mimic display, CRT, and flat-panel display. The system level and major component level alarms are displayed on the wall mimic that shows the overview for the plant status. The important process and component alarms are displayed through alarm windows depicted on the flat-panel display. Those include, for example, R.G. 1.97 Category 1 parameters, alarms that require quick response by the operator, and alarms frequently used. The CRT treats all plant information including detailed alarm information driven by plant computer. It is required that the flat-panel display and CRT provide alarm data to generate mimic wall alarm and the flat-panel display alarms be provided with operator so as to support continuous operation in the event of failure of CRT system. The following section describes the design of flat-panel alarm system, which has alarm windows.

3. ESTABLISHMENT OF DESIGN REQUIREMENTS

The system overview is summarized as follows;

- The alarm system provides its major functions, that are alerting, informing, guiding and confirming, to assist the operator to monitor the plant and to take the necessary action required to preserve normal operating conditions.

- The system supports continued plant operation in the event of failure of CRT system.

- The system processes new algorithms to improve the man machine interfaces, which are signal validation, alarm filtering/suppression, alarm prioritization, pattern recognition and other features.

- Alarms are displayed on alarm tiles and message windows depicted on the spatially dedicated flat-panel displays in the main control room (MCR) and remote shutdown panel (RSP).

- The system has a segmented and distributed architecture to localize the any failures and to realize the real-time processing.

The system performs input signal processing, alarm processing, alarm display and controls, and interface with other plant systems.

- Input signals to the system are put into limit check, engineering unit conversion, and signal validation to calculate the representative values from multiple channel sensors. The signal validation uses a simple averaging algorithm without analytic process model so that real-time processing is realizable.

- Alarms are generated under dark-board at power design concept and based on the validated parameters to reduce the nuisance alarm. Alarm processing uses proven or provable techniques not to require new research or big analyses.

- Alarm display and control are designed to maximize the man-machine interface function. Therefore alarms generated on the displays are coded by color and shape, grouped by system, function, priority and etc. Alarm control adopts the touch-operation. The flashing rates and audible tones are distinctive by alarm status and priority. Alarm display design maintains the consistency with that of other information.

- The system interfaces with other plant systems via communication data network to receive input data and to transmit the alarm data processed within the system.

The system provides a high degree of reliability and its availability goal is more than 99%. Thus the system is designed to be redundant and maintains a diversity with other information systems. The system covers all plant power conditions, transients and trip conditions. Any failures from each component are accommodated and alarmed to the operator. The design is flexible and expandable to adopt changing needs through the life of system. The software design incorporates a top-down structured design and prevents the unexpected results. The developed software are put into the verification and validation (V&V) process to assure its quality.

Figure 1 presents the system configuration. The system is designed as a microprocessor based real-time system. Main processors perform input signal processing, alarm processing, data storage, and interfacing with other information systems. Display processors generate the alarm displays within the required response time. The displays use color and perform all man-machine interface functions with touch-operation. The data communication network which is deterministic, provides a data pass within the system and with backbone network containing all plant information.

The design is proceeded in accordance with the design process proposed by human factor engineering program plan, equipment qualification plan and software quality assurance plan being developed by other KAERI groups. The system prototype is developed to verify not only the major system functions and design requirements but the technologies which have not yet implemented in conventional power plants. The following evaluations are included; evaluation of system performance, validity check of input signal processing and alarm processing algorithms, evaluation of network performance, and availability and suitability verification for display design and man machine interface functions.

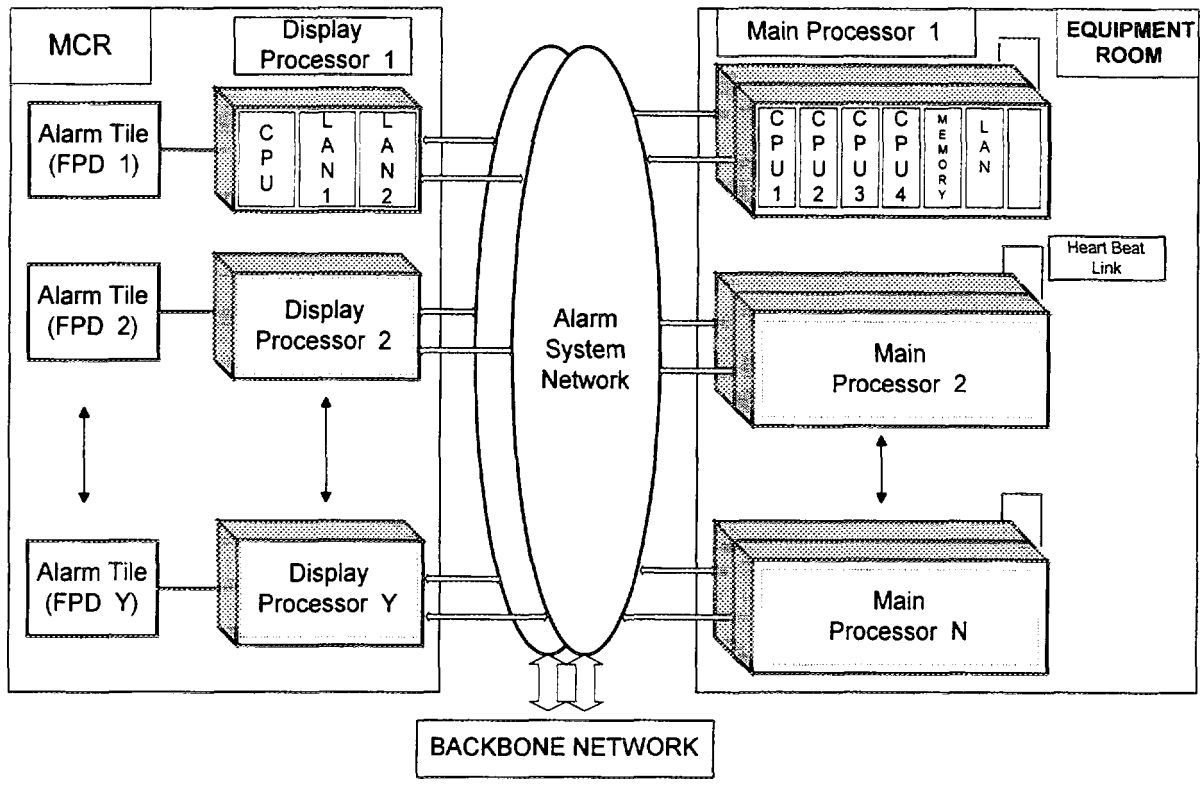


Figure 1: Alarm System Configuration

4. IMPLEMENTATION

This section describes on-going tasks to complete the design.

4.1 Refinement of Design Requirements

The design requirements are iteratively revised to incorporate the results from V&V as the design proceeds.

4.2 Alarm Selection

Alarm parameters will be selected based on the function and task analysis.

4.3 Signal Validation

This algorithm calculates the representative value from multiple channel sensor inputs, which are the values converted to engineering unit, to reduce the operator's stimulus overload and task loading. The results are inputted to alarm processing logics. The algorithm being developed is based on the mathematical averaging with degree of inconsistency calculation.[5] The functions of algorithm are at least to determine the representative value, to evaluate the bad sensor, and range check comparing the calculated value with maximum/minimum range.

4.4 Alarm Processing

The nuisance or irrelevant alarms are filtered out and the alarms which are less important under the given operating condition are suppressed.[6] Figure 2 presents the schematic of alarm processing. The algorithm being developed considers the alarm filtering techniques such as the plant operating mode dependency alarm generation by changing setpoint, and the time delay or deadband to eliminate the chattering alarm. Alarms are also activated based on the equipment status to allow the operator to monitor only real problems related to equipment status changes. The redundant alarms and less important alarms suppressed are accessible by operator upon request. Alarms activated from parallel working devices are displayed on a single alarm tile. Alarms are prioritized by its importance to plant safety and operation. The status alarms, that are not necessary to take action but displayed in the conventional system, are separated from this system and displayed on the CRT system.

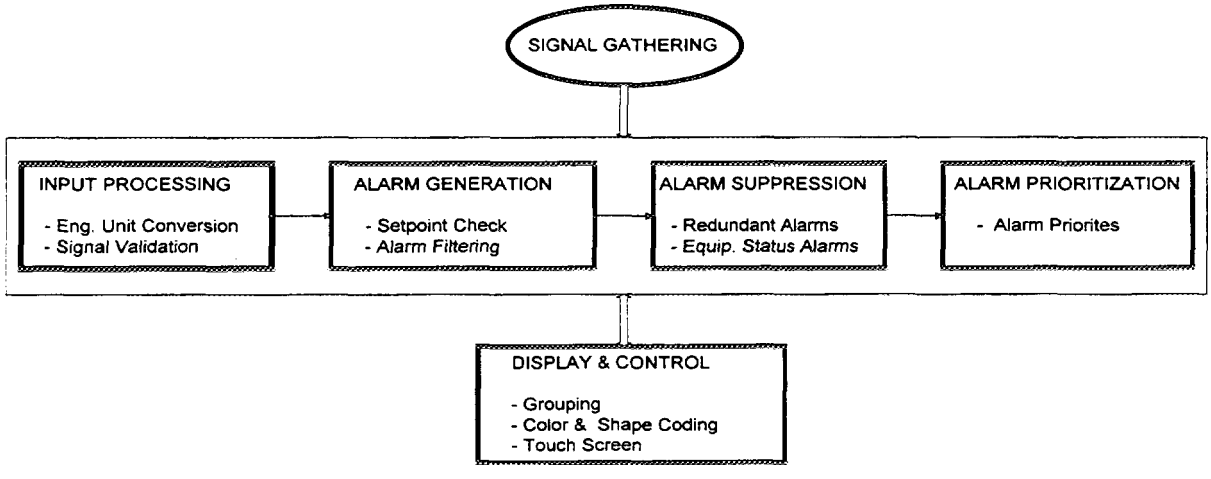


Figure 2: Schematic of Alarm Processing

4.5 Display Design

Alarms are displayed on the spatially dedicated flat-panel displays within the control panels. Alarms are grouped by system, function, priority, etc. Displays are designed incorporating the human factors considerations to reduce the operator workload. To increase the operator's cognition both color and shape coding are applied to the display design, which is unique in the control room and consistent with other information systems. The display contains at least alarm message, alarm status, alarm priority, current value, setpoint value, point identification, and is divided into two windows, alarm tile/message and alarm list. 3 to 4 flashing rate are considered to present the various alarm status.

4.6 Alarm Audibles and Controls Design

Audible tones direct the operator's attention to the control room area on which the alarm is presented. These are distinctive by alarm status and priority. Alarm controls are touch-operated

on the displays. Alarm sequences are combined with silence, acknowledge, reset, ringback, and realarm.

4.7 Prototype Development

The prototype is being developed under the minimum scope based on the system configuration shown in Figure 1, which is possible to verify the design. In the future the scope will be extended to the whole system for full scope simulation.

The prototype consists of a main processor, 2 display processors, 2 color flat-panel displays, and alarm data network. The system maintains the redundancy with the exception of display processor and flat-panel displays. For software design DOS or real-time OS are examined, which should be a proven product gained industry acceptance through its usage. C++ language is used for application software.

4.7.1 Main Processor

The main processor is composed of the standard backplane bus and plug-in modules for segmented CPU boards with interfacing chip or controller, IC memory board, network board, and other boards. The processor performs tasks such as input signal gathering and processing, data storage, alarm processing, communication and diagnosis. The system is a multi-processing system on the basis of tasks, to improve its performance and to be protected from any problems which may be unexpectedly caused. The processor is constructed as a dual system with primary processor and backup processor, and the heart-beat function is added to fail-over to the backup processor without interrupting the alarm information when fault occurred in the main processor. In normal operation, both processors are on-line active, and the primary processor transmits at regular intervals the heart-beat to the backup processor.

The standard backplane bus provides a data path among plug-in modules within main processor without disturbing the internal activities of other modules interfaced with this bus. This bus is an industrial open standard system and provides the high performances and the solutions for constructing versatile system.

Each CPU board has a processor, main memory, timer/counter, real-time clock, watchdog timer, bus and buffers, interrupt logic and controller, and other devices to achieve the tasks. For the high performance and reliable multiprocessing, the CPU performs its tasks separately and the dynamic random access memory is utilized such that all tasks are memory resident.

The memory board contains an alarm database in the shared memory. The network board has a baseband and token-passing protocol.

4.7.2 Display Processor

The display processor is a computer system consisting of a CPU board with memory, interfacing chip or controller, and I/O interface devices and network boards. The processor generates the static and dynamic alarm information within the required response time based on the data from

main processor. The CPU performs high reliable function such as communication, alarm display processing, and diagnosis. The display CPU also utilize dynamic random access memory such that a task is memory resident.

The network boards are designed to be redundant and have the same function as that of main processor.

4.7.3 Color Flat-Panel Display

Spatially dedicated flat-panel displays present alarm and perform all man-machine interface functions with touch operation. TFT LCD or EL displays are examined taking account into viewing angle, brightness, the number of color and the trend of technology.

4.7.4 Data Network

The data network uses LAN that is designed to be redundant to permit on-line maintenance, testing and repair. The network has a baseband and token-passing protocol and deterministic architecture.[7] A baseband and token-passing network provides a robust network that is not susceptible to failure if cable comes loose or disconnected. The token-passing protocol has virtually no chance of errors since every transaction are acknowledged.

5. CONCLUSIONS

The design of alarm system incorporates not only new algorithms for alarm processing and display but also digital and data network technologies, which do not have much experience in nuclear power plants. As well it is required in the MMIS design of nuclear power plants that human factor engineering principles should be incorporated. For these reasons the establishment of design procedures and the equipment (hardware and software) qualification become major issues in the development of MMIS in nuclear industry. Even though many researches propose the design guidelines, there exists still many difficulties to overcome the strict requirements.

As a way to solve them, KAERI is preparing the standard design procedures, equipment qualification plans, and verification and validation plans including software verification and validation method. The final alarm system design will be established in accordance with them, and the new algorithms and technologies applied will be verified through the prototype and/or other methods. We are trying to find the best design for alarm reduction and display which is able to provide the operator with alarms without the loss of the necessary operational information. Therefore it is expected these design activities will lead to the good design.

REFERENCES

[1] NUREG/CR-3987, "Computerized Annunciator Systems", U.S. NRC, Jun., 1985.
[2] EPRI ALWR URD, Vol. II, Rev. 03, Chapter 10, EPRI, Nov., 1991.
[3] I.S. Koo et al., "Design Requirements of Instrumentation and Control Systems for Next Generation Reactor", KAERI/TR-423/94, Mar., 1994 (in Korean).

[4] I.S. Koo, "Draft Design Requirements for Instrumentation and Control Systems in Next Generation Nuclear Power Plant", VTT Symposium 147: Advanced Control and Instrumentation Systems in Nuclear Power Plants - Design, verification and validation, IAEA/IWG/ATWR & NPPCI Technical Committee Meeting, June 20-23, 1994, p. 263 Technical Research Centre of Finland, Espoo/Helsinki, Finland (1994).

[5] I.K. Hwang et al., The development of a signal validation scheme for the redundant multi-channel measurement system", Journal of Korean Nuclear Society, Vol. 26, No. 3, p 367-373, Sep., 1994.

[6] C.K. Lee et al., "The Evaluation of Advanced Alarm Processing Technology", Proceedings of the Korean Nuclear Society Spring Meeting", Vol. 1, p 321-326, Cheju, Korea, May 1996 (in Korean).

[7] D.H. Kim et al., "Development of Design Methodology for Communication Network in Nuclear Power Plants", KAERI/TR-700/96, Jun., 1996 (in Korean).

SESSION VII

GENERAL DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

GENERAL DISCUSSION, CONCLUSIONS AND RECOMMENDATIONS

It is my pleasure to provide a summary of the conference on "Experiences and Improvements in Advanced Alarm Annunciation Systems in Nuclear Power Plants".

In my opinion, and judging from comments made to me during the last day, the objectives of the meeting have been met. Namely, the meeting did provide a forum for the presentation and discussion on R&D, in-plant experiences and improvements to annunciation systems. In the Welcoming Address, I quoted from two references published in 1974. Several areas of annunciation were highlighted as needing improvement. Based on the papers presented this week, I am pleased to report that we have made considerable progress.

Improvement Area	**Progress Reported at this Meeting**
Design philosophy	Papers gave examples of definitions for alarms Definite link to plant operating philosophy
Alarms versus status messages	Several groups separating messages into fault/abnormal versus status
Too many alarms	Extensive use of conditioning, and prioritizing based on consequences and urgency
Better hierarchy of information	Designs and implementation based on object oriented approaches, defining relationships between alarms, and use of function-oriented alarms
Analysis effort	Tools being designed and used to allow cost effective analysis of large numbers of alarms

Though much progress has been made, there were three main areas that stood out where future work is still required. Each of these topics goes beyond the annunciation domain as they address issues at both an overall control centre and plant design level. As such, they are excellent topics for future Specialists' Meetings.

Cost-Effective Design and Regulatory Process

This area addresses whether a function-oriented design approach is more effective than current systems-oriented approaches, both from a design and regulatory viewpoint. Several papers at this meeting reported that a function-oriented approach was a key to creating an effective alarm system.

Cost- Effective Evaluation of Improvements

With increasing emphasis on provenness before innovations will be accepted into an existing plant or new designs, cost effective methods for evaluating improvements need to become accepted industry practice. A range of approaches were presented at the meeting.

Classification and Categorization of Plant Information Systems

The area of categorizing systems based on reliability, impact on plant safety, and other factors is becoming increasingly important. Approaches need to be defined if utilities and regulators are to agree to the introduction of "operator aids", diagnostic systems, etc.

In closing, I would like to thank the presenters, session chairs, and conference participants for making this an excellent forum for the sharing of information. Special thanks to Monica Cliche and Judy Gilchrist for their logistical and administrative support; the smooth operation of the meeting is a tribute to their behind-the-scenes efforts. I would also like to express my appreciation to other members of the organizing committee for their contribution to the organization of the meeting: Eric Davey, Mark Feher, Jad Popovic, Debbie Gillard, and Felicity Harrison.

I wish everyone a safe journey and look forward to meeting each of you at a future meeting.

Lawrence Lupton
Chairperson, Conference Organizing Committee

LIST OF PARTICIPANTS

LIST OF PARTICIPANTS

Name:	Address:	Telephone:	Fax:
CANADA			
Rick Basso	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 3420	613-584-9541
Sam Basu	Ontario Hydro, Bruce A Nuclear Generating Station, P.O. Box 3000 Tiverton, ON N0G 2T0	519-361-3670	519-361-6410
Dave Beattie	Humansystems Incorporated 111 Farquhar Street, 2nd floor Guelph, ON N1H 3N4	519-836-5911	519-836-1722
Lorna Beresford	Ontario Hydro Darlington Generating Station, P.O. Box 4000 Bowmanville, ON L1C 3W2	905-623-6670	
Mike Bosnich	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 3964	613-584-9541
Lyndsay Brazier	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 6270	613-584-9541
Fiona Bremner	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 6272	613-584-9541
Eric Davey	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 3425	613-584-9541
Michel Désaulniers	Hydro Quebec, Centrale Nucleaire Gentilly 2, 4900 Boul. Becancour Gentilly, PQ G0X 1G0	819-298-2943 Ext 5038	819-298-5648
Raymond Dufresne	Hydro Quebec Centrale Nucleaire Gentilly 2, 4900 Boul. Becancour Gentilly, PQ G0X 1G0	819-298-2943 Ext. 5293	819-298-5694
Mostafa Elbehairy	Ontario Hydro Darlington Generating Station, P.O. Box 4000 Bowmanville, ON L1C 3W2	905-623-6670	
Jody Everitt	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 3674	613-584-9541
Mark Feher	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 3917	613-584-9541
Felicity Harrison	AECB, Martel Building 280 Slater Street Ottawa, ON K1P 5S9	613-995-3808	613-995-5086
Davelyn Hickey	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 4359	613-584-9541

Name:	Address:	Telephone:	Fax:
Jim Hinton	AECL Sheridan Park Research Community 2251 Speakman Drive Mississauga, ON L5K 1B2	905-823-9040 Ext 3166	
Paul Jones	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 3453	613-584-9541
Ross Judd	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 3175	613-584-9541
Loay Khartabil	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 6269	613-584-9541
Tim Long	Ontario Hydro Darlington Generating Station P.O. Box 4000 Bowmanville, ON L1C 3W2	905-623-6670	
Lawrence Lupton	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 3433	613-584-9541
Gerry Lynch	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 3898	613-584-4434
Garry Mitchel	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 4095	613-584-9541
Roy Olmstead	AECL Sheridan Park Research Community 2251 Speakman Drive Mississauga, ON L5K 1B2	905-823-9040 Ext 5024	
Jadranka Popovic	AECL Sheridan Park Research Community 2251 Speakman Drive Mississauga, ON L5K 1B2	905-823-9040 Ext 4709	
Yi Qin	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 3812	613-584-9541
Diego Rivera	AECL Sheridan Park Research Community 2251 Speakman Drive Mississauga, ON L5K 1B2	905-823-9040 Ext 3184	905-855-8173
Al Rosevear	NB Power 515 King Street, P.O. 2000 Fredericton, NB E3B 4X1	506-458-4444	
Ushnish Sengupta	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 4493	613-584-9541

Name:	Address:	Telephone:	Fax:
Debbie Gillard	Ontario Hydro Darlington Generating Station P.O. Box 4000 Bowmanville, ON L1C 3W2	905-623-6670	
Ramnik Shah	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 3419	613-584-1770
Brian Smith	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 6063	613-584-9541
Mike Thompson	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 4043	613-584-9541
Gabe Tosello	AECL Chalk River Laboratories Chalk River, ON K0J 1J0	613-584-3311 Ext 3466	613-584-9541
FRANCE			
Williams Cette	IPSN - CEA BP 6 92265 Fontenay Aux Roses Cedex France	46-54-9585	33-7-46-54-9599
Dominique Pirus	EdF - Spten 12/14 Avenue Dutrievoz F-69628 Villeurbanne Cedex, France	33-7282-7477	011-33-7282-7704
Marc Pont	EdF EPN/MCP DXP Quartier Michelet 13-27 Esplanade Charles de Gaulle F-92060 Paris la Defense Cedex, France	16-1-49-02-0292	011-33-1-49-02-0112
GERMANY			
Freddy Seidel	Federal Office for Radiation Protection, P.O. 100149, D-38201 Salzpitter, Germany	5341-225-151	49-5341-225-225
JAPAN			
Masayoshi Abe	Nuclear Power Planning Group Nuclear Power Department Tohuko Electric Power Company, Inc. 3-7-1 Ichibancho, Aoba-ku Sendai 980 Japan	81-22-225-3634	81-22-217-3567
Masahiro Imase	Mitsubishi electric Corp. Nuclear Power Department, Wadaski-cho 1-1-2, Hyogo-ku Kobe, Japan		
Yuji Kobayashi	Toshiba Corporation Isogo Nuclear Engineering Center 8, Shinsugita-cho, Isogo-ku, Yokohoma, 235 Japan	81-45-770-2316	011-81-45-770-2316
Yukiharu Ohga	Power & Industrial Systems R&D Division Hitachi Ltd. 7-2-1 Omika-cho, Hitchai-shi, Ibaraki-ken, 319-12 Japan	81-294-53-3111 ext 5143	81-294-53-2830
Yoshihiko Ozaki	Frontier Technology Section, O-Arai Engineering Center, Power Reactor & Nuclear Fuel Development Corporation, 4002, Narita-Cho, O-arai-Machi, Ibaraki-Ken, 311-13 Japan		011-81-29-266-3868

Name:	Address:	Telephone:	Fax:
Manabu Shimada	Kansai Electric Power Co., Ltd. Nakanoshimo 3-3-22, Kita-Ku, Osaka, 530-70 Japan	06-441-8821	06-441-4277
NORWAY			
Andreas Bye	Institutt for Energiteknikk, OECD Halden Reactor Project, P.O. Box 173, N-1751, Halden, Norway	47-69-183100	47-69-187109
REPUBLIC OF KOREA			
Myoung-Eun Che	KEPCO 167, Samsong-Dong Kangnam-ku Seoul 135-791 Republic of Korea	02-550-4952	011-82-2-550-4999
Hak-Yeong Chung	KEPCO 103-16, Mungi Dong Yosung Gu, Taejon Republic of Korea	82-42-865-5731	82-42-865-5314(5104)
Chang-Shik Ham	KAERI - Advanced I&C Project 150, Dukjin-dong, Yusong, Taejon, 305-353, Republic of Korea	82 42-868-2922	82-42-868-8357
Chang-Gi Kim	Yong-gwang 1&2 KEPCO 514, Kye-ma, Hong-none, Yong-gwang, Jeon-nam, 513-880 Republic of Korea	02-550-4952	82-2-550-4999
Han-Soo Kim	Nuclear Plant Construction Korea Electric Power Corporation Seoul, Korea		(011) 822-3456-5799
Jung Taek Kim	KAERI - Advanced I&C Project P.O. Box 105 Yusong, Taejon 305-600, Republic of Korea	82-42-868-2404	82-42-868-8357
Cheol-Kwon Lee	Korea Atomic Energy Research Instititute P.O. Box 105 Yusong, Taejon, 305-600, Republic of Korea	42-868-8657	82-42-861-1388
Hee Yang Oh	Nuclear Plant Construction Korea Electric Power Corporation Seoul, Korea		
SLOVAK REPUBLIC			
Adam Gieci	NPPRI Beethovenova 5, 917 01 Trnava, Slovak Republik	42-805-605-410	42-805-501-365
Marián Hrehus	NPPRI Fackova 1, 919 35 hrnciarovce, Slovakia	42-805-605-332	42-805-501-365
Ludovit Molnar	Slovak Technical University Faculty of Electrical Engineering and Information Technology Ilkovicova 3, 812 19 Bratislava, Slovakia	42-7-729-502	42-7-720-415
Vladimir Vojtek	Slovak Technical University Faculty of Electrical Engineering and Information Technology Ilkovicova 3, 812 19 Bratislava, Slovakia	42-7-791-387	

Name:	Address:	Telephone:	Fax:
SWEDEN			
Bengt Jansson	Forsmarks Kraftgrupp AB Vattenfall S-742 03 Oesthammar, Sweden	46-173-810-00	46-173-551-16
Gerd A. Svensson	Swedish Nuclear Power Inspect. S-10658 Stockholm, Sweden	46-8-698-8400	46-8-661-9086
UNITED STATES OF AMERICA			
Cliff Doutt	US Nuclear Regulatory Commission Mail Station 8H3 Owen 11555 Rockville Pike Rockville, MD USA 20852 2738	301-415-2847	301-415-3577
James Easter	Westinghouse Electric Corporation P.O. Box 355 Pittsburgh, PA USA 15230	412-374-5137	412-374-5744
John O'Hara	Brookhaven National Laboratory Building 130 Upton, NewYork USA 11973	516-344-3638	516-344-4900